ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ЗРЕНИЯ В БОРЬБЕ С АНТИТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТЬЮ

Саенко И. Б.[1]

DOI:10.21681/3034-4050-2025-4-2-9

Ключевые слова: *терроризм; машинное обучение; глубокое обучение; обработка изображений; распознавание лиц; обнаружение аномалий; предиктивная аналитика; социальные сети.*

Аннотация

Цель: *анализ содержания и возможностей применения технологий искусственного интеллекта и машинного зрения, которые могут быть применены в антитеррористической деятельности, и формулировка проблем, свойственных этой предметной области, с обоснованием направлений их решения.*

Метод: *системный анализ антитеррористической деятельности и технологий искусственного интеллекта, направленный на выявление проблемной ситуации в новой предметной области.*

Результат: *обосновывается необходимость применения технологии искусственного интеллекта и машинного зрения для повышения эффективности антитеррористической деятельности. Дается характеристика ключевых технологий искусственного интеллекта и машинного зрения, оказывающих существенное воздействие на защиту от терроризма, таких как обработка изображений, распознавание лиц, обнаружение аномалий, предиктивная аналитика и мониторинг социальных сетей. Обсуждаются новые проблемы, порождаемые использованием искусственного интеллекта и машинного зрения, связанные с подготовкой обучающих наборов данных и этичностью применения инструментария искусственного интеллекта.*

Научная новизна: *анализ работ по тематике применения технологий искусственного интеллекта и машинного зрения в области борьбы с терроризмом впервые показал, что в наибольшей степени здесь могут быть применимы технологии обработки изображений и распознавание лиц, обнаружения аномалий, предиктивная аналитика и мониторинг социальных сетей. Применение этих технологий в интересах антитеррористической деятельности приводит к возникновению новых проблем, требующих своего скорейшего решения, которые обусловлены необходимостью качественной подготовки обучающих наборов данных и разработки новых нравственных и юридических норм, касающихся применения инструментария искусственного интеллекта.*

Введение

В настоящее время террористическая деятельность стала одной из основных угроз национальной и общественной безопасности, с которой сталкиваются все страны мира, включая Российскую Федерацию. Характерным примером является теракт, совершенный мигрантами в Москве в «Крокус Сити Холле» 22 мая 2024 года, унесший жизни более 60 человек. К числу последних резонансных террористических событий также следует отнести теракты, в которых погибли одни из высших руководителей нашего военного ведомства – генерал-лейтенант Кириллов И. А. в декабре 2024 года и генерал-лейтенант Москалик Я. Я. в апреле 2025 года. Причем последние два теракта были организованы практически по одной и той же схеме.

Одной из причин, затрудняющей антитеррористическую деятельность и предотвращение терактов, является необходимость обеспечения демократических свобод гражданского населения страны. Противоречие между усилением антитеррористической деятельности, направленной на защиту граждан от внутренних угроз безопасности, и соблюдением прав и свобод личности, которые составляют основу демократического общества, требует своего скорейшего разрешения. Существует

1 Саенко Игорь Борисович, доктор технических наук, профессор, профессор кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Будённого, Санкт-Петербург, Россия. E-mail: ibsaen@mail.ru

настоятельная потребность в овладении стратегиями, которые не только смягчают угрозу терроризма, но и защищают основные права и свободы, характерные для открытого демократического общества [1, 2]. Одно из возможных, но достаточно эффективных направлений разрешения этого противоречия видится в применении технологии искусственного интеллекта (ИИ) и машинного зрения в интересах антитеррористической деятельности [3, 4].

