Вестник РУДН. Серия: Юридические науки 2026 Т. 30. № 1. 70–89
RUDN JOURNAL OF LAW. ISSN 2313-2337 (Print), ISSN 2408-9001 (Online) http://journals.rudn.ru/law

ПРАВО И ЦИФРОВЫЕ ТЕХНОЛОГИИ

LAW AND DIGITAL TECHNOLOGIES

https://doi.org/10.22363/2313-2337-2026-30-1-70-89
EDN: QYRWDJ

Научная статья / Research Article

Антикриминальный потенциал машинного обучения: предиктивная аналитика предупреждения цифрового вовлечения в террористическую деятельность

М.М. Маджумаев ✉, О.А. Кузнецова

Российский университет дружбы народов, *г. Москва, Российская Федерация*
✉ murad.mad@outlook.com

Аннотация. Развивающиеся цифровые технологии, а также характерные для нового поколения Интернета, Web3, псевдонимность и децентрализованные системы именования, наряду с анонимностью, общедоступностью и трансграничным характером информационных потоков, эксплуатируются террористическими группировками для вербовки новых членов и исполнителей отдельных общественно опасных деяний. Традиционные реактивные меры по противодействию терроризму оказываются недостаточными в условиях быстрого распространения незаконного контента, которые оставляют заметные цифровые следы. В этой связи важно изучить возможности передовых вычислительных методологий, в частности антикриминального потенциала искусственного интеллекта в предотвращении преступлений террористической направленности. Исследование направлено на изучение и продвижение потенциала машинного обучения и предиктивной аналитики как надежного механизма выявления и предотвращения участия в террористической деятельности путем определения индикаторов и цифровых следов, которые способствуют стратегическому переходу к проактивным парадигмам безопасности. В работе представлена мультимодальная аналитическая структура, сочетающая в себе обработку естественного языка, компьютерное зрение, аудиоанализ и анализ социальных сетей, с подробным описанием процесса машинного обучения от предварительной обработки данных до внедрения модели. В качестве практического применения рассматривается система «RED-Alert», а также предлагается новый модуль «Пороговое адаптивное вмешательство» (ПОРА), который использует графовые нейронные сети и анализ временных рядов для оценки цифровых рисков. Системы машинного обучения демонстрируют значительную эффективность в выявлении угроз и создании базы цифровых доказательств. Это требует переоценки ответственности провайдеров интернет-услуг, особенно в части коллективного цифрового бездействия. Предлагается дифференцированный подход к установлению

ответственности, который учитывает техническое влияние провайдеров интернет-услуг. При этом описываемые индикаторы риска, определенные с помощью искусственного интеллекта, остаются вспомогательными инструментами в установлении вины субъекта. Машинное обучение и предиктивная аналитика способны преобразовать деятельность по предупреждению терроризма.

Ключевые слова: искусственный интеллект, нейронная сеть (нейросеть), цифровые следы, Пороговое адаптивное вмешательство (ПОРА), ответственность провайдеров интернет-услуг, система «RED-Alert», предупреждение преступлений

Вклад авторов: *Маджумаев М.М.* – разработка концепции исследования, подбор и анализ материалов, написание введения, текста статьи и заключения; *Кузнецова О.А.* – обзор исследований по теме научной статьи, написание введения и работа с научными выводами статьи. Оба автора ознакомились с окончательной версией статьи и одобрили ее.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Финансирование. Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478, https://rscf.ru/project/25-28-01478/

Поступила в редакцию: 22 июля 2025 г.
Принята к печати: 15 января 2026 г.

Для цитирования:

Маджумаев М.М., Кузнецова О.А. Антикриминальный потенциал машинного обучения: предиктивная аналитика предупреждения цифрового вовлечения в террористическую деятельность // RUDN Journal of Law. 2026. Т. 30. № 1. С. 70–89. https://doi.org/10.22363/2313-2337-2026-30-1-70-89 EDN: QYRWDJ

Anti-Crime Potential of Machine Learning: Predictive Analytics for Preventing Digital Terrorism Activities

Murad M. Madzhumayev ✉, Olga A. Kuznetsova

RUDN University, Moscow, Russian Federation
✉ murad.mad@outlook.com

Abstract. Advances in digital technology – particularly Web3's pseudonymity and decentralized naming systems, combined with information flows' anonymity, accessibility, and cross-border nature – enable terrorist organizations to recruit members and perpetrate discrete socially dangerous acts. Conventional reactive counterterrorism measures prove inadequate against rapid illicit content dissemination that leaves detectable digital traces. This study explores artificial intelligence's (AI) counter-criminal potential on machine learning and predictive analytics for proactively identifying and preventing terrorist activity through behavioral indicators and digital footprints that facilitate a strategic shift to proactive security paradigms. The research develops a multimodal analytical framework integrating natural language processing, computer vision, audio analysis, and social network analysis, detailing the complete machine learning pipeline from data preprocessing to model deployment. It examines the "RED-Alert" system as practical implementation and proposes a novel "Threshold Adaptive Intervention" (PORA) module utilizing graph neural networks and time-series analysis for digital risk assessment. Machine learning excels at threat detection and digital evidence generating, necessitating reevaluation of internet service providers' (ISP) liability – particularly collective digital inaction. A differentiated liability framework accounts for providers' technical influence while treating AI-derived risk indicators as ancillary tools for establishing individual culpability. Machine learning and predictive analytics enable a strategic shift to proactive counterterrorism.

Key words: artificial intelligence, neural network, digital traces, Threshold Adaptive Intervention (PORA), ISP liability, RED-Alert system, crime prevention

Authors' contribution: *Madzhumayev M.M.* – research concept development, material selection and analysis, drafting introduction, main body, and conclusion; *Kuznetsova O.A.* – literature review, introduction drafting, scientific conclusions editing. Both authors reviewed and approved the final version of the manuscript.

Conflict of interest. The authors declare no conflict of interest.

Funding. The research was supported by the Russian Science Foundation (RSF) under grant No. 25-28-01478 https://rscf.ru/project/25-28-01478/

Received: 22th July 2025
Accepted: 15th January 2026

For citation:

Madzhumayev, M.M., Kuznetsova, O.A. (2026) Anti-Crime Potential of Machine Learning: Predictive Analytics for Preventing Digital Terrorism Activities. *RUDN Journal of Law.* 30 (1), 70–89. (in Russian). https://doi.org/10.22363/2313-2337-2026-30-1-70-89 EDN: QYRWDJ

Введение

Стремительное развитие цифровых технологий, сети Интернет и особенно его нового поколения Web3, построенного на основе технологии блокчейн, предполагающей децентрализацию, существенно расширило арсенал высокотехнологичных средств для совершения преступлений террористической направленности. Киберсреда обладает определенными характеристиками, придающими ей «привлекательность» для лиц, вовлеченных в террористическую деятельность. Прежде всего, анонимность, общедоступность и трансграничность обеспечивают «эффективное» распространение насильственной идеологии, вербовку сторонников и координацию действий (со)участников.

Деструктивная информация мгновенно распространяется в социальных сетях, специализированных сайтах и форумах, практически минуя мануальный контроль модераторов. Полный контроль такого информационного трафика вручную требует принятия специальных мер и привлечения дополнительных финансовых средств. К тому же существующие механизмы контроля становятся все сложнее, а правоохранительным органам все труднее контролировать и обеспечивать ограничение доступа к онлайн-контенту из-за присущей Web3 псевдонимности и децентрализованных систем именования.

