

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

**ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
В ОХРАНЕ ОБЩЕСТВЕННОГО ПОРЯДКА
И ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ
НА ТЕРРИТОРИЯХ, ВНОВЬ ПРИСОЕДИНЕННЫХ В СОСТАВ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Методические рекомендации

**Воронеж
2026**

УДК 351.74
ББК 32.96

Коллектив авторов: Е. М. Абросимова, С. А. Гречаный, О. В. Толстых, Д. А. Сошнева, Ю. С. Никитина.

Рецензенты:

А. А. Баранников – начальник Управления Федеральной службы войск национальной гвардии Российской Федерации по Воронежской области, полковник полиции;

Н. Н. Бородин – начальник УВО по г. Орлу – филиала ФГКУ «УВО ВНГ России по Орловской области», полковник полиции.

Применение информационных технологий в охране общественного порядка и обеспечении общественной безопасности на территориях, вновь присоединенных в состав Российской Федерации [Электронный ресурс] / Е. М. Абросимова, С. А. Гречаный, О. В. Толстых, Д. А. Сошнева, Ю. С. Никитина. – 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 использовании автоматизированных информационных систем для управления безопасностью на территориях, недавно присоединенных к Российской Федерации. 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. Учитывая эти аспекты, проанализированы компоненты интегрированных систем безопасности, доступные на отечественном рынке технических средств, и определены оптимальные решения для применения в органах внутренних дел. Даны рекомендации по повышению эффективности обеспечения безопасности объектов МВД России с использованием современных автоматизированных информационных технологий.

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 978-5-00229-276-9

УДК 351.74
ББК 32.96

© Воронежский институт МВД России, 2026

СОДЕРЖАНИЕ

Введение	4
Анализ вопроса охраны общественного порядка	
1. и обеспечения общественной безопасности на территориях, присоединенных к Российской Федерации	5
1.1. Правовое положение территорий, присоединенных к Российской Федерации	5
1.2. Основы правового регулирования внедрения информационных технологий в деятельность по охране общественного порядка и обеспечению общественной безопасности	8
Роль и современное состояние	
2. внедрения информационных систем в обеспечении общественной безопасности на территориях, присоединенных к Российской Федерации	16
2.1. Современное состояние внедрения интеллектуальных и интегрированных систем безопасности в России	16
2.2. Перспективы повышения эффективности применения информационных технологий в охране общественного порядка и обеспечении общественной безопасности на территориях, присоединенных к Российской Федерации	24
Заключение	31
Список литературы	33

ВВЕДЕНИЕ

Актуальность научно-исследовательской работы заключается в том, что в период современной России приходится сталкиваться с комплексом внутренних и внешних вызовов, оказывающих значительное влияние на различные аспекты жизнедеятельности страны. Текущие геополитические реалии, беспрецедентное давление со стороны отдельных мировых держав отражаются на миграционных процессах как внутри нашей страны, так и за ее пределами.

Современное общество сталкивается с множеством вызовов, связанных с обеспечением безопасности и охраны общественного порядка. В условиях динамично меняющегося мира, где технологии проникают во все сферы жизни, применение информационных технологий (ИТ) становится неотъемлемой частью эффективного управления правоохранительными органами. Особенно актуальна данная проблема для территорий, недавно присоединенных к Российской Федерации, где необходимо не только адаптировать существующие подходы к охране порядка, но и внедрять инновационные решения, способствующие повышению уровня безопасности и укреплению правопорядка.

Исследование применения ИТ в охране общественного порядка на этих территориях представляет собой важный шаг к пониманию специфики и особенностей новых регионов. В условиях многообразия культурных, социально-экономических и правовых реалий, интеграция современных технологий может стать ключевым фактором в формировании эффективной системы безопасности. Это включает в себя использование систем видеонаблюдения, аналитических платформ для обработки данных, а также мобильных приложений, способствующих взаимодействию граждан и правоохранительных органов.

ГЛАВА 1. АНАЛИЗ ВОПРОСА ОХРАНЫ ОБЩЕСТВЕННОГО ПОРЯДКА И ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ НА ТЕРРИТОРИЯХ, ПРИСОЕДИНЕННЫХ К РОССИЙСКОЙ ФЕДЕРАЦИИ

1.1. Правовое положение территорий, присоединенных к Российской Федерации

В период современного развития Российская Федерация сталкивается с комплексом внутренних и внешних вызовов, оказывающих значительное влияние на различные аспекты ее жизнедеятельности. В контексте текущих геополитических реалий, давление со стороны отдельных мировых держав приобретает беспрецедентный характер, что отражается на миграционных процессах как внутри страны, так и за ее пределами.

Важным фактором, оказывающим влияние на миграционную ситуацию, является проведение Российской Федерацией специальной военной операции (СВО), начатой 24 февраля 2022 года. Предшествовало этому признание независимости Луганской Народной Республики и Донецкой Народной Республики и обращение их представителей за помощью в защите от военных действий со стороны Украины.

Российская Федерация, обладая статусом многонационального государства и придерживаясь принципов толерантности, считает своим долгом обеспечить защиту прав и безопасности граждан, проживающих на территориях, подвергшихся военным действиям [20]. Эти территории обладают стратегической географической и экономической значимостью, что делает их объектом интересов со стороны Украины, действия которой противоречат нормам международного права.

В процессе специальной военной операции, проводимой Российской Федерацией, была осуществлена оккупация значительной части Запорожской области Украины, включая такие населённые пункты, как Бердянск, Васильевка, Мелитополь и Энергодар, последний из которых является месторасположением Запорожской атомной электростанции. На оккупированных территориях была организована военно-гражданская администрация, руководителем которой стал Евгений Балицкий, ранее занимающий должность депутата Верховной рады Украины от Партии регионов. Мелитополь, являющийся наиболее крупным городом в пределах оккупированной части Запорожской области, был определён временным административным центром. В то же время областной центр Запорожье, население которого составляет приблизительно 50% от общего числа жителей региона, остался под контролем украинских властей. К началу марта 2022 года российские войска установили контроль над Херсонской областью, где была сформирована аналогичная военно-гражданская

администрация под руководством Владимира Сальдо, ранее занимавшего пост мэра Херсона.