ИИ получил значительное внимание и достаточно широкое распространение во всем мире как инструмент, который может обрабатывать в реальном или сопоставимом с реальным масштабе времени огромные объемы данных и обнаруживать закономерности и корреляции в данных, невидимые человеческому глазу, что может повысить эффективность и результативность анализа сложной информации [5]. Однако, несмотря на высокие уровень интеграции ИИ в общество и частоту популярного использования этого термина, универсального определения ИИ не существует. Этот термин обычно понимается для описания дисциплины, связанной с разработкой технологических инструментов, использующих такие человеческие качества, как планирование, обучение, рассуждение и анализ [6]. Наиболее популярными в настоящее время разделами этой научной дисциплины являются методы машинного, в том числе глубокого, обучения. В большинстве случаев применение этих методов ассоциируется с искусственными нейронными сетями. Однако и другие области, такие как обработка нечётких данных (нечётких алгоритмов, нечётких моделей, нейро-нечётких сетей и т.д.) [7] или применение биоинспирированных подходов (эволюционных алгоритмов, методов роевого интеллекта и т.д.) [8], также имеют важное значение.

Под машинным зрением понимается применение компьютерного зрения для промышленности и производства. При этом компьютерное зрение представляет собой общий набор методов, позволяющих компьютерам видеть, в то время как предметной областью машинного зрения, как инженерного направления, являются цифровые устройства ввода-вывода и компьютерные сети, предназначенные для контроля производственного оборудования, такие, например, как роботы-манипуляторы [9]. Таким образом, машинное зрение является подразделом инженерии, связанным с вычислительной техникой, оптикой, машиностроением и промышленной автоматизацией. При этом в последнее время машинное зрение, как и компьютерное зрение в целом, тесно связывается с решением задач распознавания изображений с применением нейронных сетей [10]. Поэтому вполне правомерно считать машинное зрение одним из направлений ИИ [11], которое также имеет особую важность для совершенствования антитеррористической деятельности.

Целью настоящей статьи является рассмотрение возможностей и проблем применения ИИ, включая машинное зрение, в интересах антитеррористической деятельности.

Возможности применения ИИ в интересах антитеррористической деятельности

ИИ привлекает всеобщее внимание способностью обрабатывать большие наборы данных, выявляя при этом скрытые закономерности и идеи, которые зачастую остаются недоступными для человеческого анализа. Эта способность значительно повышает эффективность и результативность анализа сложной информации. Преимущества ИИ, как многогранной технологии, распространяются на многочисленные области, включая борьбу с терроризмом. В этой сфере возможности ИИ являются бесценными и проявляются в быстрой расшифровке и интерпретации сложных данных, что позволяет считать ИИ кладезем инновационных методов обнаружения потенциальных угроз и формулирования эффективных превентивных стратегий. Использование ИИ в борьбе с терроризмом не только демонстрирует его существенный потенциал в организации безопасности и обороны, но и подчеркивает его преобразующее влияние на различные секторы, подчеркивая его важную роль в современных аналитических методологиях.

Прежде всего, крайне важно признать глубокую зависимость технологии ИИ от данных. Без точных и надежных данных для обучения моделей ИИ, особенно в борьбе с терроризмом, существует значительный риск не в полной мере использовать эту новаторскую технологию для решения самых насущных проблем антитеррористической деятельности. По сути, ИИ работает,

тщательно изучая большие наборы данных для выявления закономерностей и составления прогнозов. Учитывая уникальные возможности систем ИИ, задача заключается в навигации по этим огромным резервам данных для извлечения действенных идей. В нынешнюю эпоху, переполненную данными — от взаимодействий в социальных сетях и финансовых транзакций до видеозаписей видеонаблюдения в общественных местах – постоянно собирается огромный объем данных. Этот взрыв «больших данных» представляет собой палку о двух концах: с одной стороны, есть возможность, а с другой – существует проблема их эффективного использования. Поэтому в качестве ключевых технологий ИИ, которые могут быть достаточно эффективно использоваться в антитеррористической деятельности, следует выделить следующие:

- обработка изображений и распознавание лиц;
- обнаружение аномалий;
- предиктивная аналитика;
- мониторинг социальных сетей.

Эти технологии ИИ являются важными инструментами для укрепления мер, а также идентификации и предотвращения потенциальных угроз безопасности. Рассмотрим эти технологии подробнее.