В настоящем исследовании категории машинного обучения и предиктивной аналитики рассматриваются в контексте их потенциала для предупреждения террористической деятельности, определение которой установлено пунктом 2 статьи 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму»[1]. Предлагаемые меры и алгоритмы направлены на выявление и предупреждение конкретных форм осуществления террористической деятельности в информационно-телекоммуникационных сетях, включая сеть Интернет. К данным формам, составляющим предмет настоящего анализа, относятся: организация, планирование, подготовка, финансирование и осуществление террористического акта, а также действия, связанные с организационной поддержкой и формированием преступных структур, такие как организация незаконного вооруженного формирования, преступного

[1] Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // Собрание законодательства Российской Федерации от 13 марта 2006 г. № 11 ст. 1146.

сообщества (преступной организации) или организованной группы для реализации террористического акта, равно как и участие в такой структуре. Особое внимание уделяется выявлению информационных и коммуникативных составляющих террористической деятельности, включая подстрекательство к террористическому акту, вербовку, вооружение, обучение и использование террористов, информационное или иное пособничество в планировании, подготовке или реализации террористического акта, а также пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления таковой.

Основываясь на устоявшихся правовых определениях, под публичными призывами к осуществлению террористической деятельности применительно к статье 205.2 Уголовного кодекса Российской Федерации (далее – УК РФ)[2] понимаются изложенные в любой форме (устно, письменно, с использованием технических средств) обращения к третьим лицам в целях побуждения их к осуществлению деятельности террористического характера, а именно к совершению преступлений, установленных статьями 205–206, 208, 211, 220, 221, 277, 278, 279, 360, 361 УК РФ[3]. Под публичным оправданием терроризма следует понимать публичное заявление о признании идеологии и практики терроризма правильными, заслуживающими поддержки и подражания (примечание 1 к ст. 205.2. УК РФ). Соответственно, под пропагандой терроризма понимается систематическое распространение материалов и (или) информации, направленных на формирование у лица идеологии терроризма, убеждение в ее привлекательности или формирование представления о допустимости участия в террористической деятельности (примечание 2 к ст. 205.2 УК РФ).

Современная цифровая экосистема, которой присущи огромные масштабы, скорость и внутренняя сложность, порождает необходимость внедрения и применения передовых аналитических технологий для распознавания латентных закономерностей, сигнализирующих о противоправной деятельности. Предиктивная аналитика, как один из таких приемов, ориентированный на оценку данных и в том числе способный взаимодействовать с искусственным интеллектом, представляет собой методологическую основу, которая оперирует статистическими алгоритмами, моделями машинного обучения и методами добычи данных (data mining) (Strielkowski et al., 2023). Она позволяет анализировать текущие и исторические данные для прогнозирования будущих событий или определения вероятностных исходов (Strielkowski et al., 2023). В отличие от описательной или диагностической аналитики, которые направлены на изучение того, что произошло и почему это произошло, предиктивная аналитика является прежде всего прогностической, нацеленной на предвидение будущих событий или моделей поведения на основе предполагаемых взаимосвязей в данных.

Выявляя ранние индикаторы, аномальные цифровые следы и развивающиеся сетевые структуры, связанные с планированием или осуществлением террористической деятельности до того, как она полностью осуществится, предиктивная аналитика становится тем самым уникальным и необходимым инструментом для

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрании законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954.

[3] Постановление Пленума Верховного Суда РФ от 9 февраля 2012 г. № 1 (с изменениями, внесенными постановлением Пленума от 3 ноября 2016 г. № 41) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности». Режим доступа: https://vsrf.ru/documents/own/8266/ (дата обращения: 02.01.2025).

упреждающего обнаружения угроз, их пресечения и стратегического распределения ресурсов. Это особенно важно для преодоления проблем, связанных с эфемерным и часто замаскированным характером цифровых коммуникаций, поддерживаемых террористическими элементами (формированиями), посредством внедрения методологии, основанной на данных, для навигации и интерпретации сложных информационных массивов большого масштаба.

Формы цифрового вовлечения лиц в террористическую деятельность

Вовлечение в террористическую деятельность в сети Интернет может принимать самые разные формы, перечень которых не является исчерпывающим и включает следующие:

– создание и размещение на тематических хостингах аудио-, фото- и видеоматериалов, со сценами насилия, призывами к террористической деятельности или оправданием террористических актов;

– ведение блогов и подкастов пропагандистского содержания, которые «популяризируют» идеологию насилия и склоняют к совершению преступлений террористической направленности;

– разработка приложений и игр, имплицитно или эксплицитно пропагандирующих терроризм, предназначенных для вовлечения молодежи;

– регулярное создание и распространение мемов, графических иллюстраций и других средств визуального контента с целью «нормализации» радикальных и насильственных идей среди целевой аудитории;

– эксплуатация соцсетей и мессенджеров для массового или целевого распространения пропагандистских материалов или прямой связи с потенциальными сторонниками;

– составление и распространение инструкций по изготовлению оружия, включая 3D-модели (в будущем и 5D-модели), CAD-файлы для печати на 3D- и 5D-принтерах (в будущем) или взрывчатых веществ;

– проведение интерактивных виртуальных собраний, тренингов для вербовки и обучения участников (в том числе в метавселенной);

– организация краудфандинга, в том числе через анонимные платежные платформы, а также вовлечение криптоактивов для финансирования террористической деятельности;

– манипулирование алгоритмами поисковых систем и социальных платформ для распространения идеологически «заряженного» контента, включая хэштег-кампании и скоординированные действия ботов; и другие.

Террористическая деятельность в цифровом пространстве (любое вовлечение в нее) с использованием информационных и коммуникационных технологий представляет собой осуществляемую целенаправленную деятельность, адресованную на распространение идеологии насилия и использование практик воздействия на принятие решений органами государственной власти, органами государственной власти субъектов, органами местного самоуправления или международными организациями, связанную с устрашением населения и (или) иными формами противоправных насильственных действий. В основном эта деятельность осуществляется на стадии приготовления (создания условий) к преступлению, оставляя цифровые следы, обнаружение которых может служить важным индикатором для выявления и пресечения готовящихся преступлений террористической направленности.

Антикриминальный потенциал искусственного интеллекта: предиктивная аналитика на основе машинного обучения

Гетерогенный характер цифрового взаимодействия между пользователями требует мультимодального аналитического подхода. Распространение материалов и (или) информации, наполненных различными оттенками идеологического содержания и часто сопровождающихся «закодированными» формулировками, эвфемизмами и культурно-специфическими языковыми нюансами, обусловливает необходимость использования современных инструментов обработки естественного языка (NLP). Для выявления потенциально опасных сообщений (сигналов) и направлений их распространения необходимо использовать алгоритмы семантического анализа, определения настроений, тематического моделирования и извлечения контекстной информации.

Учитывая все более широкое распространение аудио- и визуальных средств передачи сообщений террористическими элементами, технологии машинного обучения, компьютерного зрения и аудиоанализа могут быть использованы для распознавания объектов, идентификации лиц, анализа сцен и обнаружения характерных акустических сигналов (Rodriguez, 2025), указывающих на насилие или радикализацию (призывы (ключевые слова), выстрелы, взрывы и т.д.).

Технологии искусственного интеллекта, в частности предиктивная аналитика на основе машинного обучения, позволяют автоматизировать процесс анализа данных, выявлять закономерности и признаки (Taheri & Salimi Beni, 2025; Strielkowski et al., 2023) потенциальной террористической угрозы, а также прогнозировать вероятные сценарии преступной деятельности, основываясь на обработке больших массивов данных, содержащих текстовые, визуальные, аудио и другие цифровые элементы. Как следствие, все это позволит сформировать материалы, которые помогут изобличить виновных и собрать необходимые доказательства.

