

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

**ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА В ИНТЕРЕСАХ РЕШЕНИЯ ЗАДАЧ
ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ**

Методические рекомендации

**Воронеж
2026**

ББК 16.6
УДК 004.8

Коллектив авторов: Багринцева О.В., Гречаный С.А., Меркулова Н.И., Калков Д.Ю., Бондаренко Е.С.

Рецензенты: А.И. Леонов – заместитель начальника межмуниципального отдела МВД России на особо важных и режимных объектах Воронежской области, подполковник внутренней службы; С.С. Нехорошева – старший инспектор отдела кадров УРПС ГУ МВД России по Воронежской области, кандидат юридических наук, майор полиции..

Исследование возможностей искусственного интеллекта в интересах решения задач правоохранительных органов : методические рекомендации [Электронный ресурс] / О.В. Багринцева [и др.] – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2026. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования : процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows; CD-ROM дисковод.

Методические рекомендации фокусируются на исследовании возможностей искусственного интеллекта в интересах решения задач правоохранительных органов. В издании представлен анализ нормативно-правовой базы, регулирующей применение этих систем в подразделениях МВД России, а также рассмотрены уровни и методы интеграции различных подсистем в единые комплексы безопасности. Даны рекомендации по использованию возможностей искусственного интеллекта в интересах решения задач правоохранительных органов.

Издание адресовано курсантам и слушателям радиотехнического факультета, обучающимся по специальности 11.05.02 «Специальные радиотехнические системы», а также слушателям факультета заочного обучения по направлению 11.03.01 «Радиотехника», слушателям факультета переподготовки и повышения квалификации, а также факультета профессиональной подготовки.

ISBN 978-5-00229-278-3

© Воронежский институт МВД России, 2026

ОГЛАВЛЕНИЕ

Введение	4
1. Обзор современных возможностей искусственного интеллекта, оценка стратегий работы с данными, структуризация маркеров угроз в киберпространствах	5
1.1. Изучение источников информации	5
1.2. Анализ статистических данных, в том числе о мошенничествах, совершенных с помощью искусственного интеллекта и преступлениях в киберпространстве	12
2. Выбор нуждающегося в реконструкции профессионального контента, выработка решений по разоблачению с помощью искусственного интеллекта дип-фейков в автоматизированном режиме	15
2.1. Анализ мультимодальных массивов данных, подлежащих инструментальной компоновке с помощью искусственного интеллекта	15
2.2. Выявление перспектив развития информационных технологий	21
Заключение	28
Список использованных источников	30

ВВЕДЕНИЕ

В последние десятилетия искусственный интеллект (ИИ) стал неотъемлемой частью нашей жизни, проникая в различные сферы деятельности, от медицины и образования до финансов и транспорта. С развитием технологий ИИ возникает необходимость в правовом регулировании, которое должно учитывать как инновационные возможности, так и потенциальные риски, связанные с использованием этих технологий. Правовые аспекты ИИ представляют собой сложную и многогранную область, требующую внимательного анализа и осмысления. В данной работе рассматриваются правовые аспекты ИИ как в России, так и за рубежом, что позволяет выявить как общие тенденции, так и специфические особенности правового регулирования в разных странах.

Актуальность данной темы обусловлена тем, что стремительное развитие технологий ИИ создает новые вызовы для правовых систем. С одной стороны, ИИ открывает новые горизонты для экономического роста и повышения качества жизни, с другой стороны, он порождает множество правовых и этических вопросов. Например, как обеспечить защиту прав человека в условиях, когда решения принимаются алгоритмами? Как регулировать ответственность за действия, совершенные с использованием ИИ? Эти и многие другие вопросы требуют комплексного подхода и глубокого анализа.

В рамках работы будут освещены несколько ключевых тем. В первой части будет представлен обзор правового регулирования ИИ в России, включая существующие законодательные инициативы и подходы к нормотворчеству. Этические аспекты использования ИИ займут отдельное место в исследовании, поскольку они играют важную роль в формировании общественного мнения и правовых норм.

Также будет уделено внимание ключевым институтам, отвечающим за регулирование ИИ, включая как государственные органы, так и частные компании, работающие в сфере технологий. Современные вызовы и тенденции в регуляции ИИ будут проанализированы с акцентом на глобальные тренды, такие как необходимость обеспечения безопасности данных и защиты прав потребителей. Наконец, работа завершится обсуждением перспектив развития правового регулирования ИИ, что позволит сделать выводы о том, как государства могут адаптироваться к быстро меняющемуся технологическому ландшафту.

Таким образом, данная работа направлена на понимание того, как меняется правовая среда под воздействием технологий ИИ. Исследование правовых аспектов ИИ является важным шагом к созданию сбалансированной и эффективной правовой системы, способной учитывать как инновационные возможности, так и риски, связанные с использованием новых технологий.

ГЛАВА 1. ОБЗОР СОВРЕМЕННЫХ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, ОЦЕНКА СТРАТЕГИЙ РАБОТЫ С ДАННЫМИ, СТРУКТУРИЗАЦИЯ МАРКЕРОВ УГРОЗ В КИБЕРПРОСТРАНСТВАХ

1.1. Изучение источников информации

Правовые аспекты искусственного интеллекта приобретают все большее значение в современном мире из-за широкого применения этих технологий в различных сферах деятельности. Важность правового регулирования заключается в том, что оно способствует формированию безопасной и предсказуемой среды для использования ИИ, мешая при этом возможным злоупотреблениям и обеспечивая защиту прав граждан. Изменения в законодательстве должны учитывать особенности работы ИИ и связанные с этим этические вопросы, которые возникли еще в начале разработки систем, имитирующих человеческий интеллект.

С понятием «искусственный интеллект» связано множество определений, и оно эволюционировало на протяжении десятилетий. На разных этапах развития науки и технологий возникали неоднозначные правовые вопросы, особенно в контексте ответственности за действия, совершенные с помощью ИИ. Прежде чем углубляться в правоприменение, необходимо было четко определить, что подразумевается под ИИ и как к этому относится действующее законодательство. В России понятие «искусственный интеллект» впервые официально закреплено в законодательстве в 2019 году через указ Президента Российской Федерации, который обозначил направления для дальнейшего развития технологий [17].

История правовых вопросов, связанных с ИИ, опирается на литературу и философские дискуссии. Первые идеи о роботах и их взаимодействии с обществом появились в произведениях научной фантастики, что способствовало формированию общественного мнения относительно потенциальных рисков и возможностей [19]. Современные проблемы правового регулирования возникновения ИИ, включая этические аспекты, активизировались за последнее десятилетие, когда технологии начали внедряться в повседневную жизнь.

Для обеспечения эффективного правового регулирования важным шагом является введение экспериментальных правовых режимов (ЭПР), которые позволяют тестировать инновации с минимальными правовыми барьерами [16]. Они актуальны в секторах, таких как медицина, финансовые услуги и беспилотный транспорт, где применения ИИ могут улучшить эффективность процессов. Существует необходимость

детального анализа правовых преград, которые могут тормозить внедрение этих технологий в экономику [6].

На международной арене вопросы правового регулирования ИИ открывают новые возможности для сотрудничества и обмена опытом между странами. Обсуждение глобальных стандартов и этических норм с участием различных международных организаций позволяет создать единый подход к проблемам, связанным с использованием ИИ [18]. Важно, чтобы регулирования не только ограничивало потенциальные риски, но и стимулировало развитие инновационных технологий.

Таким образом, правовые аспекты искусственного интеллекта играют ключевую роль в гармонизации отношений между обществом и технологиями, нужно внимательно изучать и учитывать как позитивный, так и негативный вклад ИИ в различные сферы.

Экспериментальные правовые режимы

Развитие ИИ поддерживается также через введение экспериментальных правовых режимов

– Федеральный закон от 31.07.2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»,

– Федеральный закон от 02.07.2021 № 331-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»

Регулирование искусственного интеллекта стало предметом активного обсуждения на международном уровне, а в России также разрабатываются новые нормативные акты. Основные вызовы связаны с необходимостью защиты прав человека, этическими ограничениями и вопросами ответственности за действия ИИ. Концепция, предложенная Минцифры России, ориентируется на безопасное внедрение технологий ИИ с упором на создание более гибкой правовой базы [5]. Эта концепция подразумевает применение как гибридного подхода, так и обязательного страхования в качестве меры защиты от возможного ущерба, что может лечь в основу будущих законопроектов.