Технология **обработки изображений и распознавания лиц** может значительно повысить меры безопасности, выявляя известных или предполагаемых террористов в режиме реального времени в различных условиях и локациях, таких как аэропорты, вокзалы и публичные мероприятия. По сути, эта технология, используя средства машинного зрения, сканирует лица в толпе, чтобы сопоставить их с базами данных известных лиц. Кроме того, последние разработки в технологической отрасли сделали обычным явлением использование камер на базе ИИ, способных обнаруживать даже оружие.

Используя существующие сети средств машинного зрения в таких масштабных средах, как школы, аэропорты или корпоративные кампусы, алгоритмы могут обнаруживать огнестрельное оружие или дробовики. Сначала система помечает огнестрельное оружие оранжевым цветом как подозрительное, а затем в течение нескольких секунд быстро переходит на красный уровень тревоги [12]. Сотрудник службы безопасности получает уведомление на свой мобильный телефон; впоследствии программное обеспечение предоставляет неподвижное изображение, на котором подробно описано огнестрельное оружие и идентифицируется подозреваемый. Это облегчает процесс принятия решения о том, следует ли задействовать службы быстрого реагирования или отклонить оповещение как ложную тревогу. Например, ИИ может различать пистолет и головку разбрызгивателя. Тем не менее, как упоминалось выше, эта технология в значительной степени опирается на огромные объемы данных, которые необходимо уточнить. Поскольку она продолжает собирать видеоданные и совершенствовать алгоритмы и модели для лучшего распознавания объектов, можно ожидать, что с течением времени точность будет неуклонно повышаться. Однако внедрение технологии обработки изображений и распознавания лиц вызывает опасения относительно конфиденциальности, потенциальной предвзятости и точности идентификации лиц в разных демографических группах.

Технология **обнаружения аномалий** на базе ИИ играет ключевую роль в борьбе с терроризмом, потому что она позволяет выявлять отклонения от обычных моделей и поведения. Системы обнаружения аномалий отлично раскрывают подозрительную деятельность в финансовых транзакциях, схемах поездок и онлайн-коммуникациях, выступая в качестве упреждающих инструментов для раннего обнаружения потенциальных угроз. Их эффективность в упреждающем выявлении угроз помогает предотвращать атаки до их возникновения, уделяя особое внимание сокращению ложных срабатываний и сохранению конфиденциальности.

Особенно важно обнаружение аномалий с помощью ИИ в сфере отчетов о подозрительной деятельности (ОПД) [13]. ОПД, необходимые для обнаружения и противодействия финансовым преступлениям, таким как отмывание денег и финансирование терроризма, традиционно сложны из-за необходимости фильтрации огромных объемов транзакционных данных. ИИ упрощает этот процесс, объединяя скорость, точность и эффективность, чтобы финансовые учреждения могли более эффективно выявлять аномалии. При этом возможно использование предварительно сформированных наборов данных о террористической деятельности, например, Global

Terrorism Database (GTD) [14]. Используя передовое машинное обучение и распознавание образов, ИИ улучшает процесс формирования ОПД, предоставляя возможности мониторинга в реальном времени, которые значительно уменьшают возможность того, что финансовые преступления останутся незамеченными. Тем не менее, включение ИИ в соответствие с требованиями ОПД создает проблемы, включая этические соображения и конфиденциальность данных, а также необходимость идти в ногу с меняющимися правилами. Несмотря на эти препятствия, сохраняется критическая роль человеческого суждения, особенно для оценки сложных или неопределенных ситуаций, выявленных ИИ.

Технология **прогнозной аналитики** использует исторические данные и алгоритмы ИИ для прогнозирования будущих событий, включая потенциальные террористические угрозы [15]. Анализируя огромные объемы данных, включая сообщения, транзакции и перемещения, прогнозные модели могут подсказать, когда и где может произойти террористический акт. Хотя этические соображения относительно наблюдения и риска профилирования многообещающие, они требуют тщательного управления. Кроме того, надежность прогнозов и потенциальная возможность чрезмерной зависимости от автоматизированных систем являются критическими проблемами.