Таким образом, Российская Федерация обязана реализовать цели, поставленные перед Специальной военной операцией, включая обеспечение безопасности граждан. На данный момент значительная часть поставленных задач уже выполнена, что дало возможность гражданам четырех субъектов принять самостоятельные решения относительно их будущего. Следует отметить, что правовое регулирование, связанное с проведением СВО, оказывает влияние на правовой статус жителей четырех новых субъектов Российской Федерации, что требует дополнительного анализа и исследования в контексте международного права и внутреннего законодательства.

В рамках научного дискурса следует подчеркнуть, что российские исследователи осуществляют всесторонний анализ правового положения участников специальной военной операции. Однако вопрос правового статуса граждан, проживающих на территориях, которые были присоединены к Российской Федерации, остается недостаточно освещенным. Эти лица, являясь соотечественниками, оказались в сложной жизненной ситуации по причинам, не зависящим от их воли. В связи с этим, уточнение и детализирование правового статуса в общем и административно-правового статуса в частности представляет собой важный фактор, способствующий ускорению процесса интеграции населения Донбасса в правовую систему Российской Федерации [21].

Федеральные конституционные законы от 4 октября 2022 года № 5-ФКЗ, № 6-ФКЗ, № 7-ФКЗ и № 8-ФКЗ определили, что в состав Российской Федерации вошли Донецкая Народная Республика, Луганская Народная Республика, Херсонская и Запорожская области, установив переходный период до 1 января 2026 года. Эти нормативные акты также определили процедуру признания гражданства Российской Федерации для лиц, постоянно проживающих на указанных территориях.

При анализе указанных федеральных конституционных законов можно сделать вывод о том, что правовой статус жителей новых субъектов фактически эквивалентен статусу граждан Российской Федерации. В контексте административно-правового статуса гражданина Российской Федерации, следует принять во внимание позицию профессора Ю. Н. Старилова, который определяет административно-правовой статус как совокупность прав и обязанностей индивида в рамках административно-правовых отношений [22]. Исходя из этого, можно заключить, что жители четырех новых субъектов обладают полным административно-правовым статусом, аналогичным статусу граждан Российской Федерации.

Тем не менее представляется логичным предположить, что данный статус может быть охарактеризован как специальный административно-

правовой статус, по крайней мере, в течение времени действия переходных положений.

Логический вывод, представленный в данном контексте, находит свое обоснование в следующих аспектах:

1. На территориях Донецкой Народной Республики, Луганской Народной Республики, а также Запорожской и Херсонской областей введено военное положение в соответствии с Указом Президента Российской Федерации от 19 октября 2022 года № 756. Данный указ предусматривает реализацию мер территориальной обороны и вводит комплекс ограничений прав и свобод граждан для лиц, постоянно проживающих или временно находящихся на указанных территориях.

2. Процесс интеграции данных территорий в правовую, экономическую и налоговую систему Российской Федерации предполагает сохранение действия ранее принятых нормативных правовых актов на данных территориях, за исключением тех, которые противоречат Конституции Российской Федерации. Это указывает на наличие специфики в правовом регулировании административно-правового статуса граждан на упомянутых территориях.

3. Социальная защита граждан Донецкой и Луганской Народных Республик, а также Запорожской и Херсонской областей реализуется через финансовые стимулы для проживания на данных территориях. Это отражено в Федеральном законе от 17 февраля 2023 года № 18-ФЗ «Об особенностях правового регулирования отношений в сфере социальной защиты и социального обслуживания граждан, проживающих на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области». Законоположение предусматривает сохранение действующих до переходного периода социальных выплат в случае их превосходства над новыми установленными.

4. Текущий период характеризуется интеграцией правовых норм, действующих в Российской Федерации, и адаптацией существующего законодательства к новым условиям, регулирующим статус граждан на указанных территориях.

Исходя из специфики правового статуса, можно классифицировать граждан четырех субъектов Российской Федерации на следующие категории:

1. Граждане, вынужденные покинуть районы, где проводились или продолжаются военные операции, что квалифицирует их как внутренние перемещенных лиц.

2. Лица, проживающие на территориях Донецкой Народной Республики (ДНР), Луганской Народной Республики (ЛНР), а также Херсонской и Запорожской областей, которые участвуют в мероприятиях

территориальной обороны, а также те, которые в результате военных действий остались без жилья.

3. Иностранные граждане, отказавшиеся от приобретения гражданства Российской Федерации, но проживающие на территориях указанных субъектов на основании легальных документов.

4. Граждане ДНР, ЛНР, Херсонской и Запорожской областей, которые продолжают проживать в данных регионах в условиях введенного экстраординарного правового режима, а именно военного положения.

1.2. Основы правового регулирования внедрения информационных технологий в деятельность по охране общественного порядка и обеспечению общественной безопасности

В контексте устойчивого сохранения повышенного уровня рисков как техногенного, так и природного происхождения, а также в условиях продолжающейся урбанизации актуализируется потребность в укреплении общественной безопасности, поддержании правопорядка и безопасности окружающей среды. Это предполагает необходимость значительного улучшения координации действий органов и служб, ответственных за реализацию указанных функций. Решение данных задач предполагается осуществлять через внедрение интегрированной информационной системы, которая будет способствовать прогнозированию, мониторингу, предупреждению и нейтрализации потенциальных угроз, а также обеспечивать контроль за процессами ликвидации последствий чрезвычайных ситуаций и правонарушений. Интеграция информационно-управляющих подсистем дежурных и диспетчерских служб, а также муниципальных служб под управлением данной системы, позволит обеспечить оперативное взаимодействие между ними.

Второй фактор, обуславливающий необходимость применения информационных технологий (ИТ) в управленческой и правоохранительной деятельности, связан с информационно-техническим аспектом современной преступности. Анализ правоприменительной практики и судебной статистики показывает тенденцию к увеличению числа преступлений в сфере компьютерной информации, а также преступлений, совершаемых с использованием компьютерных технологий. В связи с этим, раскрытие и расследование таких преступлений представляется возможным только при использовании современных информационных технологий правоохранительными органами [23].