На глобальном уровне обратная ситуация наблюдается в странах ЕС, где вступило в силу законодательство, классифицирующее ИИ-технологии по уровням риска. Эти правила жестче, чем нынешние меры в России, и требуют от компаний соблюдения строгих стандартов этики и безопасности. Однако в США и Великобритании законодательства пока не имеют таких жестких рамок, что создает риски для потребителей и вызывает обеспокоенность экспертов [3].

В ответ на вызовы, вызванные быстрым развитием технологий, российские органы власти активно осмысливают адаптацию нормативных актов. Потребность в создании чёткой системы правил, регулирующих применение ИИ, становится всё более актуальной. Проблема неопределённой ответственности за ошибки ИИ требует ясных решений, чтобы не оставить вопрос о том, кто несёт ответственность за действия автоматизированных систем, без ответа [10].

Ключевое направление – это интеграция новых требований в существующую правовую базу, чтобы учитывать динамику изменения технологий. В этом контексте появляется необходимость в адаптации как нормативных, так и правоприменительных практик. Эти изменения могут включать обязательные требования к маркировке ИИ и систем, которые их используют, что также поднимет вопросы прозрачности и ответственности [11].

ИТЕМ инновации в области искусственного интеллекта, такие как предиктивная аналитика, требуют постоянного пересмотра существующих правил, поскольку эти технологии могут изменять бизнес-процессы и вводить новые аспекты юридической ответственности. Мировой тренд сообщает о том, что компании должны учитывать правовые аспекты ИИ, которые могут затрагивать как внутренние бизнес-операции, так и взаимодействие с внешними участниками [12].

На данный момент в России отсутствует единый комплект правовых норм, регулирующих все аспекты ИИ, а различные элементы законодательства нуждаются в упорядочении с учётом международного опыта. Таким образом, задача рационального регулирования становится ключевым приоритетом для власти, бизнеса и общества в целом, с целью создания безопасной и этической среды для внедрения ИИ-технологий.

Этические аспекты использования ИИ

Вопросы этики искусственного интеллекта становятся всё более актуальными по мере его внедрения в различные сферы жизни. Принятие в 2021 году «Рекомендации по этическим аспектам искусственного интеллекта» 193 государствами-членами ЮНЕСКО стало значимым шагом в нормировании этих вопросов на международном уровне. Основная цель данного документа заключается в защите прав человека и его достоинства, а также в обеспечении принципов прозрачности, справедливости и необходимости человеческого надзора за ИИ-системами [11].

Этические стандарты в сфере использования ИИ необходимы по причине его влияния на множество аспектов жизни. Примеры использования ИИ, от медицинских диагностических систем до автоматизированных систем правоприменения, демонстрируют как потенциальные преимущества, так и возможные риски, включая предвзятости алгоритмов и утрату персональной информации. Элементы

этики ИИ активно обсуждаются среди учёных и практиков, что подчеркивает важность применения существующих норм в условиях новых вызовов [5].

Фундаментальные аспекты этики, как правосубъектность ИИ и его долгосрочные последствия, сочетаются с прикладными вопросами, связанными с использованием ИИ в разнообразных областях. Например, в здравоохранении применение ИИ должно следовать моральным и правовым нормам, которые защищают пациента и обеспечивают его безопасность. При этом недостаточная регуляция часто приводит к спорным ситуациям, требующим внимательного разрешения [9].

Несмотря на наличие существующих норм, многие этические вопросы, связанные с ИИ, остаются открытыми. Например, исследования показывают, что внедрение ИИ в общественную жизнь поднимает вопросы о необходимости создания этических кодексов, обеспечивающих безопасность и комфорт пользователей [7]. Эти кодексы могут стать полезным инструментом для структурирования ответственности, однако их обязательность остается под вопросом.

Обсуждение этических аспектов использования ИИ должно стать основой для дальнейших правовых норм и регуляций. Необходимость создания стандартизированных подходов призвана отразить как технологии, так и моральные принципы человеческого взаимодействия с ними. Этический подход к ИИ не только направлен на решение уже известных проблем, но и предполагает постоянное обновление норм, чтобы отвечать на вызовы, связанные с новыми технологиями [14].

В заключение, этика ИИ требует внимательного отношения со стороны общества, бизнеса и государственного сектора. Привлечение всех заинтересованных сторон к этому обсуждению может помочь сформировать общий консенсус вокруг норм, регулирующих использование ИИ, что, в свою очередь, создаст более безопасную и равноправную среду для его внедрения.

Ключевые институты права и IT-компаний

Создание правовой базы для искусственного интеллекта требует взаимодействия как государственных учреждений, так и частного сектора. Эффективное регулирование зависит от того, как государственные органы смогут адаптироваться к быстро меняющимся условиям, инициированным новыми технологиями. Основные задачи включают формирование и внедрение нормативно-правовых актов, направленных на развитие ИИ в различных отраслях, включая медицину, транспорт и сферу услуг. В этих условиях ведущее значение приобретает сотрудничество между государственными структурами и IT-компаниями, способными провести необходимые исследования и практические испытания новых решений [16].

Важным аспектом является создание экспериментальных правовых режимов, которые позволяют тестировать технологии в реальных условиях. Это требует от государства гибкости в регулировании. Например, разработка концепции регулирования ИИ до 2030 года, инициированная Минцифры, включает в себя консолидацию мнений отраслевых участников и экспертов [5]. Без поддержки и активного участия бизнеса такие инициативы могут оказаться невостребованными.

Во многих странах, таких как США и государства ЕС, наблюдается более активное участие частного сектора в формировании политики регулирования ИИ. Например, в Европейском Союзе принятие AI Act требует от разработчиков обеспечения прозрачности и надежности ИИ-систем. Это приводит к необходимости значительных инвестиций и активной работы над юридическими механизмами, которые бы позволяли соответствовать новым требованиям [2]. В отличие от этого, в России, адаптация к мировым стандартам и конфронтация с местной бюрократией могут тормозить внедрение инновационных решений.

Государственные институты, такие как Минцифры, играют ключевую роль в разработке и внедрении стандартов, определяющих принципы этического использования ИИ. Например, в России ведется мониторинг нормативных актов, касающихся ИИ, что позволяет выявлять необходимость регулирования новых отношений, возникающих в результате технологий [16]. Подобный подход обеспечивает более целенаправленное взаимодействие между заинтересованными сторонами и данными особенностям рынка.

Существование платформ и консорциумов, объединяющих государственный и частный сектора, также способствует созданию необходимой правовой инфраструктуры. Это позволяет объединять усилия для разработки новых стандартов и технологий, уменьшая время на внедрение и повышая эффективность [15]. Компании, как правило, обладают более глубокими знаниями о конкретных технологиях и задачах, которые они решают, что делает их партнерами по разработке регуляторных инструментов, способных быстро адаптироваться под новые вызовы и потребности рынка.

В конечном счете, успех регулирования ИИ в России будет зависеть не только от законодательных инициатив, но и от партнерства между государственными учреждениями и частным сектором. Это взаимодействие должно основываться на принципах прозрачности, гибкости и готовности к изменениям в условиях технологических новаций, что станет основой для внедрения эффективных и этических решений в области ИИ.

Современные вызовы и тенденции в регуляции ИИ

Регулирование искусственного интеллекта стало предметом активного обсуждения на международном уровне, а в России также

разрабатываются новые нормативные акты. Основные вызовы связаны с необходимостью защиты прав человека, этическими ограничениями и вопросами ответственности за действия ИИ. Концепция, предложенная Минцифры России, ориентируется на безопасное внедрение технологий ИИ с упором на создание более гибкой правовой базы [5]. Эта концепция подразумевает применение как гибридного подхода, так и обязательного страхования в качестве меры защиты от возможного ущерба, что может лечь в основу будущих законопроектов.