Внедрение такой технологии сталкивается с трудностями, особенно из-за ограничений данных. Террористические атаки с различными мотивами и методами создают уникальные цифровые следы, на которые влияют такие факторы, как убеждения или психическое здоровье, количество участников и режимы связи (возможно, зашифрованные). Выявление закономерностей в пределах одного набора данных затруднено, но улучшается с помощью анализа кросс-наборов данных, который требует детального изучения и увеличивает размерность набора данных. Алгоритмы машинного обучения для массового наблюдения должны обучаться на различных наборах данных, чтобы эффективно обнаруживать закономерности. Это вводит «проклятие размерности» в больших данных, где более сложные наборы данных препятствуют статистическому анализу, снижая точность и производительность алгоритма. Более подробная информация о каждом подозреваемом повышает точность, но требует больших наборов данных, что делает скудные задокументированные террористические атаки недостаточными для тщательного обучения.

С другой стороны, глубокие нейронные сети, такие как известные своей точностью сверточные [16] и рекуррентные [17], значительно усиливают структуру предиктивной аналитики. Превосходно справляясь с распознаванием сложных образов в больших наборах данных, эти типы нейронных сетей хорошо подходят для задач прогнозирования, так как они способны моделировать сложные многомерные данные, не снижая точность прогноза. Благодаря обширному обучению на исторических и текущих данных эти сети достигают более высокой точности прогнозирования, чем многие статистические методы. Их многослойная обработка обеспечивает понимание данных, необходимое для точного прогнозирования результатов в различных контекстах. Глубокие сети также совершенствуют процесс принятия решений, предлагая механизмы визуализации и оценки, тем самым обеспечивая более точные и обоснованные решения. Эти сети могут смягчить некоторые проблемы, вызванные проклятием размерности, путем постепенного уменьшения размерности данных. Это делает их ценным инструментом в предиктивной аналитике и других областях, требующих сложного анализа наборов данных.

Технология **мониторинга социальных сетей** вызывает в последние годы значительный интерес в связи с тем, что объемы данных, связанных с поведением людей в Интернете, особенно на платформах социальных сетей, претерпевает значительное увеличение [18]. Исследователи и службы безопасности усердно изучают использование данных социальных сетей для прогнозирования террористической деятельности. Это исследование основано на убеждении, что закономерности использования и взаимодействия в социальных сетях могут раскрыть важную информацию о намерениях, связях и потенциальных планах человека, что делает их критически важным активом для упреждающего устранения угроз. Действительно верно, что террористические группы часто используют

социальные сети для пропаганды, вербовки и общения. Использование ИИ для мониторинга этих платформ помогает выявлять и пресекать такую деятельность. Технологии ИИ, такие как большие языковые модели [19], искусно анализируют текст, изображения и видео на предмет экстремистского контента, помечая их для последующего просмотра человеком. Эффективность этих инструментов ИИ зависит от их способности понимать контекст и нюансы, тем самым снижая вероятность ошибочной цензуры законного контента при точном выявлении подлинных угроз.

Проблемы применения ИИ в интересах антитеррористической деятельности

В 2017 году в ходе Всероссийского открытого урока Президент России В. В. Путин сделал историческое заявление, заявив следующее: «Искусственный интеллект – это будущее не только России, это будущее всего человечества. Здесь колоссальные возможности и трудно прогнозируемые сегодня угрозы. Тот, кто станет лидером в этой сфере, будет властелином мира. И очень бы не хотелось, чтобы эта монополия была сосредоточена в чьих-то конкретных руках». Это заявление привлекло к ИИ широкое внимание как международной общественности, так и передовых технологических лабораторий. Теперь важно понимать значение и причины потенциального влияния ИИ на национальную безопасность, являются ли его эффекты революционными или просто постепенными.

Эффективность ИИ в значительной степени зависит от качества входных данных, что подчеркивает настоятельную потребность в целостной стратегии обработки данных, которая легко интегрирует ИИ в существующие технологические структуры. Кроме того, эффективность ИИ в обработке данных определяется не только объемом данных, но и их репрезентативностью и отсутствием предвзятости, что имеет решающее значение для точной интерпретации сложного поведения человека.