Третий аспект, требующий внедрения и развития ИТ, связан с необходимостью оперативности принятия управленческих решений. В условиях динамично развивающейся экономики и всех сфер человеческой деятельности, основанных на информационных технологиях, в критических

ситуациях требуется немедленное принятие адекватных управленческих решений. Для этого необходимо мгновенное получение и анализ информации из всех доступных источников, что невозможно без использования современных автоматизированных информационных поисковых систем, баз данных, систем анализа и оповещения.

Внедрение информационных технологий (ИТ) в сферу государственного управления обусловлено множеством факторов, включая экономическую эффективность, оптимизацию бюрократических процедур, улучшение качества государственных услуг и повышение общего уровня жизни населения.

Среди прочего, имплементация ИТ ставит перед органами государственной и муниципальной власти задачу создания коммуникативной платформы для местных органов самоуправления. Это необходимо для минимизации рисков, связанных с обеспечением общественной безопасности, поддержанием правопорядка и сохранением безопасной жизненной среды, что предполагает межведомственное взаимодействие и оперативное реагирование на чрезвычайные ситуации.

Создание единого информационного пространства, учитывающего дифференциацию прав доступа к информации различного типа, способствует эффективному информационному обмену между субъектами всех уровней исполнительной власти в контексте обеспечения безопасности.

Единое информационное пространство, представляющее собой интеграцию технических средств информационной среды и активное взаимодействие ее участников, приводит к формированию специфической виртуальной реальности.

В контексте государственной политики в области развития виртуальной реальности в различных сегментах общественной жизни следует отметить инициативу Правительства Российской Федерации по созданию 27 виртуальных музеев к 2018 году. Это предполагает обеспечение доступа граждан к культурным объектам и информации государственных архивов на региональном уровне, в том числе путем создания веб-сайтов и информационных порталов учреждений культуры в интернете, формирования электронных баз данных фондов музеев и архивов, а также создания электронных копий уникальных экспонатов музейных коллекций [24].

В рамках реализации Стратегии государственной культурной политики Российской Федерации планируется модернизация материально-технической базы образовательных учреждений в области культуры, включая детские школы искусств, а также создание предпосылок для использования электронных билетов в музеях, театрах и на культурно-развлекательных мероприятиях. Данный инновационный подход предполагает трансформацию социального статуса культуры на

качественно новом уровне, в том числе через формирование виртуальных театральных площадок, концертных залов и музеев на территории всех субъектов Федерации.

В контексте информационного общества актуализируется задача обеспечения доступа к культурным ценностям в цифровом формате, что включает в себя возможность ознакомления с музейными экспозициями, историческими и природными достопримечательностями, туристическими маршрутами в режиме онлайн. Это предполагает использование технологий визуализации, проведение виртуальных экскурсий, создание видеороликов и фотоматериалов.

Как было отмечено выше, новейшие информационные технологии XXI века очень востребованы в современном мире и применяются практически в любой деятельности. В частности, информационная технологизация не прошла мимо такой сферы деятельности как правоохранительная. Говоря о правоохранительных органах, стоит подчеркнуть, что охрана общественного порядка и обеспечение общественной безопасности является одним из ключевых аспектов их деятельности. Сотрудники органов внутренних дел, Федеральной службы войск национальной гвардии РФ осуществляют патрулирование по улицам населенных пунктов, а также принимают меры реагирования на изменяющуюся оперативную обстановку. Однако даже их деятельность нуждается в систематизации и информатизации в целях повышения эффективности охраны и снятия общего уровня нагрузки с сотрудников правоохранительных органов.

В частности, говоря о роли информационной технологизации в правоохранительной деятельности, стоит отметить, что любая деятельность, направленная на совершение юридически значимых действий, предполагающих наступление конкретных правовых последствий, тесно связана с таким понятием как «информация». В переводе с латинского языка слово «информация» (informatio) означает «разъяснение, изложение». До середины XX века данный термин интерпретировался как «сообщение, осведомляющее о положении дел, о состоянии чего-нибудь».

На сегодняшний день данный термин официально закреплён в Федеральном законе Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ, где в п. 1 ст. 2 законодатель называет информацией абсолютно «любые сведения (сообщения, данные) независимо от формы их представления». Закрепив это определение и регламентировав основы деятельности, связанной с защитой информации и применением информационных технологий в современной России, на наш взгляд, законодатель подчеркивает важность придания информации состояния защищенности, при которой несанкционированный доступ к ней минимизируется.

Информация в любой форме ее представления всегда являлась основным объектом юридической деятельности и, соответственно, в условиях развития информационных устройств для юристов важно обеспечить быстрый доступ к информации и оперативную и удобную работу с ней. Поэтому президентская программа правовой информатизации органов государственной власти в РФ, утвержденная Указом Президента РФ от 4 августа 1995 года № 808, в первую очередь была направлена на создание условий, в которых должно было происходить образование единого информационно-правового пространства органов государственной власти РФ, значительно облегчающего работу с нормативными правовыми актами и иными юридическими документами.

Доступ к такой системе сегодня осуществляется при помощи информационно-коммуникационных технологий, позволяющих должностным лицам органов государственной власти осуществлять мониторинг законодательства в своей сфере юридической деятельности и получать всю необходимую информацию оперативно и удобно.

Говоря о процессе информатизации в Российской Федерации, стоит отметить нормативно-правовую базу, регламентирующую порядок внедрения информационно-технологических достижений, а также порядок работы с информацией.

К основным нормативным правовым актам в рассматриваемой области общественных отношений относятся:

1. Окинавская хартия Глобального информационного общества, принятая 22 июля 2000 г. на о. Окинава [18]. Это важнейший международно-правовой акт, подписанный лидерами стран G8 – так называемой, «Большой восьмерки» (США, Великобритания, Франция, Япония, Германия, Россия, Канада, Италия).

Данный международный договор закрепляет следующие основные положения:

- активное использование информационно-телекоммуникационных технологий в государственном секторе и содействие предоставлению в режиме реального времени услуг, необходимых для повышения уровня доступности власти для всех граждан;

- принятие права каждого человека на доступ к информационным ресурсам;

- невозможность создания искусственных ограничений развития сферы информационных технологий на законодательном уровне.