Искусственный интеллект представляет собой совокупность систематизированных структур, включающих вычислительные модели, алгоритмы, имитирующие человеческие способности, предназначенные для автономного решения задач без необходимости практического участия самого человека (Avanesyan, 2024; Filipova, 2024). Системы искусственного интеллекта по сути представляют собой процесс, который функционирует посредством процедурного сбора, классификации, синтеза и анализа данных и выдает результаты, аналогичные или превосходящие человеческие способности.

В существующих определениях искусственного интеллекта эти способности во многих случаях принято считать когнитивными функциями человека. Например, в п.п. «а» п. 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года[4], в п. «2» ч. 1 ст. 2 Федерального закона от 24.04.2020 № 123-ФЗ[5],

[4] Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Официальный интернет-портал правовой информации. Режим доступа: http://publication.pravo.gov.ru/document/view/0001201910110003 (дата обращения: 09.01.2025).

[5] Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства Российской Федерации от 27 апреля 2020 г. № 17 ст. 2701.

в п. п. 3.18 ГОСТ Р 59277-2020[6], п. 3.15 ГОСТ Р 70950-2023[7] и др. Однако на сегодняшний день уже можно утверждать, что помимо когнитивных функций человека, искусственный интеллект способен имитировать широкий спектр человеческих способностей, включая сенсорные, эмоциональные, моторные и физические (в сочетании с робототехникой), а также метакогнитивные способности.

Когнитивные способности человека, т.е. совокупность мозговых процессов, участвующих в познании окружающего мира, по классификации профессора М.В. Фаликмана, могут включать в себя такие способности, как восприятие, внимание, память, мышление, речь и воображение (Aisner & Naumov, 2021; Falikman, 2014). Системам искусственного интеллекта присущи (либо по крайней мере они способны имитировать), как минимум, такие способности, как обучаемость, память, мышление (логика), решение задач, планирование, прогнозирование, внимание и с некоторой долей условности креативность (Farina et al., 2024).

Согласно структуре сенсорной системы, предложенной профессором И.П. Павловым, она состоит из зрительной, слуховой и кожно-кинестетической сенсорных систем (Lomtatidze & Alekseeva, 2022). Это набор нервных путей и центров, отвечающих за прием, кодирование, передачу и обработку информации (декодирование) (Lomtatidze & Alekseeva, 2022). Системы искусственного интеллекта могут воспроизводить (имитировать) сенсорные способности, присущие человеку, такие как зрение, слух (Zhou, Men & Tsai, 2023) и осязание.

В частности, компьютерное зрение, направление в искусственном интеллекте (ИИ), которое позволяет компьютерам и системам интерпретировать и анализировать визуальные данные и извлекать значимую информацию из цифровых изображений, видео и других визуальных данных (Ponkin et al., 2024). Среди наиболее распространенных применений можно назвать следующие: обнаружение и распознавание объектов, обработка, понимание и анализ визуального контента (изображений, видео, документов), поиск товаров, классификация и поиск изображений, а также модерация контента. Компьютерное зрение активно применяется, например, в медицине, где алгоритмы компьютерного зрения способствуют анализу рентгеновских, магнитно-резонансных, компьютерных томографических изображений (Mishchenko, Misnik & Aleksandrov, 2024), в распознавании визуальных образов и распознавании лиц (Huang et al., 2023).

Способность слуха используется в распознавании речи, например, в виртуальных голосовых помощниках Алиса от Яндекса, Google Ассистент, Siri Apple (Apple Intelligence); в медицине, например, цифровые стетоскопы способствуют выявлению аномалий и анализу шумов сердца по акустическим данным (Arjoune et al., 2023); в криминалистике и судебной экспертизе различные программы используются для выявления дипфейк аудиоконтента (Aneja et al., 2024) и видеоконтента.

[6] Национальный стандарт РФ ГОСТ Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 23 декабря 2020 г. № 1372-ст) // Стандартинформ, Москва, 2021 г.

[7] Национальный стандарт РФ ГОСТ Р 70950-2023 «Технологии искусственного интеллекта в образовании. Функциональная подсистема управления успеваемостью обучающихся по программам подготовки научных и научно-педагогических кадров в аспирантуре. Общие положения и методика испытаний» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 октября 2023 г. № 1178-ст) // Российский институт стандартизации, Москва, 2023 г.

В качестве примеров тактильных (осязательных) возможностей систем искусственного интеллекта могут служить операции разнообразных роботов (как бытовых, так и промышленных), устройства виртуальной реальности с тактильной обратной связью (Zhang et al., 2022), а также применяющиеся в медицине при проведении хирургических вмешательств средства (Minopoulos et al., 2023).

При выполнении конкретной задачи они могут проявлять, хотя и ограниченно, эмоциональные (конечно, не на уровне человека) способности (Vilenskaya, 2020), такие как: распознавание эмоций, моделирование эмоций и эмпатия (хоть и условно).

При сочетании с робототехникой искусственному интеллекту также присущи моторные и физические способности (Germanov, 2016) к передвижению, координации. Такая их функция даже указана в определениях понятия «робот» в ISO/TS 15066:2016 и ГОСТ Р 60.1.2.3-2021.

К числу их свойств также можно отнести метакогнитивные способности (Voyushina, 2021) в виде самоанализа (анализировать и, при необходимости, корректировать свои действия) и предоставления объяснений своим решениям (действиям или выводам).

Одним из главных достоинств систем искусственного интеллекта является их способность к самостоятельному обучению (Helm et al., 2020; Bini, 2018), обеспечивающая приспособление системы к новым условиям и оптимизацию ее производительности как при непосредственном вмешательстве человека, так и без него. Именно на этом свойстве основана одна из подтехнологий искусственного интеллекта – машинное обучение. Ее предназначение сводится к созданию вычислительных программ или самообучающихся систем, которые обладают потенциалом наращивать свою функциональность из аккумулированного «опыта» (Gopal, 2019). Причем нарабатывается такой «опыт» по мере анализа данных, производимого специализированными алгоритмами (Azevedo, Rocha & Pereira, 2024). Эти алгоритмы в машинном обучении служат определению паттернов в массивах данных, путем применения частнонаучных методов в естественных науках: математике, статистике (Azevedo, Rocha & Pereira, 2024) и т.д.

К основным возможностям машинного обучения профессор Мадан Гопал справедливо относит регрессионный анализ (числовое прогнозирование), классификацию (распознавание образов), кластеризацию, оптимизацию и управление (Gopal, 2019).

В процессе машинного обучения при предиктивной аналитике система обычно последовательно проходит через следующие три основных этапа: предварительная (первичная) обработка данных (data pre-processing), обучение модели (model building) и развертывание с получением результатов (model serving) (El Mestari, Lenzini & Demirci, 2024; Pattyam, 2019).

На стадии первичной обработки очищаются и преобразовываются исходные данные с целью доведения их до состояния, пригодного к дальнейшему использованию (El Mestari, Lenzini, & Demirci 2024; Pattyam, 2019). При этом в зависимости от массива данных и решаемой задачи определяются конкретные подзадачи. На втором этапе происходит обучение модели, в ходе которого система учится на основе данных строить модель (гипотезу) (El Mestari, Lenzini & Demirci, 2024; Pattyam, 2019).