ИИ играет ключевую роль в усилении усилий по борьбе с терроризмом за счет эффективной обработки и анализа больших наборов данных. Он поддерживает выявление закономерностей и связей в данных, связанных с терроризмом, таких как отчеты об инцидентах и контртеррористические мероприятия, тем самым помогая прогнозировать и предотвращать террористические угрозы.

Использование технологий машинного обучения, таких как обработка изображений, распознавание лиц, обнаружение аномалий, предиктивная аналитика и мониторинг социальных сетей, имеет жизненно важное значение для продвижения мер по борьбе с терроризмом. Эти технологии используют данные уникальным образом; например, обработка изображений и распознавание лиц помогают идентифицировать людей по визуальным данным, в то время как обнаружение аномалий выявляет необычные закономерности, которые могут сигнализировать об угрозах безопасности. Прогностическая аналитика использует исторические данные для прогнозирования будущих событий, а мониторинг социальных сетей заблаговременно обнаруживает угрожающие сообщения. Однако эти технологии часто воспринимаются скептически, рассматриваются как потенциально антиутопические и инвазивные, вызывающие опасения по поводу вторжения в личную жизнь, дискриминации и случайного вреда.

Существует настоятельная необходимость в установлении четких норм использования ИИ в сфере безопасности. Эффективное развертывание ИИ в борьбе с терроризмом требует не только сбора данных, но и этичного управления данными, приоритета конфиденциальности и безопасности данных для обеспечения того, чтобы технологические достижения приносили пользу обществу при соблюдении прав личности [20]. Баланс между улучшением безопасности и защитой свобод представляет собой значительную проблему, требующую тонкого подхода к использованию ИИ в борьбе с терроризмом, учитывающего этические дилеммы, техническую надежность и риск ошибок.

Прозрачное, регулируемое и этичное применение инструментов ИИ имеет важное значение для предотвращения терроризма при защите индивидуальных свобод и прав. Интеграция ИИ в стратегии борьбы с терроризмом представляет собой значительный шаг вперед в улучшении мер безопасности и возможностей прогнозирования. Тем не менее, преодоление этических соображений и технических проблем, связанных с его использованием, остается пока еще нерешенной проблемой.

Заключение

Дальнейшее повышение эффективности антитеррористической деятельности напрямую зависит от успеха в разрешении существующего противоречия между усилением деятельности, направленной на защиту граждан от внутренних угроз безопасности, и соблюдением демократических прав и свобод личности. Наиболее перспективным направлением разрешения этой проблемы является применение ИИ и машинного зрения. Ключевые технологии ИИ и машинного зрения, такие, как обработка изображений, распознавание лиц, обнаружение аномалий, предиктивная аналитика и мониторинг социальных сетей, позволяют эффективно обрабатывать и анализировать большие объемы данных и выявлять скрытые закономерности и идеи.

В то же время применение ИИ и машинного зрения в области борьбы с терроризмом вызывает новые проблемы, связанные с подготовкой обучающих наборов данных и этичностью применения инструментария ИИ. Преодоление этих проблем открывает путь к широкому внедрению технологий ИИ и машинного зрения в антитеррористическую деятельность и существенное повышение ее эффективности.