Принятие данной хартии стало важным шагом в развитии информационных технологий в России и свидетельствовало о развитии международного сотрудничества по вопросам информационного развития и обеспечения информационной безопасности.

2. Конституция Российской Федерации. Основной закон РФ закрепляет основы обеспечения информационного развития и защиты информации

(ст.ст 71, 79.1, 114 Конституции РФ) [1]. В частности, многие ученые-конституционалисты обратили внимание на новые редакции пунктов «и» и «м» ст. 71 Конституции РФ, устанавливающие предметы федерального ведения в системе разделения полномочий между органами государственной власти Российской Федерации и субъектами РФ. По мнению А. Г. Дейенко, данная новелла становится отправной точкой для реализации в российском законодательстве концепции цифрового суверенитета личности, дальнейшего укрепления гарантий соблюдения конституционных прав и свобод личности в киберпространстве [25].

Данные положения, на наш взгляд, отражают принципиально значимые конституционные начала о нахождении в непосредственном ведении РФ информационных технологий и оборота цифровых данных, что еще раз подчеркивает значимость информационной технологизации.

3. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ [2]. Данный документ является основным нормативным правовым актом, регламентирующим вопросы использования информации, информационных систем и защите информации от несанкционированного доступа. В частности, говоря об процессе информационной технологизации, стоит обратить особое внимание на положение п. 1 ч. 2 ст. 12 Настоящего Федерального закона, которая закрепляет особую обязанность государственных и муниципальных органов в разработке и реализации целевых программ применения достижений науки в области информационных технологий. Например, это государственная программа «Информационное общество», проводимая с 2010 по 2020 годы в целях социально-экономического развития населения при помощи информационно-коммуникационных устройств и иных технологий.

Наряду с данным Федеральным законом, на наш взгляд, крайне важно отметить Федеральный закон «О науке и государственной научно-технической политике» от 23 августа 1996 № 127-ФЗ, где глава VI.1 закрепляет основы государственной поддержки информационной деятельности. В частности, законодатель закрепляет за государством деятельность по финансированию инновационных проектов (в том числе и в сфере информационной технологизации), а также реализации научно-технической политики в разных областях [3].

В рассматриваемой области правового регулирования также включены иные нормативные правовые акты федерального законодательства, а именно: Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»[4], Федеральный закон от 9 февраля 2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [5], Федеральный закон «Об электронной подписи» от 06 апреля 2011 года № 63-ФЗ [6], Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» [7] и др.

Также стоит отметить, что в соответствии с ч. 1 ст. 11 Федерального закона Российской Федерации от 07 ноября 2011 г. № 3-ФЗ «О полиции» [8] МВД России в своей деятельности использует достижения науки и техники. Данная норма позволяет данной правоохранительной системе использовать, в том числе, и информационные технологии. Однако, к сожалению, Войска национальной гвардии России такой регламентацией не обладают, что требует соответствующих изменений в законодательстве.

4. Подзаконные нормативные правовые акты.

Их условно можно разделить на две группы:

– стандартные: например, Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [10]; Постановление Правительства РФ от 08 июня 2011 г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» [11], Письмо МВД России от 30 апреля 2019 г. № 3/197705064809 «О предоставлении информации», Указ Президента РФ от 2 марта 2022 г. № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации» [31] и так далее, то есть не имеющие никакого идейно-целевого характера юридического действия.

– концептуальные: Концепция правовой информатизации Российской Федерации 1993 г. [12], Доктрина информационной безопасности Российской Федерации 2016 г. [14], Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [13] и т.д., то есть имеющие определенную идею, выражающую стремление государства к установлению определенного порядка реализации норм в общественных отношениях.

Прогноз научно-технологического развития Российской Федерации до 2030 года включает в себя исследования в области коммуникационных систем с терабитными скоростями передачи данных, разработку новых методов биометрической идентификации, интеграции и анализа мультимодальных биометрических данных, а также создание условий для полной совместимости контента в различных сетевых средах и глобальной идентификации информационных объектов. Кроме того, предполагается разработка технологий для распознавания и анализа аудио, фото, видео и других видов медийных информационных носителей [17].

Одновременно с этим необходимо учитывать потенциальные риски и угрозы, связанные с развитием информационных технологий, которые могут оказать влияние на безопасность и стабильность информационного пространства.

В контексте анализа угроз информационной безопасности можно выделить следующие ключевые аспекты:

1. Возможность нарушения информационного обеспечения функций органов государственной власти, муниципальных образований и служб, что может повлечь за собой дестабилизацию управленческих процессов.

2. Риски перехвата и несанкционированного доступа к трансляциям телерадиовещания и системам оповещения, что может привести к распространению недостоверной информации среди населения.

3. Угроза несанкционированного доступа к управлению информационными ресурсами, что может привести к изменению или уничтожению критически важных данных.

4. Возможность целенаправленного негативного информационного воздействия на общественное сознание через средства массовой информации и интернет, что может способствовать дезинформации и манипуляции общественным мнением.

5. Ограничение прав граждан на получение достоверной информации и ее обмен, включая манипуляции массовым сознанием через информационно-психологическое воздействие.

6. Провокация социальной, межнациональной и религиозной напряженности через деятельность СМИ, в том числе электронных.

7. Распространение злоупотреблений в кредитно-финансовой сфере, связанных с проникновением в компьютерные системы и сети.

В свете указанных угроз Центральный банк Российской Федерации выражает обеспокоенность по поводу операций с виртуальными валютами, которые могут быть квалифицированы как участие в сомнительных транзакциях, противоречащих законодательству о противодействии легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма.

В контексте прогноза научно-технологического развития Российской Федерации акцентируется внимание на необходимости разработки и внедрения эффективных средств защиты компьютерных инфраструктур и программных систем для обеспечения безопасности данных в условиях эволюции информационных технологий.

Терроризм, как на внутреннем, так и на международном уровне, представляет собой одну из актуальных угроз общественному развитию, требующую комплексного подхода к противодействию на всех уровнях.