На глобальном уровне обратная ситуация наблюдается в странах ЕС, где вступило в силу законодательство, классифицирующее ИИ-технологии по уровням риска. Эти правила жестче, чем нынешние меры в России, и требуют от компаний соблюдения строгих стандартов этики и безопасности. Однако в США и Великобритании законодательства пока не имеют таких жестких рамок, что создает риски для потребителей и вызывает обеспокоенность экспертов [3].

В ответ на вызовы, вызванные быстрым развитием технологий, российские органы власти активно осмысливают адаптацию нормативных актов. Потребность в создании чёткой системы правил, регулирующих применение ИИ, становится всё более актуальной. Проблема неопределенной ответственности за ошибки ИИ требует ясных решений, чтобы не оставить вопрос о том, кто несет ответственность за действия автоматизированных систем, без ответа [10].

Ключевое направление – это интеграция новых требований в существующую правовую базу, чтобы учитывать динамику изменения технологий. В этом контексте появляется необходимость в адаптации как нормативных, так и правоприменительных практик. Эти изменения могут включать обязательные требования к маркировке ИИ и систем, которые их используют, что также поднимет вопросы прозрачности и ответственности [11].

ИТЕМ инновации в области искусственного интеллекта, такие как предиктивная аналитика, требуют постоянного пересмотра существующих правил, поскольку эти технологии могут изменять бизнес-процессы и вводить новые аспекты юридической ответственности. Мировой тренд сообщает о том, что компании должны учитывать правовые аспекты ИИ, которые могут затрагивать как внутренние бизнес-операции, так и взаимодействие с внешними участниками [12].

На данный момент в России отсутствует единый комплект правовых норм, регулирующих все аспекты ИИ, а различные элементы законодательства нуждаются в упорядочении с учётом международного опыта. Таким образом, задача рационального регулирования становится ключевым приоритетом для власти, бизнеса и общества в целом, с целью создания безопасной и этической среды для внедрения ИИ-технологий.

Перспективы развития правового регулирования ИИ

Современные тренды в правовом регулировании искусственного интеллекта предполагают серьезные изменения в подходах как в России, так и за ее пределами. Одним из актуальных направлений стало создание комплексной правовой базы, учитывающей особенности использования ИИ в различных отраслях. Существует вероятность введения строгого нормативно-правового регулирования, направленного на стимулирование инноваций и защиту прав пользователей. Это предполагает необходимость пересмотра существующих норм с целью их адаптации к новым технологиям и вызовам, например, в области безопасности и защиты данных [16].

Разработка Кодекса этики для ИИ станет важным шагом к общественной и корпоративной ответственности. Внедрение этических норм уже осуществляется через различные комитеты, что также требует активного участия бизнеса и государства. Ожидается, что такие проявления сподвигнут к улучшению взаимодействия между разработчиками технологий и пользователями, способствуя росту доверия к ИИ как к инструменту, а не угрозе [10].

Экспериментальные правовые режимы обеспечат возможность тестирования новых технологий без необходимости соблюдения всех предусмотренных норм. Это открывает перед компаниями перспективы для внедрения ИИ в таких отраслях, как медицина и транспорт, где новые технологии могут значительно повысить уровень обслуживания и безопасности [5]. В рамках таких режимов важно создание условий для коллегиального обмена знаниями с последующим анализом результатов, что в свою очередь, поспособствует дальнейшему улучшению регуляторной среды.

Финансирование и подготовка кадров также остаются важными аспектами. Увеличение инвестиций в научные исследования и программы повышения квалификации специалистов позволит обеспечивать качественное развитие технологий, уменьшая разрыв между теорией и практикой [19].

Международное сотрудничество может сыграть решающую роль в формировании единого подхода к правовому регулированию ИИ. Взаимодействие с зарубежными коллегами в области стандартизации и регулирования откроет новые горизонты для обмена опытом и разработки универсальных принципов, способствующих безопасному и эффективному использованию ИИ [4].

Следовательно, будущее правового регулирования в области ИИ требует синергии усилий со стороны всех участников процесса: государства, бизнеса, научной среды и общества. Успех этих инициатив будет зависеть от готовности адаптироваться к темпам изменений и внедрения новых норм, что в конечном итоге приведет к более безопасному

и эффективному использованию технологий ИИ на благо социального блага.

1.2. Анализ статистических данных, в том числе о мошенничествах, совершенных с помощью искусственного интеллекта и преступлениях в киберпространстве

В современную цифровую эпоху данные стали новым стратегическим ресурсом, а киберпространство – пятой областью противостояния после суши, моря, воздуха и космоса. Анализ статистических данных является ключевым инструментом для понимания динамики и масштабов угроз в этой области. Особую актуальность сегодня приобретает изучение двух взаимосвязанных тенденций: стремительного роста традиционных киберпреступлений и появления принципиально новых рисков, связанных со злоупотреблением технологиями искусственного интеллекта (ИИ). Статистика не просто фиксирует количество инцидентов; она позволяет выявить уязвимости, спрогнозировать тренды и выработать эффективные меры противодействия. Данная работа посвящена анализу текущей статистики в сфере киберпреступности и мошенничеств с использованием ИИ, чтобы оценить их реальные масштабы и определить основные векторы атак. Современная криминогенная обстановка характеризуется стремительной цифровизацией преступной деятельности. Рост числа киберпреступлений является прямым следствием технологической эволюции, предоставляющей злоумышленникам новые, более изощренные инструменты.

Современная криминогенная обстановка характеризуется стремительной цифровизацией преступной деятельности. Рост числа киберпреступлений является прямым следствием технологической эволюции, предоставляющей злоумышленникам новые, более изощренные инструменты.

Общий тренд роста киберпреступности:

Мошенничества с использованием ИИ – качественно новый вызов:

Технологии искусственного интеллекта, в частности генеративные модели, создали новый класс высокотехнологичных угроз. Согласно отчетам аналитических центров (например, Group-IB, Positive Technologies), в 2024 году более 60% крупных мошеннических схем использовали элементы ИИ.

Дипфейк (Deepfake) – это синтетический медиафайл (изображение, аудио или видео), созданный с использованием методов искусственного

интеллекта и машинного обучения, главным образом, для подмены одного человека другим или для реалистичного изменения его действий и речи.

Дипфейки перестали быть забавой энтузиастов и превратились в инструмент гибридных войн, кибератак, манипуляции общественным мнением, шантажа и дезинформации. Скорость их создания и распространения в социальных сетях такова, что ручная верификация становится неэффективной. Это создает острую потребность в разработке и внедрении автоматизированных систем детекции, способных в реальном времени анализировать потоки данных и выявлять подделки. Эволюция дипфейков прошла несколько этапов:

1. Ранние методы (до 2014 г.): Использование простых методов наложения лица (face-swap) и компьютерной графики (CGI). Результаты были легко узнаваемы из-за низкого реализма.

2. Прорыв с появлением GAN (2014 г.): Изобретение Яном Гудфеллоу генеративно-сопоставительных сетей (GAN) стало ключевым моментом. В GAN две нейронные сети работают вместе: генератор создает поддельные изображения, а дискриминатор пытается отличить их от настоящих. В процессе противоборства генератор учится создавать все более совершенные подделки.

3. Эпоха автоэнкодеров и диффузионных моделей (2020-н.в.): Появление таких моделей, как StyleGAN, а позже – Stable Diffusion и Midjourney, позволило создавать дипфейки не только высочайшего качества, но и с минимальными вычислительными затратами, сделав технологию доступной массовому пользователю.

Дипфейки – инструмент гибридных войн и киберпреступности, преступники используют их для:

1) Манипуляция общественным мнением Дипфейк с «обращением» президента Владимира Путина (2022 г.).

Суть: появилось видео, где диктор российского государственного телеканала якобы зачитывает экстренное обращение президента о мобилизации. Видео было сделано методом lip-sync: лицо диктора было анимировано так, чтобы совпадать с поддельной аудиодорожкой. Сообщение содержало панические нотки и явно было направлено на дестабилизацию обстановки в стране.