Обучение как таковое в рассматриваемой подтехнологии искусственного интеллекта (в машинном обучении) происходит в трех формах: контролируемое (наблюдаемое) обучение (supervised learning), неконтролируемое (ненаблюдаемое)

обучение (unsupervised learning) и обучение с подкреплением (reinforcement learning) (Azevedo, Rocha & Pereira, 2024; Barbierato & Gatti, 2024).

Как правило, в первой форме обучения система обрабатывает данные, содержащие правильный ответ на каждое задание, и проецирует их на новые задачи, которые она выполняет (Kayikci & Khoshgoftaar, 2024). А во втором случае система учится, работая с данными, в которых заранее не известен верный вариант ответа, и пытается самостоятельно разобраться в их структуре (Kayikci & Khoshgoftaar, 2024). Что касается последнего типа обучения, то здесь система, взаимодействуя с окружающей средой (виртуальным пространством) по принципу проб и ошибок, пытается получить своеобразное «вознаграждение» в виде набранных очков, где ими выступают правильные стратегии (решения) (Kayikci & Khoshgoftaar, 2024).

Главной целью машинного обучения во всех этих типах обучения считается формулирование гипотезы (предположения) или модели, с помощью которых можно обобщить знания по учебным данным и распространить их на новые неизвестные выборки данных (Azevedo, Rocha & Pereira, 2024). При этом, несомненно, как и отмечает профессор М. Гопал, оптимальная модель (либо гипотеза) должна обладать простотой и низким коэффициентом эмпирических ошибок в данных (Azevedo, Rocha & Pereira, 2024; Gopal, 2019). В зависимости от размера набора данных происходит выбор методов оценки. Обычно при работе с достаточно большими массивами данных принято разделять их на три независимых подмножества: обучающее множество (для разработки исходной модели), валидационное множество (для оптимизации модели и улучшения ее обобщающей способности) и тестовое множество (для расчета уровня ошибок итоговой модели) (Azevedo, Rocha & Pereira, 2024; Gopal, 2019). Перечисленные подмножества формируются автономно друг от друга, тем самым подтверждается особая важность использования достаточно большого набора данных.

В завершение, на стадии развертывания и вывода, обученная модель доводится до рабочего состояния и становится доступной пользователям или системам в виде готового продукта (сервиса) для ввода новых данных и получения прогнозов и выводов (El Mestari, Lenzini & Demirci, 2024).

Вышеизложенное дает основание предположить, что машинное обучение обладает весьма серьезными возможностями для проактивного выявления и предупреждения террористической деятельности посредством высокотехнологичного анализа данных (Westbrook & Maguire, 2024) и прогностического моделирования. Системы машинного обучения, использующие такие методики, как распознавание образов, классификация, кластеризация и оптимизация, способны обрабатывать обширные массивы данных для выявления поведенческих аномалий, которые могут сигнализировать о грядущих рисках. Такой структурированный подход к предварительной обработке данных, обучению моделей и их развертыванию для получения выводов в режиме реального времени позволит своевременно обнаружить потенциальные факторы риска и облегчит реализацию превентивных мер.

Раннее обнаружение и предупреждение террористического контента

1 июня 2017 г. в ряде стран ЕС начала реализовываться «Система раннего обнаружения и предупреждения террористического контента» («RED-Alert»[8]),

[8] Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing. Available at: https://cordis.europa.eu/project/id/740688 [Accessed 2nd January 2025].

включающая обработку естественного языка в режиме реального времени, анализ социальных связей и комплексную обработку событий. Разработчики при создании системы, способной обрабатывать огромные объемы данных, используя преимущественно метод пакетной нормализации (batch метод) (Yuan et al., 2019) и метод потоковой обработки (stream метод) (Marcu & Bouvry, 2024) для обработки данных в режиме реального времени, использовали такие возможности машинного обучения, как: обработка естественного языка, комплексная обработка событий, семантический анализ мультимедиа (распознавание речи, лиц, объектов, звуковых сигналов) и анализ социальных связей (Naqvi et al., 2019; Florea et al., 2022).

Модуль обработки естественного языка задействован в выполнении ряда базовых функций по анализу, интерпретации и систематизации смысловых значений текстов на разных языках. Сначала происходит определение языка и стиля речи, в ходе которого система идентифицирует язык, диалект или группу смешанных языков (в том числе макаронизмы) (Naqvi et al., 2019), (Florea et al., 2022), таких как спанглиш, рунглиш, франгле, и переводит слова в их исходную форму. Затем выполняется контекстуальное разграничение, где для выявления и уточнения смысла используются фрагментация, маркировка частей речи и статистические модели, обученные на наборах данных по конкретной тематике (Naqvi et al., 2019; Florea et al., 2022). Наконец, модуль обработки естественного языка осуществляет онтологическое сопоставление, связывая слова и фразы с уникальными, не зависящими от языка понятиями в конкретной предметной области, таким образом расшифровывая скрытые подтекстовые смыслы сообщения (Naqvi et al., 2019; Florea et al., 2022). В соответствии со спецификой такого комплексного процесса точное толкование смысла текста обеспечивается за счет преодоления различных культурных и контекстуальных барьеров (нюансов).

Следующий модуль – комплексной обработки событий – предназначен для постобработки данных, которые уже были предварительно обработаны другими модулями, такими как обработка естественного языка, анализ социальных сетей и др. Он позволяет принимать различные RAW-файлы (это формат файла, в котором сохраняются данные с матрицы камеры или смартфона при съемке, то есть формат файла цифрового изображения с необработанными данными) и динамические данные, однако в нем отсутствует механизм модификации файла для учета актуальных разведывательных данных (Naqvi et al., 2019; Florea et al., 2022). Учитывая ограничения секретности, правоохранительные органы не могут делиться разведывательными данными в процессе их разработки, в связи с чем в работе данного модуля приходится использовать симулированные входные данные и(или) типовые конфигурации.

Модуль комплексной обработки событий работает на основе алгоритмов сопоставления образцов для выявления тенденций, причинно-следственных связей и динамики данных. На основе полученных данных создаются структурированные оповещения в формате JSON (легковесный, человекочитаемый текстовый формат для обмена данными между сервером и веб-приложениями, основанный на парах «ключ-значение» и списках (массивах), что делает его простым для парсинга машинами и понятным для людей, являясь современным стандартом для API и передачи данных) для использования в аналитике и интеграции со сторонними правоохранительными системами (Naqvi et al., 2019; Florea et al., 2022). В распределенной системе, предназначенной для обработки потоков данных в реальном времени, осуществляется

управление вводом данных для обеспечения непрерывного стриминга данных в режиме реального времени и поддержки параллельных приложений этого модуля. Последние, в свою очередь, позволяют сравнивать различные типы распределений данных, шаблоны или промежуточные результаты для дальнейшей обработки.

Третий модуль, инструмент семантического анализа мультимедиа, призван содействовать расширенному использованию возможностей обработки мультимедийного контента. Распознавая речь, он разделяет аудиопотоки, определяет язык, переводит разговорную речь в текстовый формат и работает с десятью языками (среди которых английский, арабский, французский, немецкий, иврит, русский, испанский и др.) (Naqvi et al., 2019; Florea et al., 2022). Инструмент работает в автономном режиме, не завися от сторонних веб-интерфейсов, что существенно повышает его защищенность.

При распознавании лиц используется каскадный классификатор на основе признаков Хаара (Cucarella et al., 2024) (признаки цифрового изображения, используемые в распознавании образов), который ориентируется на разницу в интенсивности пикселей для обнаружения фронтальных и профильных лиц на изображениях. Для обнаружения объектов используется современная система глубокого обучения Faster R-CNN (алгоритм глубокого обучения для обнаружения объектов (object detection), который значительно ускорил и повысил точность моделей-предшественников (R-CNN, Fast R-CNN), заменив медленный поиск регионов (selective search) на обучаемую Сеть Предложения Регионов (RPN), генерирующую потенциальные области объектов прямо внутри нейросети, что делает его мощным инструментом для задач, где требуется высокая точность, например, в системах безопасности или автономном вождении).