В контексте эволюции информационных технологий и усиления мер противодействия терроризму в июле 2016 года в Российской Федерации были введены нормативные акты, обязывающие операторов связи и субъектов, осуществляющих распространение информации в сети Интернет, осуществлять хранение данных пользователей и предоставлять их по запросу уполномоченных государственных органов. Для обеспечения эффективного доступа к данным была дополнена нормативно-правовая база

в сфере оперативно-разыскной деятельности нововведением, предусматривающим получение компьютерной информации в качестве оперативно-разыскного мероприятия.

Согласно обновленным положениям российского законодательства, в частности законам «О противодействии терроризму», «Об органах безопасности», «О связи», «Об информации, информационных технологиях и защите информации», операторы связи обязаны осуществлять хранение на территории Российской Федерации данных о фактах приема, передачи, доставки и обработки голосовых вызовов, текстовых сообщений, изображений, звуковых и видеозаписей, а также прочих видов сообщений, отправляемых пользователями услугами связи, в течение трехлетнего периода после завершения соответствующих операций. Данные о текстовых сообщениях, голосовых вызовах, изображениях, звуковых и видеозаписях должны храниться до шести месяцев после их приема, передачи, доставки или обработки. Предоставление этой информации уполномоченным органам, осуществляющим оперативно-разыскную деятельность или обеспечивающим безопасность Российской Федерации, является обязательным.

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

2.1. Современное состояние внедрения интеллектуальных и интегрированных систем безопасности в России

Обеспечение безопасности объектов, которые классифицируются как стратегически важные, – это их защита от потенциальных угроз террористического характера и диверсионных действий, а также возможных природных катастроф, способных нарушить их функционирование.

Для информирования, превентивных мер и устранения различных угроз, связанных с преступными действиями, разрабатываются интегрированные системы безопасности (ИСБ), представляющие собой комплекс технических подсистем, объединенных в единую информационную среду на основе общей программной платформы.

Ключевые компоненты ИСБ включают, но не ограничиваются следующими подсистемами:

- система охранно-пожарной сигнализации;
- система охранного освещения;
- система тревожной сигнализации;
- система связи;
- системы контроля и управления доступом, включая средства для проведения досмотра;
- система оповещения и управления эвакуацией, оснащенная звуковыми и световыми сигнализаторами, мониторами, световыми табло и другими устройствами;
- система защиты информации;
- система обеспечения резервного электропитания;
- система противодействия неправомерному использованию беспилотных летательных аппаратов.

Подсистемы ИСБ характеризуются не только аппаратно-программными связями, но и информационной интеграцией, что является их ключевой особенностью. Обеспечивается двусторонняя связь для оперативной передачи управленческих команд и информации. Несмотря на централизованное управление, каждая подсистема способна функционировать автономно. В зависимости от специфических требований заказчика на современном этапе разрабатываются охранные комплексы, включающие в себя разнообразные подсистемы.

Говоря о современном состоянии внедрения таких систем, стоит упомянуть ключевые:

1. Система «Безопасный город» представляет собой комплексную технологическую платформу, объединяющую различные элементы инфраструктуры для обеспечения безопасности и охраны общественного порядка в городской среде. В её состав входят видеокамеры высокой чёткости, датчики чрезвычайных ситуаций (ЧС), а также центры обработки данных (ЦОДы), которые обеспечивают сбор, хранение и анализ большого объёма информации в режиме реального времени. Благодаря интеграции этих компонентов система способна не только фиксировать происходящие события, но и проводить интеллектуальный анализ поведения людей и окружающей обстановки.

Одной из ключевых возможностей системы является распознавание конфликтных ситуаций, таких как драки, с помощью алгоритмов компьютерного зрения и анализа видео. Система анализирует жесты, скорость и направление движений участников, что позволяет оперативно выявлять признаки агрессии или насилия ещё на ранних стадиях развития инцидента. Это даёт правоохранительным органам возможность быстро реагировать, направляя патрули или специализированные подразделения к месту событий, что существенно снижает время реагирования и повышает эффективность предотвращения правонарушений.

Кроме того, «Безопасный город» обладает функциями прогнозирования чрезвычайных ситуаций природного и техногенного характера, например, наводнений, пожаров или аварий. Используя данные с датчиков ЧС и метеорологическую информацию, система анализирует риски и может заранее предупреждать соответствующие службы и население, что способствует минимизации ущерба и сохранению жизни людей. Центры обработки данных обеспечивают непрерывный мониторинг и обработку поступающей информации, позволяя принимать обоснованные и своевременные решения.

Роль системы «Безопасный город» в эффективности применения мер по охране общественного порядка заключается в значительном повышении оперативности и точности действий правоохранительных органов. Интеллектуальный анализ и автоматизация процессов мониторинга позволяют снизить нагрузку на персонал, уменьшить количество ошибок и пропущенных инцидентов, а также повысить уровень профилактики правонарушений. В результате создаётся более безопасная городская среда, где риски для граждан минимизируются, а органы правопорядка получают мощный инструмент для защиты общественного порядка в условиях динамичного и сложного городского пространства.

Система «Безопасный город» включает в себя ряд конкретных технических устройств, обеспечивающих её эффективное функционирование и высокую степень автоматизации мониторинга безопасности:

– видеокамеры наблюдения (CCTV): высокочувствительные камеры с функцией панорамирования, наклона и зума (PTZ-камеры), а также камеры

с поддержкой ночного видения и инфракрасной подсветки для круглосуточного контроля. Камеры оснащены встроенными модулями для передачи видеопотока в реальном времени;

- интеллектуальные видеокамеры с функцией видеоаналитики: устройства, способные самостоятельно распознавать ситуации, например, определять драки, подозрительные движения, оставленные предметы, а также анализировать скорость и направление движения людей.