Литература

1. Карцхия А. А., Макаренко Г. И., Макаренко Д. Г. Правовые перспективы технологий искусственного интеллекта // Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. – С. 154–161. EDN: UCHFJY.
2. Карцхия А. А., Макаренко Г. И. Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. – 2024. – № 1(59). – С. 2–14. – DOI: 10.21681/2311-3456-2024-1-2-14. EDN: JTGKFM.
3. Гедгафов М. М. Роль искусственного интеллекта в противодействии терроризму // Журнал прикладных исследований. – 2023. – № 8. – С. 91–95. DOI: 10.47576/2949-1878_2023_8_91. EDN: QSQIIR.
4. Черкесов А. Ю. Искусственный интеллект в противодействии террористическим угрозам в глобальном информационном пространстве // Пробелы в российском законодательстве. – 2023. – Т. 16, № 5. – С. 166–170. EDN: LUUCYI.
5. Канкулов А. Х., Пантелеев В. А. Искусственный интеллект как метод борьбы с преступностью и терроризмом // Аграрное и земельное право. – 2024. – № 1(229). – С. 280–282. DOI: 10.47643/1815-1329_2024_1_280. EDN: SYXWUP.
6. Лаврухин М. В. Использование искусственного интеллекта в противодействии терроризму и оптимизация требований обеспечения транспортной безопасности к объектам дорожного хозяйства // Транспортное право и безопасность. – 2022. – № 4(44). – С. 126–143. EDN: TERJNU.
7. Молотникова А. А., Акуз А. В. Гибридные нейро-нечёткие сети в криминологии // Вестник Таганрогского института имени А. П. Чехова. – 2024. – № 2. – С. 68–76. EDN: ANZQQH.
8. Котенко И. В., Шоров А. В., Нестерук Ф. Г. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. – 2011. – № 3(18). – С. 19–73. EDN: OKHLLL.
9. Молотков П. П., Радайкин А. П. Методы машинного зрения в робототехнике // Наука и образование. Сборник трудов участников XVII Международной научной конференции. – Красноярск, 2025. – С. 74–77. EDN: NUYSTQ.
10. Силионов И. Н. Применение нейронных сетей в области компьютерного зрения для создания систем умного наблюдения и безопасности // Вестник науки. – 2025. – Т. 3, № 3(84). – С. 594–601. EDN: SQQJMF.
11. Сопильняк А. Ю. Современные подсистемы машинного зрения в интеллектуальных информационных системах // Advances in Science and Technology. Сборник статей LXVI международной научно-практической конференции. Москва, 2025. – С. 87–88. EDN: BELVMU.
12. Nale P., Gite S., Dharrao D. Real-Time Weapons Detection System using Computer Vision // 2023 Third International Conference on Smart Technologies, Communication and Robotics (STCR). Sathyamangalam, India, 2023. – Pp. 1–6. DOI: 10.1109/STCR59085.2023.10396960.
13. Sengupta A., Kundu A., Mukhopadhyay A. An Approach to Detect and Classify Potentially Suspicious Activity from Real-Time Log Data using Anomaly Detection Methods // 2024 3rd International Conference for Innovation in Technology (INOCON). Bangalore, India, 2024. – Pp. 1–9. DOI: 10.1109/INOCON60754.2024.10511679.

14. Abdalsalam M., Li Ch., Dahou A., Kryvinska N. Terrorism Attack Classification Using Machine Learning: The Effectiveness of Using Textual Features Extracted from GTD Dataset // Computer Modeling in Engineering & Sciences. – 2024. – Vol. 138, No. 2. – Pp. 1427–1467. DOI: 10.32604/cmes.2023.029911.
15. Pan X., Zhang T. Machine learning-based target prediction for terrorist attacks // Journal of Physics: Conference Series. – 2023. – Vol. 2577. – Article 012007, pp. 1–14. DOI: 10.1088/1742-6596/2577/1/012007.
16. Lu R., Huang J., Qu Y., Li L. Study on Combined-CNN Model for Classification of Terrorism Text // 2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). Shanghai, China, 2024. – Pp. 453–457. DOI: 10.1109/ICAACE61206.2024.10548392.
17. Lansky J. et al. Deep Learning-Based Intrusion Detection Systems: A Systematic Review // IEEE Access. – 2021. – Vol. 9. – Pp. 101574–101599. DOI: 10.1109/ACCESS.2021.3097247.
18. Kibtiah T. M., Miranda E., Fernando Y., Aryuni M. Terrorism, Social Media and Text Mining Technique: Review of Six Years Past Studies // 2020 International Conference on Information Management and Technology (ICIMTech). Bandung, Indonesia, 2020. – Pp. 571–576. DOI: 10.1109/ICIMTech50083.2020.9211148.
19. Hasanov I., Virtanen S., Hakkala A., Isoaho J. Application of Large Language Models in Cybersecurity: A Systematic Literature Review // IEEE Access. – 2024. – Vol. 12. – Pp. 176751–176778. DOI: 10.1109/ACCESS.2024.3505983.
20. Карцхия А. А., Макаренко Г. И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. – 2024. – № 1. – С. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19. EDN: NONHLC.