Кроме того, функция распознавания звука использует рекуррентную конволюционную (сверточную) нейронную сеть (применяется для распознавания объектов и маркировки сцен) (Zhao, Jin & Hu, 2017) для классификации аудиособытий путем обучения распознаванию важных временных и спектральных изменений. Алгоритмы выделения верхних частот отфильтровывают шум и выделяют только важные частоты, такие как выстрелы, взрывы и т. д. (Naqvi et al., 2019; Florea et al., 2022). Эта интегрированная функциональность позволяет инструменту производить глубокий семантический разбор, на основе которого строится аналитика, необходимая правоохранительным органам и службам безопасности.

Наконец, модуль анализа социальных связей отслеживает взаимоотношения между динамическими формированиями, чтобы выявить релевантные группировки и структуры для проведения контртеррористических операций. Здесь предусмотрены три основные функции. Во-первых, он проверяет, как связи и их составные элементы, или узлы (например, (со)участники), трансформируются с течением времени, а затем отслеживает развитие отношений внутри групп и сообществ с помощью встроенных алгоритмов (Naqvi et al., 2019; Florea et al., 2022). Таким образом, можно наблюдать за ростом, спадом или реорганизацией сообществ, сравнивая изменения между отдельными фрагментами взаимодействия.

Во-вторых, используя накопленный в прошлом «опыт» (знания), этот модуль прогнозирует недостающие (или скрытые) связи с учетом сетевых паттернов и общих для этих узлов атрибутов (Naqvi et al., 2019; Florea et al., 2022). Наряду с этим он опирается на известные методики выявления потенциальных связей и обновления

существующих, предоставляя аналитикам возможность выбора, какие данные о связях объединить в контексте искомой информации.

В конечном итоге, выявляя закономерности в данных, можно восстановить скрытые иерархические структуры, такие как сетевые группировки террористических объединений (Naqvi et al., 2019; Florea et al., 2022). Для выявления таких организационных структур, которые могут быть неочевидны, используются усовершенствованные алгоритмы, поскольку модуль, хотя и основан на надежных математических моделях, все же зависит от изменчивости источников данных и предположений, а значит, его результаты должны быть подтверждены профильными специалистами. Только в этом случае выводы будут надежными и пригодными для применения при осуществлении мер правового и оперативного реагирования. Следует особо отметить, что все собираемые данные не являются доказательствами, они являются лишь материалами, с которыми могут работать правоохранительные органы в целях предупреждения преступлений, а в дальнейшем могут быть использованы специалистами и экспертами для формирования доказательственной базы.

Юридическая ответственность провайдеров интернет-услуг

В связи со сложившейся сложносоставной взаимосвязью между распространением информационно-коммуникационных технологий (ИКТ) и совершением тяжких (особо тяжких) преступлений, в первую очередь вовлечением лиц в террористическую деятельность с использованием современных средств связи, очевидна необходимость пересмотра механизмов возможной уголовной ответственности провайдеров интернет-услуг. Действующее законодательство Российской Федерации, в частности Федеральные законы № 126-ФЗ «О связи» от 07.07.2003 г.[9] и № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г.[10], регулирует функции и обязанности провайдеров интернет-услуг (операторов информационной системы) применительно к контенту, но, тем не менее, стремительное развитие цифровых угроз делает необходимым разработку более точного, проактивного и технологически обоснованного подхода к их предотвращению.

Существующие контртеррористические аналитические системы, такие как «Система раннего обнаружения и предупреждения террористического контента» (RED-Alert), уже в значительной степени способствуют выявлению отдельных участников и моделей прямой цифровой пропаганды терроризма. Однако задача состоит в том, чтобы справиться с малозаметными, но в совокупности опасными явлениями коллективного цифрового бездействия, когда совокупные действия множества ответственных субъектов (провайдеров интернет-услуг, операторов информационной системы), даже если по отдельности они не представляют опасности, объединяются в предсказуемый системный риск террористической деятельности. Смена парадигмы предполагает разработку новой правовой и технологической конструкции, которая согласует предиктивную аналитику с принципами материального уголовного права, особенно для субъектов, обладающих организационными и техническими возможностями для предотвращения таких назревающих угроз.

[9] Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

[10] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрании законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.

Провайдеры интернет-услуг выполняют целый ряд функций, за которые они должны нести юридическую ответственность в разной степени. Как отмечается в специализированных технических исследованиях, к ним относятся провайдеры доступа, хостинг-провайдеры, кэш-провайдеры, магистральные провайдеры и провайдеры «последней мили» (Rassolov, 2013; Perchatkina et al., 2012; Chubukova, 2017). Несмотря на то, что российское информационное законодательство возлагает на различных участников информационных (цифровых) правоотношений, включая владельцев сайтов и хостинг-провайдеров, обязанность отслеживать контент на предмет выявления очевидного противоправного материала и (или) информации (например, призывов к осуществлению террористической деятельности, массовых беспорядков, экстремистской деятельности, склонению несовершеннолетних к противоправным действиям) и ограничивать доступ при их обнаружении, четкое распределение уголовной ответственности за их бездействие до настоящего времени остается недостаточно проработанным.

В целях более результативного и целенаправленного предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий, предлагается интегрировать в «Систему раннего обнаружения и предупреждения террористического контента» (RED-Alert) таких инструментов, как модуль «Порогового адаптивного вмешательства» (или коротко «ПОРА») со встроенным алгоритмом машинного обучения. Данный модуль не ограничивается реактивной формой реагирования в форме «уведомления и удаления (блокировки)», а представляет собой проактивную, прогностическую функцию вмешательства, основанную на научно оцениваемом риске коллективного цифрового поведения, способного нанести серьезный вред общественным интересам (отношениям).

Операционное ядро модуля «ПОРА» состоит из сложного мультимодального механизма предиктивной аналитики, который использует и значительно расширяет существующие возможности систем типа «RED-Alert» по NLP, семантическому анализу мультимедиа и анализу социальных связей.

По идее, механизм машинного обучения в модуле «ПОРА» выражается в использовании передовых графовых нейронных сетей (GNN) и алгоритмов анализа временных рядов. Поскольку GNN особенно хорошо справляются с обработкой и изучением сложных взаимосвязей в информационных (цифровых) связях, появляется реальная возможность анализа коллективной деятельности. Анализ временных рядов позволяет модели отслеживать развитие этой динамики во времени, выявляя закономерности ее ускорения или замедления.

Система непрерывно отслеживает и обрабатывает огромные потоки анонимизированных и агрегированных цифровых данных из конкретных онлайн-пространств (например, контент хостинг-провайдера, база пользователей социальных сетей). В результате она рассчитывает коэффициент риска, т. е. динамически вычисляемую вероятность наступления того или иного события, террористической активности на основе коллективного цифрового поведения.

Коэффициент риска складывается не только из совокупности отдельных индикаторов опасности, но и определяет внешние свойства группы, например, формирование высоко сплоченных, но тайных ячеек, быстрое и синхронизированное распространение потенциально провокационного контента (даже если по отдельности его невозможно обнаружить) или массовое использование методов маскировки, свидетельствующих о согласованных усилиях по достижению преступных целей. На

исторических данных обучаются модели машинного обучения, соотносящие эти групповые цифровые сигналы с реальными последствиями, что позволяет модулю ПОРА прогнозировать будущий вред с измеримой статистической достоверностью.