Подобные инциденты фиксируются по всему миру в преддверии выборов или во время социально-политических кризисов.

2) Корпоративный шантаж и мошенничество. Злоумышленники создают видео- или аудиоклоны руководителей компаний и дают указания сотрудникам перевести крупные суммы денег на контролируемые счета. Ущерб от одной такой успешной атаки может исчисляться миллионами долларов.

3) Компрометация и дискредитация лиц. Создание поддельных компрометирующих материалов для шантажа публичных персон или сотрудников, имеющих доступ к коммерческой или государственной тайне.

4) Голосовые клоны (аудиодипфейки):

Это одно из самых быстрорастущих направлений. Для клонирования голоса сейчас достаточно короткой аудиозаписи из открытых источников (подкаст, выступление, видео в соцсетях). Мошенники используют эту технологию для имитации голоса родственника с просьбой о срочном денежном переводе, якобы из-за проблем с законом или здоровьем. Эффективность таких атак крайне высока из-за психологического давления.

Скорость создания и распространения дипфейков в мессенджерах и социальных сетях такова, что традиционные методы ручной модерации и верификации не успевают за угрозой. Это создает критическую потребность в проактивных и автоматизированных системах детекции.

Анализ данных позволяет выявить не только масштабы угрозы, но и наиболее уязвимые сферы, что является первым шагом для построения эффективной системы защиты. Фокус смещается с реагирования на уже совершенные преступления на их превентивное прогнозирование и предотвращение.

ГЛАВА 2. РОЛЬ И СОВРЕМЕННОЕ СОСТОЯНИЕ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ НА ТЕРРИТОРИЯХ, ВНОВЬ ПРИСОЕДИНЕННЫХ К РОССИЙСКОЙ ФЕДЕРАЦИИ

Борьба с дипфейками – это своего рода «гонка вооружений», где ключевым преимуществом является скорость и точность их выявления. Автоматизированная система детекции должна уметь работать с разнородными данными и выявлять малейшие следы вмешательства.

2.1. Анализ мультимодальных массивов данных, подлежащих инструментальной компоновке с помощью искусственного интеллекта

Эффективное обнаружение дипфейков требует комплексного (мультимодального) анализа всех составляющих медиафайла. Недостаточно анализировать только видео или только аудио. Современные системы должны комбинировать следующие методы:

1. Визуальный анализ (анализ изображения и видео):

XceptionNet, MesoNet, EfficientNet: Специализированные архитектуры сверточных нейронных сетей (CNN), обученные на огромных датасетах типа FaceForensics++, которые содержат как реальные видео, так и дипфейки, созданные разными методами. Сеть учится выделять features (признаки) низкого уровня, характерные для артефактов генерации: специфические текстуры кожи, странные паттерны пикселей в областях бровей, губ, ноздрей.

Анализ частотного спектра (Frequency Domain Analysis): Дипфейки часто имеют отличия в частотном спектре от реальных видео. Алгоритмы, такие как DFT (Discrete Fourier Transform) или DCT (Discrete Cosine Transform), переводят изображение в частотную область, где артефакты сжатия и генерации становятся более заметными. Например, GAN-артефакты могут проявляться как специфические шумы в высокочастотном диапазоне.

Анализ артефактов глаз и взгляда.

Глаза – чрезвычайно сложный для реалистичной подделки объект.

Анализ роговичного отблеска (Corneal Specular Reflection): Роговица глаза действует как выпуклое зеркало, отражая окружающую обстановку. В оригинальном видео отражения в левом и правом глазу будут практически идентичными по форме и содержанию. В дипфейке, созданном на основе

изображений с другого фона, эти отражения часто отсутствуют, размыты или не совпадают между глазами. Алгоритмы сегментируют область глаза, выделяют отблески и сравнивают их.



Рис. 1. Анализ артефактов глаз и взгляда

Анализ движения зрачков и взгляда: Направление взгляда и синхронность движения зрачков подчиняются определенным физиологическим паттернам. Нейросети могут отслеживать траекторию взгляда и обнаруживать неестественные «прыжки» или залипания, нехарактерные для живого человека.

Анализ артефактов глаз и взгляда:

1) Роговичный отблеск: Роговица глаза как выпуклое зеркало отражает окружающую обстановку. В оригинальном видео отражения в левом и правом глазу идентичны. В дипфейке они часто отсутствуют, размыты или не совпадают.

2) Движение зрачков: Направление взгляда и синхронность движения зрачков подчиняются физиологическим паттернам. Нейросети отслеживают траекторию взгляда, выявляя неестественные «прыжки».

3) Анализ физической согласованности:

4) Согласованность освещения и теней: Алгоритмы восстанавливают карту освещения сцены по лицу. Если освещение на лице не соответствует освещению на шее, ушах или фоне – это верный признак подделки.

5) Физика движения: Модели анализируют, насколько движение кожи и волос соответствует законам физики (инерция, упругость тканей).

2. Аудиоанализ (выявление аудиодипфейков):

Для детекции аудиодипфейков (глубоких подделок голоса) используются свои методы.

Спектральный анализ: Анализ спектрограммы (визуального представления спектра звука) позволяет выявить артефакты. Синтезированный голос может иметь неестественные форманты (спектральные пики), шумы или «артефакты фонового шума», которые не меняются так, как у настоящего голоса, записанного в конкретной акустической среде.

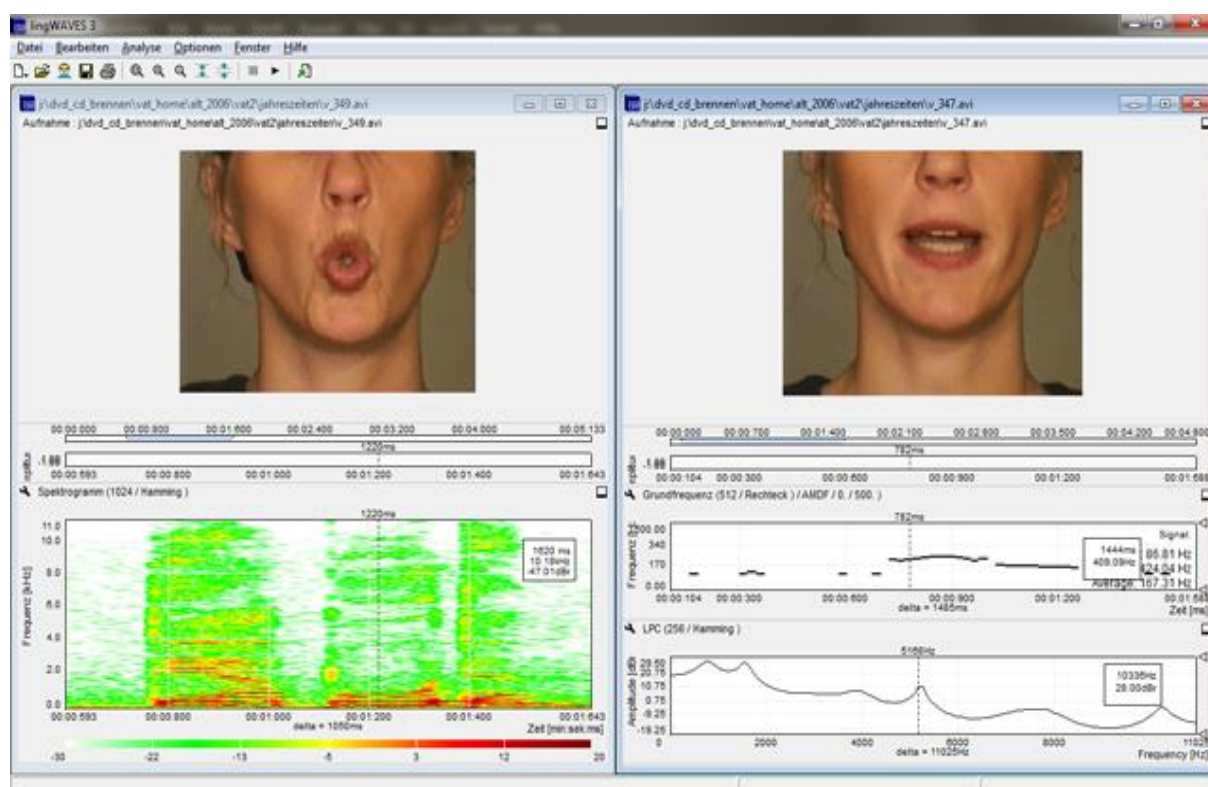


Рис. 2. Анализ артефактов речи и голоса

Анализ просодии: Просодия – это ритм, темп, интонация и ударение в речи. TTS-системы часто выдают себя неестественной просодией: монотонностью, странными паузами или неадекватными эмоциональными акцентами. Модели, основанные на рекуррентных нейронных сетях (RNN), анализируют эти временные ряды.