APPLICATION OF ARTIFICIAL INTELLIGENCE AND MACHINE VISION TECHNOLOGY IN THE FIGHT AGAINST ANTI-TERRORIST ACTIVITIES

***Sayenko I. B.*[2]**

Keywords: *terrorism, machine learning, deep learning, image processing, facial recognition, anomaly detection, predictive analytics, social networks.*

Abstract

Objective: *analysis of the content and possibilities of application of artificial intelligence and machine vision technologies that can be used in anti-terrorist activities, and formulation of problems inherent in this subject area, with justification of directions for their solution.*

Method: *system analysis of anti-terrorist activities and artificial intelligence technologies aimed at identifying a problem situation in a new subject area.*

Result: *the need for the use of artificial intelligence and machine vision technology to improve the effectiveness of anti-terrorist activities is substantiated. The characteristics of key technologies of artificial intelligence and machine vision that have a significant impact on protection against terrorism, such as image processing, face recognition, anomaly detection, predictive analytics and monitoring of social networks, are given. generated by the use of artificial intelligence and machine vision, related to the preparation of training datasets and the ethics of using artificial intelligence tools.*

Scientific novelty: *the analysis of works on the use of artificial intelligence and machine vision technologies in the field of counterterrorism for the first time showed that the technologies of image processing and face recognition, anomaly detection, predictive analytics and monitoring of social networks can be most applicable here. The use of these technologies in the interests of anti-terrorist activities leads to the emergence of new problems that require their immediate decisions that are due to the need for high-quality preparation of training datasets and the development of new moral and legal norms regarding the use of artificial intelligence tools.*

2 Igor B. Sayenko, Dr.Sc. (of tech.), Professor, Professor of the Department of Automated Special Purpose Systems, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: ibsaen@mail.ru