В случае если показатель риска модуля ПОРА в конкретной информационной среде пересекает заранее установленную отметку, может быть сформировано надежное, криптографически верифицируемое предупреждение. Такое оповещение, содержащее указания на индикатор риска, соответствующую информацию, выявленную и связанные с ним аналитические данные (например, модели поведения участников), передается уполномоченному должностному лицу (например, модератору, хостинг-провайдеру или руководству платформы, либо напрямую правоохранительным органам).

При этом следует отметить, что так называемый «коэффициент риска» или «верифицируемое предупреждение» на основе систем искусственного интеллекта не приравнивается к определению вины в целом. Данные предиктивные метрики служат исключительно для целей раннего выявления и предупреждения потенциально опасных деяний. Установление обстоятельств, подтверждающих виновность лица в совершении преступления, форма его вины и мотивы субъекта преступления, как обязательный элемент субъективной стороны состава преступления, относится к исключительной компетенции органов предварительного расследования. В силу ст. 14 УПК РФ бремя доказывания обвинения и опровержения доводов, приводимых в защиту подозреваемого или обвиняемого, лежит на стороне обвинения[11]. Обвиняемый считается невиновным, пока его виновность в совершении преступления не будет доказана в порядке, предусмотренном Уголовно-процессуальным кодексом Российской Федерации и установлена вступившим в законную силу приговором суда.

Скорее, они являются вспомогательным инструментом для профилактики потенциальных преступлений или обработки оперативной обстановки (информации) при предотвращении преступлений. Также очевидно, что использование искусственного интеллекта в этих целях привело бы к объективному вменению, которое не поддерживается в настоящей работе. Нельзя не учитывать определенные риски нарушения прав человека, допуская, что решения ИИ могут быть необъективными из-за подачи искаженных обучающих данных, непрозрачными из-за известной проблемы «черного ящика».

Уголовная ответственность, согласно ст. 5 УК РФ, основывается на принципе вины, который исключает объективное вменение. Это означает, что для привлечения провайдера интернет-услуг, точнее ответственного за него (физического) лица к уголовной ответственности за неограничение доступа к противоправному контенту необходимо установить его субъективное психическое отношение к деянию: интеллектуальное (осознание противоправности и предвидение последствий) и волевое (желание или сознательное допущение этих последствий). Действующая модель регулирования обязанностей интернет-провайдеров (операторов информационных систем) в основном построена по принципу «уведомление о противоправном контенте соответствующими субъектами и его удаление, блокирование», когда обязанность действовать возникает после официального уведомления компетентных органов, что

[11] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрании законодательства Российской Федерации от 24 декабря 2001 г. № 52 (часть I) ст. 4921.

предполагает обязательный мониторинг (например, с помощью систем как RED-Alert) до уведомления.

Существует распространенное мнение о том, что провайдеры интернет-соединений, предоставляющие только технологическую инфраструктуру для связи пользователей, например, базовый доступ к сети или маршрутизацию данных без постоянного хранения, не должны подлежать уголовной ответственности (Perchatkina, 2012; Tsirina, 2012). Основанием для такого утверждения является позиция, согласно которой уголовная ответственность (в частности, за содействие террористической деятельности (ч. 3 ст. 205.1. УК РФ)) для провайдеров возникает только в том случае, если они обладают присущими им организационными и техническими рычагами для существенного влияния на информационное содержание или взаимодействие своих пользователей. Следовательно, интернет-провайдеры, деятельность которых ограничивается чисто техническим обеспечением, включая провайдеров доступа, кэш-провайдеров, магистральных провайдеров и провайдеров «последней мили», как правило, не подлежат уголовной ответственности (Perchatkina, 2012; Tsirina, 2012).

Однако к хостинг-провайдерам могут быть применены более сложные подходы, основанные на их специфических операционных функциях. Хостинг-провайдер, единственной функцией которого является предоставление дискового пространства для стабильного размещения информации в сети, как правило, не должно подлежат к уголовной ответственности. В случаях, когда соответствующие уполномоченные органы официально уведомляют о незаконном характере размещенного контента, ситуация меняется принципиальным образом (Perchatkina, 2012; Tsirina, 2012).

Вопрос о форме вины (умысел или неосторожность) физического лица, связанного с бездействием провайдера, которое может повлечь уголовную ответственность, является дискуссионным и требует отдельного, углубленного исследования с учетом правилами квалификации преступлений, предусмотренных Уголовным кодексом Российской Федерации, что выходит за рамки целей настоящей работы. Тем не менее, следует особо подчеркнуть, что юридическая ответственность интернет-провайдера за преступное бездействие – в частности, за неограничение доступа к информации, подстрекающей или вовлекающей людей в террористическую деятельность, – является строго условной. Такая ответственность должна наступать только в том случае, если провайдер осознает общественную опасность, связанную с неограниченным доступом к такому контенту, предвидит опасные последствия (например, террористические акты и др.) и сознательно направляет свои умственные и физические усилия на то, чтобы допустить совершение такого общественно опасного деяния.

В рамках же предупредительной деятельности, провайдер интернет-услуг должен рассматриваться как ключевой субъект, обязанный участвовать в предупреждении преступлений террористической направленности, используя доступный технический потенциал.

Заключение

В данном исследовании обосновывается необходимость интеграции передовых технологий искусственного интеллекта (машинного обучения) и предиктивной аналитики в современные подходы по противодействию терроризму. Стремительно развивающаяся цифровая среда, активно используемая преступными элементами,

диктует необходимость принятия упреждающих и технологически продвинутых мер, которые не будут ограничиваться традиционными реагирующими подходами.

Исследование подтверждает эффективность комплексных аналитических возможностей на основе искусственного интеллекта в выявлении, пресечении и предотвращении использования цифровых технологий в террористической деятельности, одновременно подчеркивая их важную роль в построении достоверных баз цифровых доказательств. Это знаменует собой фундаментальный сдвиг парадигмы, усиливая способность правоохранительных органов ориентироваться и контролировать сложные информационные потоки, используемые преступными группами.

Следует особо акцентировать внимание на том, что информация, обобщаемая (генерируемая) средствами машинного обучения и предиктивной аналитики, обладает исключительно предварительным и вспомогательным характером. Получаемые данные не могут быть приравнены к доказательствам, а являются лишь оперативными материалами, которые требуют обязательной верификации и всесторонней оценки со стороны компетентных должностных лиц правоохранительных органов. При этом использование данных предиктивных индикаторов напрямую не предопределяет юридическую возможность и не создает оснований для автоматического принятия решения о привлечении какого-либо лица к уголовной ответственности, поскольку факт совершения преступления и наличие вины устанавливаются исключительно в порядке и по процедурам, предусмотренным Уголовно-процессуальным кодексом Российской Федерации.

Важно понимать, что преобразующий потенциал этих технологий неразрывно связан с тщательным созданием и строгим соблюдением надежных правовых гарантий. Первоочередная задача очевидна – укрепление национальной безопасности с использованием возможностей искусственного интеллекта должно сопровождаться защитой основных прав человека и строгим соблюдением установленных правовых принципов, включая презумпцию невиновности. Надлежащим образом реализовать эти возможности и обеспечить их ответственное использование можно только при условии, что они будут сопровождаться соответствующими правовыми гарантиями, в частности, правом на защиту от незаконного и произвольного лишения свободы, правом на справедливое судебное разбирательство и правом на защиту от пыток и жестокого обращения.