3. Кросс-модальный анализ:

Лип-синк (Lip-Sync) детекция – это кросс-модальный анализ. Система одновременно анализирует аудиодорожку и видео, чтобы проверить,

насколько точно движения губ совпадают с произносимыми фонемами. Любое расхождение выше определенного порога является признаком манипуляции.

Методы, основанные на анализе физической согласованности. Эти методы проверяют, насколько реалистично смоделированы физические законы в видео.

Анализ освещения и теней (Lighting Consistency). Алгоритмы, такие как анализ сферических гармоник, могут восстановить карту освещения сцены по лицу человека. Если освещение на лице не соответствует освещению на шее, ушах, волосах или фоне – это верный признак подделки. Например, тень от носа на щеке должна падать под тем же углом, что и тень от человека на стене позади.

Анализ физики движения (Physically Based Reasoning). Нейросети могут быть обучены предсказывать, как должно двигаться лицо в соответствии с законами физики (инерция, упругость тканей). Резкие, физически невозможные движения кожи или волос могут быть выявлены.

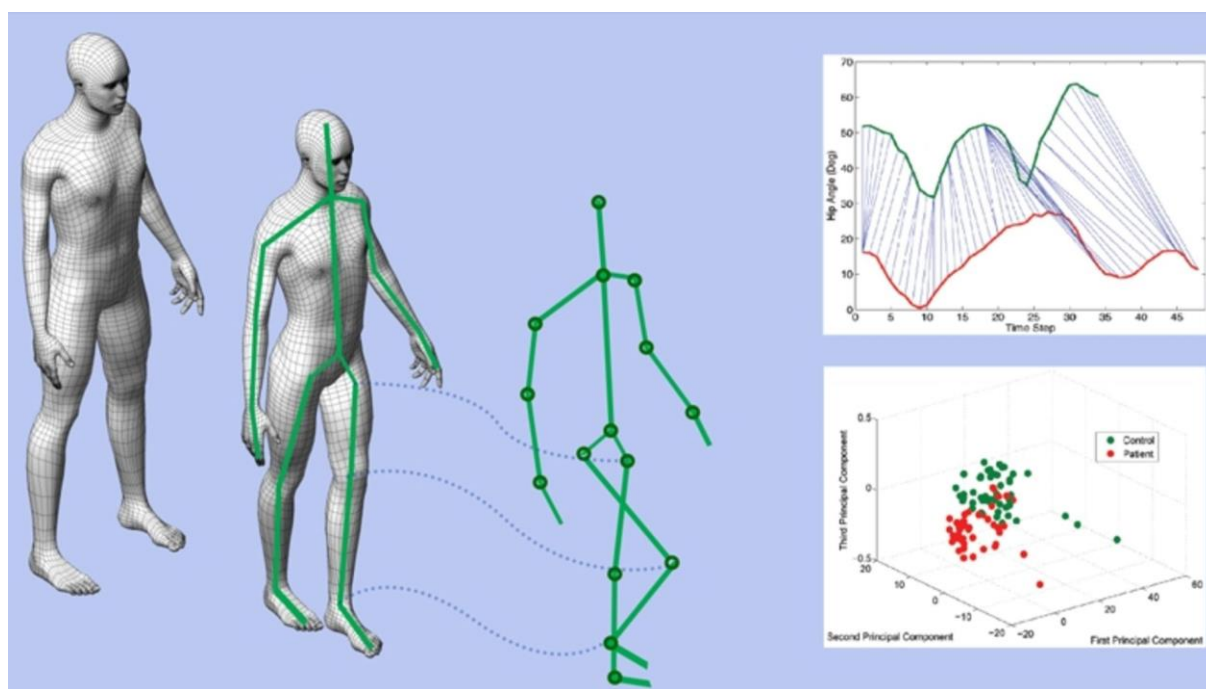


Рис. 3. Анализ физики движения человека

Методы, основанные на анализе цифровых следов (Noise и Compression Artifacts)

Каждая камера имеет уникальный «отпечаток пальца» – паттерн шума, который равномерно распределяется по всему кадру. Программы для создания дипфейков нарушают эту структуру.

4. Анализ цифровых следов (Метаданные и шумы):

Анализ шумового паттерна (Sensor Pattern Noise – SPN). У каждой матрицы фотоаппарата есть уникальный рисунок шума, вызванный несовершенством кремниевых пластин. Этот шум остается consistent across всех кадрах, снятых одной камерой. При вставке дипфейка шумовой паттерн на лице будет отличаться от паттерна на фоне или шее. Алгоритмы выделяют этот шум и ищут несоответствия.

Анализ артефактов сжатия: практически все видео в интернете сжимаются (кодеки H.264, HEVC). Процесс сжатия follows определенным законам (например, разбиение на макроблоки). Когда дипфейк вставляется в уже сжатое видео, а затем видео пережимается заново, возникают двойные артефакты сжатия. Алгоритмы могут детектировать эти несоответствия в структуре блоков на разных участках кадра.

Проверка метаданных (EXIF, XMP). Отсутствие метаданных или наличие в них следов ПО для редактирования (например, Adobe Photoshop) является косвенным, но важным признаком, запускающим более глубокую проверку.

Инструментальная компоновка подразумевает создание единого конвейера, где мультимодальные данные последовательно или параллельно обрабатываются разными алгоритмами, а их результаты агрегируются для вынесения итогового вердикта о подлинности контента.

Практические примеры: от инцидента до разоблачения

Пример: Фальшивое выступление губернатора Курской области Романа Старовойта (2023 г.)

Этот инцидент является хрестоматийным примером быстро выявленного, но все же успевшего навредить дипфейка.

Суть инцидента: в конце июня 2023 года в Telegram-каналах, а затем и в некоторых СМИ, появилось видео, где губернатор Курской области Роман Старовойт якобы обращается к жителям с призывом эвакуироваться из-за наступления ВСУ. Сообщение содержало панические нотки и явно было направлено на дестабилизацию обстановки в прифронтовом регионе.

Реакция: официальный Telegram-канал Старовойта практически мгновенно опроверг информацию, назвав видео «фейком и провокацией». Было запущено разбирательство.

Как разоблачили (признаки и методы):

1. Визуальный анализ (доступный даже вручную): Качество видео было заметно хуже, чем у официальных обращений. Наблюдались легкие «размытия» вокруг контура лица, особенно в области волос и ушей – классический артефакт некачественного face-swap.

2. Анализ синхронизации: Движения губ не идеально совпадали с аудиодорожкой, что было заметно при внимательном просмотре.

3. Контекстуальный анализ: Тон и содержание сообщения радикально расходились со всеми предыдущими официальными заявлениями губернатора, который придерживался спокойной и уверенной риторики.

4. Автоматизированная детекция (предположительно): Крупные платформы и мониторинговые центры, скорее всего, использовали быстрые CNN-модели (типа EfficientNet), которые сразу flagged видео как подозрительное по его низкоуровневым feature maps, что позволило быстро принять решение о его блокировке и опровержении.