References

1. Karchija A. A., Makarenko G. I., Makarenko D. G. Pravovye perspektivy tehnologij iskusstvennogo intellekta // Bezopasnye informacionnye tehnologii. Sbornik trudov Dvenadcatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii. Moskva, 2023. – S. 154–161. EDN: UCHFJY.
2. Karchija A. A., Makarenko G. I. Pravovye gorizonty tehnologij iskusstvennogo intellekta: nacional'nyj i mezhdunarodnyj aspekt // Voprosy kiberbezopasnosti. – 2024. – № 1 (59). – S. 2–14. – DOI: 10.21681/2311-3456-2024-1-2-14. EDN: JTGKFM.
3. Gedgafov M. M. Rol' iskusstvennogo intellekta v protivodejstvii terrorizmu // Zhurnal prikladnyh issledovanij. – 2023. – № 8. – S. 91–95. DOI: 10.47576/2949-1878_2023_8_91. EDN: QSQIIR.
4. Cherkesov A. Ju. Iskusstvennyj intellekt v protivodejstvii terroristicheskim ugrozam v global'nom informacionnom prostranstve // Probely v rossijskom zakonodatel'stve. – 2023. – T. 16, №5. – S. 166–170. EDN: LUUCYI.
5. Kankulov A. H., Panteleev V. A. Iskusstvennyj intellekt kak metod bor'by s prestupnost'ju i terrorizmom // Agrarnoe i zemel'noe pravo. – 2024. – № 1(229). – S. 280–282. DOI: 10.47643/1815-1329_2024_1_280. EDN: SYXWUP.
6. Lavruhin M. V. Ispol'zovanie iskusstvennogo intellekta v protivodejstvii terrorizmu i optimizacija trebovanij obespechenija transportnoj bezopasnosti k ob#ektam dorozhnogo hozjajstva // Transportnoe pravo i bezopasnost'. – 2022. – № 4(44). – S. 126–143. EDN: TERJNU.
7. Molotnikova A. A., Akuz A. V. Gibridnye nejro-nechjotkie seti v kriminologii // Vestnik Taganrogskogo instituta imeni A. P. Chehova. – 2024. – № 2. – S. 68–76. EDN: ANZQQH.
8. Kotenko I. V., Shorov A. V., Nesteruk F. G. Analiz bioinspirirovannyh podhodov dlja zashhity komp'juternyh sistem i setej // Trudy SPIIRAN. – 2011. – № 3(18). – S. 19–73. EDN: OKHLLL.
9. Molotkov P. P., Radajkin A. P. Metody mashinnogo zrenija v robototehnike // Nauka i obrazovanie. Sbornik trudov uchastnikov XVII Mezhdunarodnoj nauchnoj konferencii. – Krasnojarsk, 2025. – S. 74–77. EDN: NUYSTQ.
10. Silionov I. N. Primenenie nejronnyh setej v oblasti komp'juternogo zrenija dlja sozdanija sistem umnogo nabljudenija i bezopasnosti // Vestnik nauki. – 2025. – T. 3, № 3(84). – S. 594–601. EDN: SQQJMF.
11. Sopil'njak A. Ju. Sovremennye podsistemy mashinnogo zrenija v intellektual'nyh informacionnyh sistemah // Advances in Science and Technology. Sbornik statej LXVI mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva, 2025. – S. 87–88. EDN: BELVMU.
12. Nale P., Gite S., Dharrao D. Real-Time Weapons Detection System using Computer Vision // 2023 Third International Conference on Smart Technologies, Communication and Robotics (STCR). Sathyamangalam, India, 2023. – Pp. 1–6. DOI: 10.1109/STCR59085.2023.10396960.
13. Sengupta A., Kundu A., Mukhopadhyay A. An Approach to Detect and Classify Potentially Suspicious Activity from Real-Time Log Data using Anomaly Detection Methods // 2024 3rd International Conference for Innovation in Technology (INOCON). Bangalore, India, 2024. – Pp. 1–9. DOI: 10.1109/INOCON60754.2024.10511679.
14. Abdalsalam M., Li Ch., Dahou A., Kryvinska N. Terrorism Attack Classification Using Machine Learning: The Effectiveness of Using Textual Features Extracted from GTD Dataset // Computer Modeling in Engineering & Sciences. – 2024. – Vol. 138, No. 2. – Pp. 1427–1467. DOI: 10.32604/cmes.2023.029911.
15. Pan X., Zhang T. Machine learning-based target prediction for terrorist attacks // Journal of Physics: Conference Series. – 2023. – Vol. 2577. – Article 012007, pp. 1–14. DOI: 10.1088/1742-6596/2577/1/012007.
16. Lu R., Huang J., Qu Y., Li L. Study on Combined-CNN Model for Classification of Terrorism Text // 2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). Shanghai, China, 2024. – Pp. 453–457. DOI: 10.1109/ICAACE61206.2024.10548392.
17. Lansky J. et al. Deep Learning-Based Intrusion Detection Systems: A Systematic Review // IEEE Access. – 2021. – Vol. 9. – Pp. 101574–101599. DOI: 10.1109/ACCESS.2021.3097247.
18. Kibtiah T. M., Miranda E., Fernando Y., Aryuni M. Terrorism, Social Media and Text Mining Technique: Review of Six Years Past Studies // 2020 International Conference on Information Management and Technology (ICIMTech). Bandung, Indonesia, 2020. – Pp. 571–576. DOI: 10.1109/ICIMTech50083.2020.9211148.
19. Hasanov I., Virtanen S., Hakkala A., Isoaho J. Application of Large Language Models in Cybersecurity: A Systematic Literature Review // IEEE Access. – 2024. – Vol. 12. – Pp. 176751–176778. DOI: 10.1109/ACCESS.2024.3505983.
20. Karchija A. A., Makarenko G. I. Pravovye problemy primenenija iskusstvennogo intellekta v Rossii // Pravovaja informatika. – 2024. – № 1. – S. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19. EDN: NONHLC.