References / Список литературы

Aisner, L.Y. & Naumov, O.D. (2021) Human cognitive abilities: Categorial analysis. In: Krasnoyarsk State Agrarian University. *Ensuring the rights of participants in criminal proceedings with disabilities: A compensatory approach. The Proceedings of the International Scientific and Practical Conference (18-19 June 2021, Krasnoyarsk). Part 2.* Krasnoyarsk, Editorial and Publishing Centre of Krasnoyarsk State Agrarian University Publ., pp. 212–217. (In Russian). EDN: YDNNTG.

Айснер Л.Ю., Наумов О.Д. Когнитивные способности человека: категориальный анализ // Обеспечение прав участников уголовного судопроизводства с ограниченными возможностями: компенсаторный подход : материалы Международной научно-практической конференции (18–19 июня 2021 года, г. Красноярск). Часть 2. Красноярск : Редакционно-издательский центр Красноярского государственного аграрного университета, 2021. С. 212–217.

Aneja, P., Sharma, P., Sood, K., Solanki, K., Choudhary, S. K. & Mathur, S. (2024) Artificial Intelligence in Multimedia Forensics. In: Saini, K., Sonone, S.S., Sankhla, M.S., Kumar, N. (eds.) *Artificial Intelligence in Forensic Science*. Boca Raton, CRC Press, pp. 43–64.

Arjoune, Y., Nguyen, T.N., Doroshow, R.W., & Shekhar, R. (2023) Technical characterisation of digital stethoscopes: towards scalable artificial intelligence-based auscultation. *Journal of medical engineering & technology*. 47 (3), 165–178. https://doi.org/10.1080/03091902.2023.2174198

Avanesyan, G.G. (2024) Prospects for effective interaction of artificial intelligence and human personality. *World of Science. Pedagogy and Psychology*. 12 (3). 77PSMN324. (In Russian). EDN: ZGYZDA.
Аванесян Г.Г. Перспективы эффективного взаимодействия искусственного интеллекта и личности человека // Мир науки. Педагогика и психология. 2024. Т. 12. № 3. EDN: ZGYZDA.

Azevedo, B.F., Rocha, A.M.A. & Pereira, A.I. (2024) Hybrid approaches to optimization and machine learning methods: A systematic literature review. *Machine Learning*. 113, 4055–4097. https://doi.org/10.1007/s10994-023-06467-x

Barbierato, E., & Gatti, A. (2024) The challenges of machine learning: A critical review. *Electronics*. 13 (2), 416. https://doi.org/10.3390/electronics13020416

Bini, S.A. (2018) Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: What Do These Terms Mean and How Will They Impact Health Care? *The Journal of Arthroplasty*. 33 (8), 2358–2361. https://doi.org/10.1016/j.arth.2018.02.067

Chubukova, S.G. (2017) The legal nature issues of the information intermediary. *Bulletin of the Academy of Law and Management*. (2 (47)), 39–44. (In Russian). EDN: YUGWOX.
Чубукова С.Г. Проблемы правового статуса информационного посредника // Вестник академии права и управления. 2017. № 2 (47). С. 39–44. EDN: YUGWOX.

El Mestari, S.Z., Lenzini, G. & Demirci, H. (2024) Preserving data privacy in machine learning systems. *Computers & Security*. 137, 103605. https://doi.org/10.1016/j.cose.2023.103605.

Falikman, M. (2014) Cognitive Science: Fundamentals and Prospects. *Philosophical and Literary Journal Logos*. (1 (97)), 1–18. (In Russian). EDN: QEZZJC.
Фаликман М. Когнитивная наука: основоположения и перспективы // Философско-литературный журнал «Логос». 2014. № 1 (97). С. 1–18. EDN: QEZZJC.

Farina, M. et al. (2024) Machine learning in human creativity: Status and perspectives. *AI & Society*. 39, 3017–3029. https://doi.org/10.1007/s00146-023-01836-5

Filipova, I.A. (2024) Intelligent Robots, Cyborgs, Genetically Enhanced Individuals, Chimeras: The Future and the Challenges of Law. *Journal of Digital Technologies and Law*. 2 (4), 741–781. https://doi.org/10.21202/jdtl.2024.38 EDN: ATQZBA

Florea, M. et al. (2022) Complex project to develop real tools for identifying and countering terrorism: Real-time early detection and alert system for online terrorist content based on natural language processing, social network analysis, artificial intelligence and complex event processing. In Bernabe, J.B. & Skarmeta A. (eds.) *Challenges in cybersecurity and privacy-the European research landscape* (1st ed.). New York, River Publishers, 181–206.

Germanov, G.N. (2016) Physical qualities or motive abilities? Endurance as qualitative feature of motive function of the person: Scientific-theoretical analysis. *MCU Journal of Natural Sciences*. (3 (23)), 71–80. (In Russian). EDN: WLSIUF.
Германов Г.Н. Физические качества или двигательные способности? Выносливость как качественная особенность двигательной функции человека: научно-теоретический анализ // Вестник Московского городского педагогического университета. Серия: Естественные науки. 2016. № 3 (23). С. 71–80. EDN: WLSIUF.

Gopal, M. (2019) Machine learning and data mining. In: Gopal, M. (eds.) *Applied Machine Learning.* (1st ed.). New York, McGraw-Hill Education Publ., pp. 25–26.

Helm, J.M. et al. (2020) Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. *Current Reviews in Musculoskeletal Medicine.* 13, 69–76. https://doi.org/10.1007/s12178-020-09600-8

Huang, Z.Y., Chiang, C.C., Chen, J.H., Chen, Y.C., Chung, H.L., Cai, Y.P. & Hsu, H.C. (2023) A study on computer vision for facial emotion recognition. *Scientific reports*, 13 (1), 69–76. https://doi.org/10.1038/s41598-023-35446-4

Kayikci, S. & Khoshgoftaar, T.M. (2024) Blockchain meets machine learning: A survey. *Journal of Big Data*. 11 (1), 9. https://doi.org/10.1186/s40537-023-00852-y

Lomtatidze, O.V. (2022) *Physiology of Sensory Systems.* Yekaterinburg, Ural University Press, pp. 5–6. (In Russian). EDN: CSRAFP.

Ломтатидзе О.В. Физиология сенсорных систем: учебно-методическое пособие / под общ. ред. О.В. Ломтатидзе; Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. Екатеринбург : Изд. Уральского ун-тета, 2022. 120 с. EDN: CSRAFP.

Marcu, O.C., & Bouvry, P. (2024) Big data stream processing. *HAL Open science.* hal-04687320.

Minopoulos, G.M., Memos, V.A., Stergiou, K.D., Stergiou, C.L. & Psannis, K.E. (2023) A medical image visualization technique assisted with AI-based haptic feedback for robotic surgery and healthcare. *Applied Sciences.* 13 (6), 3592. https://doi.org/10.3390/app13063592

Mishchenko, I.I., Misnik, A.E. & Alexandrov, A.V. (2024) Application of computer vision and image preprocessing technologies in decision support systems. *Vestnik of Samara State Technical University. Technical Sciences Series*. 32 (4 (84)), 6–26. (In Russian). https://doi.org/10.14498/tech.2024.4.1 EDN: UCBKUO.

Мищенко И.И., Мисник А.Е., Александров А.В. Применение технологий компьютерного зрения и предварительной обработки изображений в системах поддержки принятия решений // Вестник Самарского государственного технического университета. Серия «Технические науки». 2024. Т. 32. № 4 (84). С. 6–26. https://doi.org/10.14498/tech.2024.4.1 EDN: UCBKUO.