- датчики чрезвычайных ситуаций (ЧС): различные сенсоры, включая датчики дыма, газа, температуры, уровня воды (для мониторинга наводнений), а также сейсмические датчики для обнаружения землетрясений и вибраций;

- центры обработки данных (ЦОДы): мощные серверные комплексы, обеспечивающие сбор, хранение, обработку и анализ больших объёмов информации в режиме реального времени. В ЦОДах реализуются алгоритмы искусственного интеллекта и машинного обучения для обработки видеоданных и прогноза ЧС;

- системы передачи данных: высокоскоростные каналы связи (оптоволоконные линии, беспроводные сети 4G/5G), обеспечивающие стабильную и быструю передачу информации от камер и датчиков в ЦОДы;

- интерактивные панели и рабочие станции операторов: оборудование для визуализации и управления системой, позволяющее сотрудникам правоохранительных органов оперативно получать уведомления и принимать решения;

- геоинформационные системы (ГИС): интегрированные платформы для отображения данных с камер и датчиков на цифровых картах, что облегчает локализацию инцидентов и координацию действий.

Эти технические компоненты в совокупности создают единую, многоуровневую систему, способную эффективно контролировать ситуацию в городском пространстве, своевременно выявлять и предотвращать правонарушения и чрезвычайные ситуации, тем самым значительно повышая эффективность охраны общественного порядка.

2. Система «Сфера» представляет собой комплексное решение для обеспечения общественной безопасности и охраны правопорядка за счёт высокоточной биометрической идентификации и анализа видеоданных в режиме реального времени. Основой системы являются специализированные видеокамеры с инфракрасной подсветкой, которые позволяют получать чёткое изображение лиц в условиях низкой освещённости и даже ночью. Это обеспечивает непрерывный мониторинг и распознавание лиц вне зависимости от времени суток и погодных условий.

Ключевым элементом «Сферы» является нейросетевая технология распознавания лиц, достигающая точности до 99,8%, что позволяет надёжно идентифицировать человека даже в многолюдных местах и при частичной видимости лица (например, при масках или головных уборах). Такая высокая точность минимизирует количество ложных срабатываний и

обеспечивает оперативное выявление лиц, находящихся в розыске, подозреваемых или лиц, требующих особого контроля.

Система интегрирована с единым биометрическим реестром, который объединяет базы данных МВД России, ФСБ и Росфинмониторинга. Это даёт возможность автоматически сверять распознанные лица с обширными списками правонарушителей, террористов, экстремистов и других лиц, представляющих угрозу общественной безопасности. Благодаря этому правоохранительные органы получают мощный инструмент для превентивного выявления и пресечения преступной деятельности на ранних стадиях.

В состав технических устройств системы «Сфера» входят:

- видеокамеры с инфракрасной подсветкой – обеспечивают качественное изображение лиц в любых условиях освещения;
- модули обработки видеопотока с нейросетевыми алгоритмами – специализированные вычислительные устройства (например, серверы с GPU), на которых выполняется анализ и распознавание лиц в реальном времени;
- серверные комплексы для хранения и обработки биометрических данных – обеспечивают работу единого биометрического реестра и взаимодействие с базами МВД России, ФСБ и Росфинмониторинга;
- системы передачи данных с высокой пропускной способностью – гарантируют своевременную передачу видеоданных и результатов распознавания в центры управления;
- рабочие станции операторов – оснащены специализированным программным обеспечением для мониторинга, анализа и оперативного реагирования.

Роль системы «Сфера» в эффективности охраны общественного порядка заключается в значительном повышении точности и скорости идентификации лиц, что позволяет оперативно выявлять и задерживать правонарушителей, предотвращать террористические акты и другие угрозы безопасности. Интеграция с биометрическими реестрами обеспечивает централизованный контроль и обмен информацией между различными силовыми структурами, что повышает координацию действий и снижает риски ошибок. В итоге «Сфера» способствует созданию более защищённой городской среды, где правоохранительные органы обладают современными инструментами для быстрого и точного реагирования на инциденты, существенно повышая уровень общественной безопасности.

Безусловно, перечисленные выше системы эффективны в рассматриваемой области, однако применение интегрированного подхода к разработке комплексной системы безопасности способствует достижению синергетического эффекта, обусловленного синхронным взаимодействием различных подсистем, что в свою очередь приводит к значительному усилению эффективности мер по обеспечению безопасности объектов. Интеграция интеллектуальных алгоритмов для автоматизированной

обработки данных и адекватного реагирования на разнообразные угрозы способствует эволюции систем интегрированной безопасности на принципиально новый уровень. В связи с этим актуализация и прогрессирование данных систем представляют собой важную составляющую в контексте обеспечения безопасности объектов, находящихся под эгидой органов внутренних дел Российской Федерации.

Обеспечение защиты объектов данных органов от преступных действий является сложной задачей, требующей высококвалифицированного подхода. При разработке мероприятий, направленных на усиление инженерно-технической базы и повышение уровня антитеррористической защищённости, принимаются во внимание такие факторы, как криминогенная ситуация, площадь и планировка объекта, его географическое положение, а также средства технической и инженерной защиты.

В процессе первичного анализа объекта выявляются потенциальные угрозы преступного характера. Этот этап является ключевым для разработки концептуального плана создания комплексной системы безопасности объекта.

К основным категориям угроз безопасности объекта, включающим антропогенные, техногенные и природные факторы, относятся следующие:

1. Угрозы, направленные против персонала объекта:

- физическое воздействие;
- морально-психологическое воздействие.

2. Угрозы информационным ресурсам:

- кража информации и средств её обработки (носителей);
- потеря (непреднамеренная утрата, утечка) информации;
- блокировка доступа к информации;
- уничтожение (искажение) информации;
- распространение ложной информации.

В контексте обеспечения сохранности материальных активов актуализируется спектр потенциальных угроз, включающий в себя следующие аспекты:

- акт кражи или хищения;
- умышленное или неумышленное повреждение имущества персоналом;
- преднамеренные и непреднамеренные поджоги;
- акты минирования с использованием дистанционного управления;
- повреждение конструктивных элементов зданий, мебели, ограждений, а также транспортных средств служебного и личного назначения;
- технологические аварии, природные катастрофы, пожары и другие происшествия.

Отдельное внимание уделяется новой категории угроз – неправомерному использованию беспилотных летательных аппаратов, что

может привести к угрозе жизни и здоровью граждан, а также к повреждению объектов инфраструктуры, в частности, на уровне электросетей.