Технологические и платформенные меры борьбы

Развитие и внедрение детекторов: Постоянное финансирование исследований в области AI-детекции, создание и поддержка открытых датасетов (как FaceForensics++) для обучения моделей. Крупные IT-компании (Meta, Google, Microsoft) уже внедряют такие детекторы в свои платформы (Instagram, YouTube, Bing).

Проактивная маркировка контента (Proactive Content Credentials). Перспективное направление – использование технологии «водяных знаков» на основе AI или стандарта C2PA (Coalition for Content Provenance and Authenticity). Эта технология позволяет встраивать в metadata файла криптографическую подпись, подтверждающую источник происхождения контента (какая камера, какое ПО для редактирования использовалось). Камера могла бы подписывать исходный файл, а соцсети – проверять эту подпись. Любой файл без подписи или с нарушенной цепочкой доверия автоматически помечался бы как «непроверенный».

Модерация на платформах. Соцсети должны ужесточить и автоматизировать политику модерации, оперативно удаляя вредоносные дипфейки после их обнаружения системами или пользователями, а также понижая их в выдаче.

Browser-based детекторы: Разработка расширений для браузеров, которые в реальном времени анализируют загружаемое пользователем видео и предупреждают его о возможной подделке.

Технологии не дают 100% гарантии. Поэтому критически важно обучать население.

Публичные кампании. Государственные и общественные организации должны проводить кампании, объясняющие, что такое дипфейки, как они создаются и на какие признаки стоит обращать внимание (неестественность мимики, голоса, контекст).

Включение в образовательные программы. Основы медиаграмотности и цифровой гигиены должны стать частью школьной и университетской программ.

Основные инструкции для пользователя:

1. Проверь источник: опубликовано ли это на официальном сайте/канале?
2. Включи критическое мышление: насколько правдоподобно сообщение? Соответствует ли оно предыдущим заявлениям человека?
3. Всмотрись и вслушайся: моргает ли человек естественно? Синхронны ли движения губ и звук? Не «плывут» ли контуры лица?
4. Используй поиск: не появилось ли уже опровержение от официальных лиц?
5. Воспользуйся технологиями: если есть сомнения, существуют онлайн-сервисы для проверки (например, Deepware Scanner и др.).

2.2. Выявление перспектив развития информационных технологий

Будущее борьбы с дипфейками лежит в области проактивных, а не реактивных мер, а также в глубокой интеграции технологий в платформы и образовательные процессы.

Использование нейросетей в расследованиях

Нейросети представляют собой мощный инструмент для решения задач правоохранительных органов, особенно в области расследования преступлений. Они обладают способностью обрабатывать огромные объемы данных, анализировать их и выявлять закономерности, что значительно превышает возможности традиционных методов. Например, такие системы могут автоматически распознавать лица на фотографиях и видеозаписях, что позволяет быстро идентифицировать подозреваемых и находить пропавших лиц.

Современные нейросети могут быть обучены на специфических данных, что делает их универсальными и адаптируемыми к различным условиям. В процессе обучения нейросети используют алгоритмы глубокого обучения, которые позволяют им улучшать точность распознавания со временем. Это особенно важно в криминалистике, где каждая деталь может иметь значение для раскрытия дела. Одна из перспективных разработок в этой области – система «Клон», которая помогает выявлять подделки в видеозаписях, что становится актуальным в условиях распространения дезинформации и фальсификации видеоматериалов.

Преимущество нейросетей заключается также в их способности обрабатывать информацию в реальном времени, что позволяет оперативно реагировать на потенциальные угрозы. Используя алгоритмы предсказательной аналитики, нейросети способны предсказывать места и время возможных преступлений, что даёт правоохранительным органам возможность заранее предпринимать меры. Внедрение таких систем в практику правоохранительных органов позволяет не только повышать эффективность расследований, но и сокращать время, необходимое для раскрытия преступлений.

Нейросети также применяются для анализа текстовых данных, что помогает в раскрытии преступлений, связанных с киберпреступностью и мошенничеством. Алгоритмы обработки естественного языка могут анализировать сообщения, письма и другие текстовые данные, выявляя паттерны и аномалии, которые могут свидетельствовать о преступной деятельности. Таким образом, нейросети не только ускоряют процесс расследования, но и улучшают качество собранных улик.

Не следует забывать о проблемах и вызовах, связанных с использованием нейросетей в правоохранительных органах. Несмотря на свою эффективность, такие технологии могут вызвать опасения относительно нарушений конфиденциальности и прав человека. Вопросы о том, как нейросети могут повлиять на взаимодействие между людьми в процессе работы правоохранительных органов, остаются открытыми и требуют тщательного рассмотрения.

При правильном внедрении и учёте этических аспектов, потенциал нейросетей в расследованиях преступлений окажется значительным. Правительство Российской Федерации уже планирует использование этих технологий в своих структурах, что также говорит о готовности правоохранительных органов адаптироваться к современным вызовам. Таким образом, нейросети становятся не только инструментом, но и важной частью реформы криминалистики и правоохранительной практики в целом.

Компьютерное зрение как инструмент доказательства

Компьютерное зрение (КЗ) открывает новые горизонты для правоохранительных органов, обеспечивая разнообразные инструменты для анализа визуальной информации. Системы распознавания лиц, подключенные к камерам наблюдения, позволяют оперативно идентифицировать подозреваемых и связывать их с преступлениями, используя базы данных. Это повышает вероятность быстрой реакции на криминальные действия и способствует более эффективному раскрытию дел. Более того, современные технологии КЗ могут обнаруживать скрытые элементы на месте преступления, такие как оружие или улики, что существенно облегчает задачи следственных органов.

Системы, использующие компьютерное зрение, могут анализировать видеозаписи, выделяя специфические паттерны и действия, значимые для расследования. Например, они позволяют отслеживать перемещение транспортных средств в реальном времени, что помогает в поиске подозреваемых. Технологии также могут создавать 3D-модели мест преступлений, что значительно улучшает процесс визуализации и анализа ситуации, а также помогает в судопроизводстве.

Однако внедрение компьютерного зрения связано с определенными вызовами. Важно учитывать этические аспекты, такие как защита конфиденциальности граждан. Необходимо обеспечить, чтобы алгоритмы не были предвзятыми и не приводили к дискриминации определенных групп населения. Для этого потребуется адаптация моделей КЗ под уникальные наборы данных, используемые в правоохранительных системах.

Внедрение компьютерного зрения в правоохранительные органы сопряжено с необходимостью обучать сотрудников работе с новыми технологиями. Это касается как технического оснащения, так и понимания современных этических норм в сфере использования таких систем. Будущее правоохранительных органов, использующих КЗ, зависит не только от технологического прогресса, но и от готовности адаптироваться к новым вызовам и требованиям.

Обработка естественного языка для анализа данных

Обработка естественного языка (NLP) стала важным инструментом в работе правоохранительных органов, обеспечивая новые возможности для автоматизации процессов обработки информации и взаимодействия с гражданами. Например, современные языковые модели, такие как ChatGPT, способны автоматически обрабатывать обращения граждан, что значительно снижает время ответа на запросы и повышает точность анализируемой информации. Применение таких технологий позволяет правоохранительным органам более эффективно справляться с большими объемами данных, которые ранее обрабатывались вручную, тем самым освобождая время для более сложной работы.

Комплексный подход к внедрению NLP включает в себя адаптацию содержания материалов под конкретные социальные группы. Алгоритмы машинного обучения позволяют выделять паттерны использования языка, что делает взаимодействие полиции с разными демографическими группами более целенаправленным. Например, офис шерифа во Флориде использовал технологии искусственного интеллекта для создания адаптированных публичных обращений после инцидентов, что помогло улучшить обратную связь с населением.

Автоматизация обработки обращений также требует высокой языковой грамотности сотрудников, что напрямую влияет на

эффективность их работы. Упор на обучение языковой культуре и компетенции сотрудников становится важным шагом к повышению качества обслуживания населения и улучшения имиджа правоохранительных структур. Это создает необходимость в непрерывном обучении персонала и повышении их квалификации в сфере технологий, связанных с NLP.