Naqvi, S. et al. (2019) Towards fully integrated real-time detection framework for online contents analysis-RED-alert approach. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* 257–263 https://doi.org/10.1109/EuroSPW.2019.00035

Pattyam, S.P. (2019) Advanced AI Algorithms for Predictive Analytics: Techniques and Applications in Real-Time Data Processing and Decision Making. *Distributed Learning and Broad Applications in Scientific Research*. 5, 359–384. Available at: https://dlabi.org/index.php/journal/article/view/115 [Accessed 02nd January 2025].

Perchatkina, S.A. et al. (2012) Social Internet Networks: Legal Aspects. *Journal of Russian Law*. (5 (185)), 14–24. (In Russian). EDN: OWQAVL.

Перчаткина С.А. и др. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5 (185). С. 14–24. EDN: OWQAVL.

Ponkin, I., Kupriyanovsky, V., Moreva, S. & Lapteva, A. (2024) Computer vision: Concept, functional-purpose, structure, related regulatory developments. *International Journal of Open Information Technologies*. 12 (5), 57–66. (In Russian). EDN: WDFAPU.

Понкин И.В. и др. Компьютерное зрение: концепт, функционально-целевое назначение, структура, регуляторика // International Journal of Open Information Technologies. 2024. Т. 12. № 5. С. 57–66. EDN: WDFAPU.

Quiles-Cucarella, E. et al. (2024) Multi-Index Driver Drowsiness Detection Method Based on Driver's Facial Recognition Using Haar Features and Histograms of Oriented Gradients. *Sensors*. 24 (17), 5683. https://doi.org/10.3390/s24175683

Rassolov, I.M. (2013) Legal issues in ensuring information security: Legal responsibility of telecommunications operators. *Bulletin of Moscow University of the Ministry of Internal Affairs of Russia*. (12), 103–108. (In Russian). EDN: RSCSAT.

Рассолов И.М. Правовые проблемы обеспечения информационной безопасности: юридическая ответственность операторов связи // Вестник Московского университета МВД России. 2013. № 12. С. 103–108. EDN: RSCSAT.

Rodriguez, M. (2025) Audio & Speech Perception: Speech recognition, auditory scene analysis, and multimodal audio-visual integration. *Journal of Perception and Control*. 1 (1), 11–19.

Strielkowski, W. et al. (2023) Prospects and challenges of the machine learning and data-driven methods for the predictive analysis of power systems: A review. *Energies*. 16 (10), 4025. https://doi.org/10.3390/en16104025

Strielkowski, W., Vlasov, A., Selivanov, K., Muraviev, K. & Shakhnov, V. (2023) Prospects and challenges of the machine learning and data-driven methods for the predictive analysis of power systems: A review. *Energies*. 16 (10), 4025. https://doi.org/10.3390/en16104025

Taheri, H. & Salimi, B.A. (2025) Artificial Intelligence, Machine Learning, and Smart Technologies for Nondestructive Evaluation. In: Meyendorf, N., Ida, N., Singh, R., Vrana, J. (eds) *Handbook of Nondestructive Evaluation 4.0.* Cham, Springer Publ. https://doi.org/10.1007/978-3-031-84477-5_70

Tsirina, M.A. (2012) Dissemination of pro-drug information on the Internet: Countermeasures. *Journal of Russian Law*. (4 (184)), 44–50. (In Russian). EDN: OWQBXX.

Цирина М.А. Распространение пронаркотической информации в Интернете: меры противодействия // Журнал российского права. 2012. № 4 (184). С. 44–50. EDN: OWQBXX.

Vilenskaya, G. (2020) Emotional regulation: Factors of development and forms of manifestation in behavior. *Psychological Journal.* 41 (5), 63–76. (In Russian). EDN: DBYTED.

Виленская Г.А. Эмоциональная регуляция: факторы ее развития и связанные с ней виды поведения // Психологический журнал. 2020. Т. 41. № 5. С. 63–76. EDN: DBYTED.

Voyushina, E.A. (2021) Approaches to defining the concept of "metacognitive abilities." The structure of metacognitive abilities. *Innovations. Science. Education*. (41), 758–762. (In Russian). EDN: JCKXYJ.

Воюшина Е.А. Подходы к определению Понятия «метакогнитивные способности». Структура метакогнитивных способностей // Инновации. Наука. Образование. 2021. № 41. С. 758–762. EDN: JCKXYJ.

Westbrook, D.A. & Maguire, M. (2024) Machine Learning and Artificial Intelligence in Counterterrorism: The "Realities" of Security Practitioners and Technologists. In Avis, M., Marciniak D. & Sapignoli, M. (eds.) *States of Surveillance: Ethnographies of New Technologies in Policing and Justice*. New York, Routledge Publ., pp. 164–176.

Yuan, X., Feng, Z., Norton, M. & Li, X. (2019) Generalized batch normalization: Towards accelerating deep neural networks. *Proceedings of the AAAI Conference on Artificial Intelligence.* 33 (01), 1682–1689. https://doi.org/10.1609/aaai.v33i01.33011682

Zhang, Z., Wen, F., Sun, Z., Guo, X., He, T. & Lee, C. (2022) Artificial intelligence-enabled sensing technologies in the 5G/internet of things era: From virtual reality/augmented reality to the digital twin. *Advanced Intelligent Systems.* 4 (7), 2100228.

Zhao, Y., Jin, X. & Hu, X. (2017) Recurrent convolutional neural network for speech processing. *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 5300–5304. https://doi.org/10.1109/ICASSP.2017.7953168

Zhou, A., Men, L. R. & Tsai, W. H. S. (2023) The power of AI-enabled chatbots as an organizational social listening tool. In: Place, K. R. (eds.) *Organizational Listening for Strategic Communication*. (1st ed.). New York, Routledge Publ., pp. 181–206.

Сведения об авторах:

Маджумаев Мурад Мамедович **–** кандидат юридических наук, ведущий научный сотрудник, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики, юридический институт, Российский университет дружбы народов; Российская Федерация, 117198, г. Москва, ул. Миклухо-Маклая, д. 6

ORCID: 0000-0003-3332-2850; SPIN-код: 2278-5843

e-mail: murad.mad@outlook.com

Кузнецова Ольга Алексеевна – доктор юридических наук, доцент, главный научный сотрудник, заведующий кафедрой уголовного права, уголовного процесса и криминалистики, юридический институт, Российский университет дружбы народов; Российская Федерация, 117198, г. Москва, ул. Миклухо-Маклая, д. 6

ORCID: 0000-0003-1066-3783; SPIN-код: 8755-2997

e-mail: kuznetsova-ola@rudn.ru

About the authors:

Murad M. Madzhumayev – Candidate of Legal Sciences, Leading Researcher, Senior Lecturer at the Department of Criminal Law, Criminal Procedure, and Criminalistics, Law Institute, RUDN University; Russian Federation, 117198, Moscow, 6 Miklukho-Maklaya St.

ORCID: 0000-0003-3332-2850; SPIN-code: 2278-5843

e-mail: murad.mad@outlook.com

Olga A. Kuznetsova – Doctor of Legal Sciences, Full Professor, Chief Researcher, Head of the Department of Criminal Law, Criminal Procedure and Criminalistics, Law Institute, RUDN University; Russian Federation, 117198, Moscow, 6 Miklukho-Maklaya St.

ORCID: 0000-0003-1066-3783; SPIN-code: 8755-2997

e-mail: kuznetsova-ola@rudn.ru