Таким образом, объект подвергается множеству разнообразных угроз, которые различаются по степени серьезности и потенциальным последствиям для безопасности.

В процессе проектирования систем информационной безопасности (ИСБ) в целом, а также их отдельных подсистем, принимаются во внимание многочисленные нормативные акты, регламентирующие защиту объектов от преступных действий.

К объектам, подлежащим централизованной охране, предъявляются строгие требования, включающие в себя:

- инженерно-техническое укрепление объектов;
- обеспечение антитеррористической защищенности;
- организацию охранных рубежей;
- использование охранных извещателей;
- определение основных и резервных каналов передачи информации.

Система ИСБ должна обладать функциональными характеристиками, обеспечивающими следующие задачи:

- мониторинг потенциальных угроз;
- автоматическую обработку сигналов с адекватным реагированием на инциденты;
- аутентификацию и идентификацию;
- систематизированное ведение протоколов сообщений.

Функции ИСБ должны выполняться непрерывно, что подразумевает наличие резервных источников электропитания для обеспечения непрерывной работы оборудования системы.

В контексте эволюции угрозам криминального характера актуализируется задача разработки современных стандартов для подсистемы гарантирования резервного электроснабжения, а также для создаваемой подсистемы, направленной на противодействие неправомерному использованию беспилотных летательных аппаратов (БПЛА) в интересах национальной безопасности.

В процессе проектирования интегрированной системы безопасности объекта необходимо акцентировать внимание на подсистеме обеспечения резервного электропитания. Отказ системы основного электроснабжения влечет за собой утрату функциональности остальных технических подсистем, что делает резервирование питания критически важным.

Необходимо учитывать комплекс требований к электроснабжению оборудования, которые базируются на законодательных нормах, а также на специфических условиях эксплуатации и обслуживания системы, включая её подсистемы на конкретном объекте.

Подсистема резервного электропитания должна обеспечивать непрерывное функционирование интегрированной системы безопасности

(ИСБ) в режиме ожидания в течение не менее четырех часов. Проектирование источника бесперебойного питания и аккумуляторных батарей должно основываться на расчете общего потребляемого тока всех компонентов системы.

В случае применения аккумуляторных батарей в качестве резервного источника питания, их зарядка должна осуществляться в автоматическом режиме. Расчет потребностей в резервном электропитании должен проводиться индивидуально для каждого устройства с целью оптимизации экономических затрат на кабельную продукцию. Все системы безопасности должны функционировать в пределах допустимых колебаний напряжения в диапазоне от -15% до +10% от номинального значения.

Примером может служить автоматизированный процесс переключения системы охранно-пожарной сигнализации на резервное питание, который должен осуществляться без нарушения установленных режимов работы и функционального состояния всей системы.

Для обеспечения надежного функционирования системы резервного электропитания в современных информационных системах безопасности (ИСБ) необходимо, чтобы источник питания обладал следующими параметрами: максимальный выходной ток не должен быть менее 21 ампера, а емкость аккумуляторной батареи должна составлять не менее 13,6 ампер-часов. Важно отметить, что зарядка аккумуляторных батарей, используемых в качестве резервного источника питания, должна осуществляться в автоматическом режиме.

В контексте обеспечения безопасности объектов, подверженных потенциальным угрозам со стороны беспилотных воздушных судов (БВС), актуализируется необходимость усовершенствования подсистемы резервного электропитания. БВС представляют собой риск при использовании их для осуществления террористических актов, направленных против объектов, находящихся под охраной ведомственных структур.

Применение современных «сквозных» технологий способствует расширению функциональных возможностей БВС, что увеличивает риск использования данных аппаратов для доставки средств поражения, вывода из строя транспортных средств, блокирования объектов транспортной инфраструктуры и несанкционированного получения информации. В силу реализации указанного Правительство Российской Федерации утвердило стратегию развития беспилотной авиации Российской на период до 2030 года и на перспективу до 2035 года. Это стало безусловным шагом к развитию подобных систем противодействия БПЛА.

В свете возрастающих угроз необходимо разработать и внедрить системы, способные своевременно обнаруживать запуск и полет БВС, проводить их идентификацию и эффективно перехватывать или нейтрализовать до достижения ими поставленной задачи.

Предварительный анализ предложений, представленных российскими производителями на рынке систем безопасности, показывает, что не все из предлагаемых решений соответствуют требованиям безопасности объектов Министерства внутренних дел Российской Федерации. Разработчики в основном предлагают методы обнаружения БВС путем пеленгации сигнала между оператором и беспилотным воздушным судном, использования оптических устройств и акустических датчиков для выявления работы двигателя. Однако не учитывается возможность автономного полета БВС в режиме «радиомолчания», ограниченная эффективность оптических приборов в ночное время и влияние городского шума на точность работы акустических датчиков.

В рамках разработки систем обнаружения беспилотных воздушных средств (БВС) применяются различные подходы, среди которых преобладает использование активной радиолокационной технологии. Однако в контексте специализированных инфраструктурных проектов применение данной технологии может привести к выявлению местоположения систем обнаружения, что является их существенным недостатком. Кроме того, не все системы обладают способностью подавлять сигналы всех существующих навигационных спутниковых систем.

Неопределенность в действиях БВС, а также простота в организации запусков малогабаритных беспилотников, делают их особенно угрожающими, поскольку они могут быть использованы с минимальным предварительным планированием и практически не оставляют времени для оперативного реагирования и принятия решений о контрмере.

В связи с этим системы информационной безопасности (ИСБ) должны быть оснащены способностью к функционированию в полностью автоматическом режиме, включающем в себя последовательные этапы: обнаружение, идентификация и нейтрализация угрозы.

Таким образом, внедрение интегрированных систем безопасности (ИСБ) и их подсистем, таких как «Безопасный город» и «Сфера», позволяет значительно повысить уровень общественной безопасности и эффективность работы правоохранительных органов. Эти системы обеспечивают не только мониторинг и идентификацию угроз, но и автоматизацию процессов реагирования, что является ключевым фактором в условиях сложной внутривластной обстановки.