В свою очередь, использование языковых моделей поднимает вопросы надежности и точности получаемых результатов. Важно, чтобы сотрудники понимали возможности и ограничения алгоритмов, и умели применять их в своей деятельности, не полагаясь исключительно на автоматизацию. Система обработки естественного языка должна интегрироваться в общие процессы правоохранительных органов, что обеспечит более высокий уровень доверия со стороны граждан и повысит эффективность действий полиции.

Таким образом, внедрение технологий NLP в правоохранительную деятельность предоставляет уникальные возможности для улучшения коммуникации и анализа данных, одновременно подчеркивая необходимость ответственного подхода к их использованию.

Автоматизация работы правоохранительных органов

Современная автоматизация рабочих процессов правоохранительных органов с помощью искусственного интеллекта (ИИ) предоставляет множество возможностей для оптимизации и повышения эффективности работы. Одним из примеров является комплексное управление полицейскими ресурсами. Применение ИИ позволяет не только анализировать данные о преступности, но и на основе этих данных формировать рекомендации по распределению патрулей в зонах с высоким риском преступности. Такие алгоритмы могут учитывать разные факторы, включая время суток, места событий и историю преступлений в определённых районах, что способствует более проактивному подходу к охране общественного порядка.

Планирование задач также значительно упрощается благодаря внедрению ИИ. Интеллектуальные системы могут автоматически анализировать рабочие графики, учитывать доступные ресурсы и потребности, а затем предлагать оптимальные решения для расстановки сил. Это позволяет сократить время, которое уходит на распределение задач среди сотрудников, тем самым увеличивая продуктивность целых подразделений. Более того, ИИ может помогать в мониторинге выполнения этих задач в режиме реального времени, предоставляя оперативную информацию о необходимости корректировок.

Мониторинг ситуаций с использованием технологий ИИ открывает новые горизонты для правоохранительных органов. Современные системы видеонаблюдения, поддерживаемые алгоритмами машинного обучения,

позволяют не только фиксировать правонарушения, но и оперативно реагировать на инциденты, определяя потенциально опасные ситуации. Это может быть особенно полезно в больших городах, где быстрое реагирование может значительно снизить уровень преступности. Автоматизация анализа данных и распознавания лиц в реальном времени делает эти системы более эффективными. К тому же, применение ИИ в данной области помогает выявлять закономерности, которые могут быть неочевидны для человека, что, в свою очередь, ведёт к более глубокому пониманию преступности.

Ещё одной важной составляющей автоматизации является управление взаимоотношениями с гражданами. Автоматизированные системы могут улучшить качество обратной связи, позволяя гражданам более удобно сообщать о проблемах или получать информацию. Это способствует более прозрачному взаимодействию между гражданами и правоохранительными органами, что в свою очередь повышает уровень доверия. Результаты этих взаимодействий могут аккумулироваться и анализироваться, что помогает органам поддерживать более актуальное понимание потребностей общества и соответствующим образом адаптировать свои действия.

Таким образом, интеграция современных технологий ИИ в рабочие процессы правоохранительных органов делает их более динамичными и адаптивными к требованиям времени, улучшая как оборону, так и взаимодействие с обществом.

Этические вызовы применения ИИ

Внедрение искусственного интеллекта (ИИ) в правоохранительные органы открывает новые горизонты, но также ставит перед обществом ряд этических вопросов. Необходимость обеспечения защиты данных является одной из главных задач, которые предстоит решить. Сбор и хранение больших объемов личной информации может привести к ее несанкционированному использованию или утечке, что подрывает доверие граждан к правоохранительной системе. Понимание и соблюдение принципов конфиденциальности становятся критически важными, особенно в условиях, когда информация может быть использована против самих граждан.

Другим значимым аспектом является проблема предвзятости (bias) в алгоритмах, которые применяются для анализа данных. Необоснованные выводы и решения, основанные на ошибочных данных или неполных образцах, могут привести к дискриминации и ущемлению прав определённых групп населения. Это вызывает серьезные опасения относительно справедливости правоприменения, поскольку алгоритмы могут унаследовать намеренные или ненамеренные предвзятости от разработчиков или обучающих данных. В этом контексте требуется

внедрение жестких стандартов для алгоритмической прозрачности, чтобы обеспечить возможность внешней проверки и верификации результатов работы ИИ.

Существует также необходимость формирования общественного доверия к новым технологиям в правоохранительной практике. Важно, чтобы граждане ощущали, что их права защищены, и системы, использующие ИИ, работают на благо общества, а не против него. Для достижения этого необходимо наладить эффективные коммуникации между правоохранительными учреждениями и обществом, информируя граждан о целях и методах применения ИИ. Это позволит создать более благоприятную атмосферу для принятия технологических новшеств в повседневную практику.

Критика и сторонние оценки внедрения ИИ в правоохранительные органы также имеют значение. Независимые экспертизы могут помочь выявить потенциальные риски и недостатки используемых технологий, что, в свою очередь, поможет избежать негативных последствий и недопониманий между правоохранительными органами и обществом. Разработка этических рекомендаций и стандартов становится приоритетом, чтобы минимизировать возможные этические последствия и строить взаимодействие на основе доверия.

Подводя итог, необходимо подчеркнуть, что этические аспекты применения ИИ в правоохранительных органах требуют активного внимания и участия всех заинтересованных сторон. Успех внедрения новых технологий будет зависеть от того, насколько эффективно будут решены проблемы конфиденциальности, предвзятости и доверия общества к инновациям. Применение принципов этики и прозрачности станет основой для справедливого и гармоничного сосуществования технологий и общества.

Будущее интеграции ИИ в правоохранительную практику

В будущем интеграция искусственного интеллекта (ИИ) в практику правоохранительных органов предполагает значительное развитие технологий. Министерство внутренних дел России анонсировало внедрение систем «Клон» и «Конъюнктура», ожидающееся с 2025 года. Система «Клон» будет способствовать проверке подлинности видеоизображений, в то время как «Конъюнктура» рассчитана на прогнозирование инцидентов и моделирование ответных действий в различных ситуациях. Эти разработки представляют собой шаг к более эффективному управлению безопасностью и правопорядком, что станет возможным благодаря предсказательной аналитике и глубокому анализу данных.

Существуют значительные преимущества применения ИИ, такие как улучшение оперативной эффективности за счет автоматизации анализа больших объемов данных. Предполагается, что это приведет к более

эффективному выявлению преступников и снижению уровня преступности. Однако важно учитывать и вызовы, связанные с этим внедрением, в частности, возможность ошибок в алгоритмах и высокие требования к вычислительным мощностям. Успех таких систем будет зависеть от качества обучающих данных и их приспособления к конкретной оперативной среде.

Этические аспекты применения ИИ также становятся важной темой для обсуждения. Чтобы обеспечить доверие общества к новым технологиям, необходимо разработать четкие этические нормы и алгоритмы, регулирующие использование ИИ. Вопросы приватности и конфиденциальности данных становятся критически важными в свете расширяющегося применения таких технологий. Подходы, основанные на принципах открытости и ответственности, могут помочь в построении доверительных отношений между правоохранительными органами и населением.

Возможные сценарии развития технологий ИИ предполагают значительное разнообразие. Например, в будущем можно ожидать создания сложных алгоритмов, способных не только предсказывать преступления, но и моделировать потенциальные сценарии реагирования на чрезвычайные ситуации. Это должно повысить оперативность и точность действий правоохранительных органов в условиях неопределенности. Системы, подобные «Конъюнктуре», могут адаптироваться к новым угрозам, используя методики машинного обучения и анализа больших данных для постоянного улучшения своих прогнозов.

Несмотря на технические сложности, возможности ИИ могут революционизировать полицейскую деятельность, обеспечивая более безопасные условия для граждан. Проведение научно-исследовательских работ и подготовка качественных датасетов для обучения нейросетевых моделей, запланированная на 2024 год, станет важным шагом к успешному внедрению данных технологий. Уверенность в том, что ИИ станет неотъемлемой частью правоохранительной практики, открывает новые горизонты для повышения безопасности и лучшего реагирования на угрозы.

ЗАКЛЮЧЕНИЕ

В заключение, современные технологии ИИ, такие как нейросети, компьютерное зрение и обработка естественного языка, открывают новые горизонты для повышения эффективности деятельности правоохранительной системы. Эти инструменты позволяют значительно ускорить обработку больших данных, автоматизировать рутинные процессы, усовершенствовать процедуры расследования и раскрытия преступлений, а также улучшить взаимодействие с гражданами. Внедрение систем прогнозной аналитики и автоматизированного мониторинга информационного пространства создает основу для проактивного реагирования на угрозы.

Одновременно с этим интеграция ИИ в правоохранительную практику сопряжена с комплексом серьезных вызовов. Ключевым из них является проблема дипфейков – гиперреалистичных синтетических медиа, которые представляют собой прямую угрозу информационной безопасности, общественному спокойствию и доверию к институтам власти. Как показало исследование, противодействие этому явлению требует непрерывного совершенствования автоматизированных систем детекции, основанных на мультимодальном анализе биометрических, физических и цифровых артефактов. Однако технологическая гонка не может быть выиграна исключительно силами детекторов. Не менее важными элементами стратегии борьбы являются внедрение проактивных мер, таких как цифровое маркирование контента по стандарту C2PA, и системное повышение медиаграмотности населения.

Правовое регулирование искусственного интеллекта находится в стадии активного формирования как в России, так и на международной арене. Успешное развитие этой сферы требует от законодательной системы гибкости, адаптивности и способности предвосхищать риски. Крайне важно, чтобы правовая база не только создавала условия для инноваций, но и обеспечивала надежную защиту прав граждан, устанавливала четкие рамки ответственности и этические стандарты использования технологий. В этом контексте необходим сбалансированный подход, учитывающий как инновационный потенциал ИИ, так и необходимость сохранения общественного доверия.

Таким образом, потенциал искусственного интеллекта для правоохранительных органов огромен, но его реализация возможна только

при условии комплексного подхода. Успешная интеграция ИИ зависит от синергии трех ключевых компонентов: передовых технологий, robust правового регулирования и системной образовательной работы. Только такая триединая стратегия позволит обеспечить безопасное, эффективное и этическое использование технологий будущего для защиты прав граждан и укрепления правопорядка.

СПИСОК ЛИТЕРАТУРЫ

1. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового регулирования в области цифровой экономики: Федеральный закон от 1 апреля 2020 года № 90-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.04.2025).
2. О порядке рассмотрения обращений граждан Российской Федерации: Федеральный закон от 3 апреля 2017 года № 59-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.04.2025).
3. Об электронной цифровой подписи: Федеральный закон от 10 января 2002 г. № 1-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.04.2025).
4. О техническом регулировании: Федеральный закон от 27 декабря 2002 г. № 184-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.04.2025).
5. О персональных данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.04.2025).
6. ChatGPT и правоохранительные органы: как большие языковые модели меняют методы работы? [Электронный ресурс] // external.software – Режим доступа: <https://external.software/archives/30888>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).
7. Балансировка инновации и ответственности: искусственный интеллект в полиции [Электронный ресурс] // neurounit.ai - Режим доступа: <https://neurounit.ai/blog/balansirovka-innovatsij-i-otvetstvennosti-iskusstvennyj-intellekt-v-politsii/>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).
8. Батоев В.Б. Об использовании нейронных языковых моделей в правоохранительной деятельности // Юрист - Правоведь. 2024. №2 (109). URL: <https://cyberleninka.ru/article/n/ob-ispolzovanii-neyronnyh-yazykovyh-modeley-v-pravoohranitelnoy-deyatelnosti> (28.08.2025) (дата обращения: 25.04.2025).
9. Бахтеев Д.В. Компьютерное зрение и распознавание образов в криминалистике // Российское право: образование, практика, наука. 2019. №3 (111). URL: <https://cyberleninka.ru/article/n/kompyuternoe-zrenie-i-raspoznavanie-obrazov-v-kriminalistike> (дата обращения: 25.04.2025).
10. Венедов А.А., Иванов М.А. «Цифровая форензика: обнаружение и расследование киберпреступлений». – М.: Издательский дом «Питер», 2021 (дата обращения: 25.04.2025).
11. Гельманова З. С., Бакаев Т. К. Внедрение искусственного интеллекта в деятельность органов внутренних дел // In The World Of

Science and Education. 2024. №15 декабрь ЮН. URL: <https://cyberleninka.ru/article/n/vnedrenie-iskusstvennogo-intellekta-v-deyatelnost-organov-vnutrennih-del> (дата обращения: 25.04.2025).

12. Гриняев С.Н., Соколов С.В. «Искусственный интеллект и безопасность: вызовы и угрозы нового поколения». – М.: Горячая линия – Телеком, 2020 (дата обращения: 25.04.2025).

13. Зоз В. А., Шроль А. Р. Использование технологий искусственного интеллекта в правоохранительных органах // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2021. №2. URL: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologiy-iskusstvennogo-intellekta-v-pravoohranitelnyh-organah> (дата обращения: 25.04.2025).

14. Искусственный интеллект выходит на борьбу... - CNews [Электронный ресурс] // www.cnews.ru - Режим доступа: https://www.cnews.ru/news/top/2024-01-11_iskusstvennyj_intellekt, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

15. Кетия Т.А. Применение нейросетей в деятельности органов внутренних дел // Евразийская адвокатура. 2022. №3 (58). URL: <https://cyberleninka.ru/article/n/primenenie-neyrosetey-v-deyatelnosti-organov-vnutrennih-del> (дата обращения: 25.04.2025).

16. Клон и Конъюнктура: МВД РФ анонсировало внедрение ИИ... [Электронный ресурс] // www.securitylab.ru - Режим доступа: <https://www.securitylab.ru/news/545135.php>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

17. Компьютерное зрение в контрольно-надзорной деятельности – Аркадий Фройм на TenChat.ru [Электронный ресурс] // tenchat.ru - Режим доступа: <https://tenchat.ru/media/1603050-kompyuternoye-zreniye-v-kontrolnonadzornoj-deyatelnosti>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

18. Нейросети помогают полиции раскрывать преступления даже... [Электронный ресурс] // www.1tv.ru - Режим доступа: https://www.1tv.ru/news/2025-08-24/518923-neyroseti_pomogayut_politsii_raskryvat_prestupleniya_dazhe_mnogoletney_davnosti, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

19. Организационно-правовые основы информационного... [Электронный ресурс] // www.hse.ru - Режим доступа: <https://www.hse.ru/sci/diss/1063287520>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

20. Применение искусственного интеллекта в судебной... [Электронный ресурс] // moluch.ru - Режим доступа: <https://moluch.ru/archive/501/110059>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

21. Применение технологий обработки естественного языка... [Электронный ресурс] // apni.ru - Режим доступа: <https://apni.ru/article/12493-primenenie-tehnologij-obrabotki-estestvennogo-yazyka-nlp-i-mashinnogo-obucheniya-dlya-obrabotki-obrashenij-grazhdan-v-sisteme-municipalnogo-upravleniya>, свободный. - Загл. с экрана (дата обращения: 25.04.2025).

22. Уральский государственный юридический университет [Электронный ресурс] // www.researchgate.net - Режим доступа: https://www.researchgate.net/profile/dmitry-bakhteev/publication/335802453_computer_vision_and_pattern_recognition_in_forensic_science/links/5d98f26c299b1c363fb2a80/computer-vision-and-pattern-recognition-in-forensic-science.pdf, свободный. - Загл. с экрана. (дата обращения: 25.04.2025).

Багринцева Оксана Владимировна
Гречаный Сергей Анатольевич
Меркулова Наталья Ивановна
Калков Дмитрий Юрьевич
Бондаренко Евгений Сергеевич

**ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА В ИНТЕРЕСАХ РЕШЕНИЯ ЗАДАЧ
ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ**

Методические рекомендации

Редактор В.Ю. Калинская
Компьютерная верстка Д.Ю. Калкова
Объем 0,6 МБ. Тираж 10 экз.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53