Актуальность разработки и внедрения современных стандартов для различных подсистем, включая резервное электроснабжение и противодействие неправомерному использованию беспилотных летательных аппаратов, подтверждается растущими вызовами, связанными с угрозами криминального характера. Эффективная реализация таких систем требует тщательного анализа потенциальных угроз, а также адаптации существующих технологий к специфическим условиям эксплуатации.

Создание многоуровневой системы безопасности, основанной на интеграции различных технических решений и интеллектуальных алгоритмов, является необходимым шагом к обеспечению надежной защиты объектов, находящихся под охраной органов внутренних дел Российской Федерации. В дальнейшем для повышения эффективности ИСБ необходимо продолжать исследование и разработку новых технологий, а также совершенствовать существующие подходы к управлению безопасностью, что позволит минимизировать риски и обеспечить стабильное функционирование критически важных объектов в условиях современных вызовов.

2.2. Перспективы повышения эффективности применения информационных технологий в охране общественного порядка и обеспечении общественной безопасности на территориях, присоединенных к Российской Федерации

Состояние общественного порядка на присоединённых к Российской Федерации территориях характеризуется как этап формирования и стабилизации, сопровождающийся комплексом специфических вызовов и задач. В первые периоды интеграции наблюдается необходимость установления эффективной системы правопорядка, адаптированной к местным условиям и особенностям социально-экономической и политической ситуации.

Особое внимание уделяется обеспечению безопасности граждан, защите прав и свобод населения, а также предотвращению возможных проявлений преступности и экстремизма, которые могут возникать в условиях переходного периода. Важным элементом является интеграция местных правоохранительных структур в единую систему органов внутренних дел Российской Федерации, что предполагает унификацию нормативно-правовой базы, повышение квалификации кадров и внедрение современных технологий обеспечения общественной безопасности.

К сожалению, на данный момент нет доступа к оперативным статистическим данным за последние полгода по правонарушениям на присоединённых к Российской Федерации территориях.

Однако на основании общедоступной информации и анализа типичных ситуаций в подобных регионах можно выделить следующие наиболее часто встречающиеся виды правонарушений:

1. Мелкие хулиганства – связаны с социальными и экономическими трудностями переходного периода. На фоне социально-экономической нестабильности и адаптации к новым административным условиям на этих территориях нередко возникают конфликты на бытовой почве, которые перерастают в мелкие хулиганские действия. Это могут быть драки, нарушения общественного порядка в местах массового скопления людей,

порча имущества. Например, в первые месяцы после присоединения на некоторых территориях фиксировались случаи массовых уличных конфликтов, связанных с протестными настроениями или недовольством местного населения изменениями в управлении.

2. Кражи и иные преступления против собственности – обусловлены нестабильностью и адаптацией местного населения к новым условиям. Переходный период часто сопровождается ростом имущественных преступлений: краж, грабежей, мошенничества. Нестабильность и неопределённость в экономической сфере создают благоприятные условия для таких преступлений. Например, в отдельных населённых пунктах фиксировались случаи краж из магазинов и частных домов, что связано с ухудшением уровня жизни и снижением эффективности работы правоохранительных органов на начальном этапе интеграции.

3. Нарушения миграционного законодательства – в связи с перемещением населения и изменением административного контроля. Присоединение территорий сопровождается изменением миграционного режима, что вызывает сложности с учётом и контролем перемещения населения. Нередко возникают случаи незаконного пребывания, работы без разрешений, фиктивной регистрации. Например, были выявлены группы лиц, пытавшихся использовать новые административные лазейки для нелегальной трудовой деятельности или для обхода санкций.

4. Экстремистские проявления и попытки дестабилизации – встречаются в отдельных случаях, что требует повышенного внимания правоохранительных органов. В условиях изменения политического статуса территорий возможны попытки дестабилизировать ситуацию через экстремистские действия, пропаганду, распространение запрещённой информации. Правоохранительные органы уделяют повышенное внимание выявлению и пресечению таких проявлений. Примером могут служить случаи задержания лиц, распространявших экстремистские материалы или призывы к нарушению общественного порядка.

Говоря о современном состоянии процесса внедрения информационных технологий в процесс охраны общественного порядка на присоединённых к РФ территориях, стоит сказать, что на законодательном уровне было утверждено создание интегрированной информационно-аналитической системы, которая является ключевым элементом для увеличения результативности работы правоохранительных структур. Процесс информатизации охватил все направления работы, начиная от оперативных отделов и заканчивая кадровой службой и службой обеспечения. Каждый сотрудник органов внутренних дел обязан не только владеть профессиональными умениями и навыками, но и обладать базовыми знаниями в области цифровых технологий. Это включает в себя умение работать с электронными документами, знание принципов информационной безопасности

и использование электронной почты в рамках своей профессиональной деятельности [26].

На период до 2024 года было запланировано проведение научных исследований, которые привели к разработке рекомендаций для улучшения законодательства в сфере использования цифровых технологий в работе правоохранительных органов. Усовершенствование законодательной основы в сочетании с методической поддержкой и обучением высококвалифицированных специалистов позволит внести значительные изменения в использование цифровых решений в повседневной работе правоохранительных органов.

На четвертой научно-практической конференции, посвященной применению искусственного интеллекта в полиции, которая состоялась 25 мая 2022 года в Московском университете МВД России, особое внимание было уделено вопросам внедрения машинного оборудования в профессиональную деятельность сотрудников полиции. Профессиональное образование специалистов в этой области продолжает оставаться ключевым направлением [27].

На наш взгляд, стоит коснуться рассмотрения перспектив применения систем искусственного интеллекта в обеспечении общественной безопасности непосредственно в правоохранительном ключе.

24 ноября 2023 года В. В. Путин в своем выступлении на международной конференции «Путешествие в мир искусственного интеллекта» подчеркнул значимость внедрения искусственного интеллекта в различные сферы общественной жизни, заявив, что «в будущем Россия должна стать одной из самых комфортных юрисдикций в мире для развития нейросетей» [28]. Собственно, основным нормативным правовым актом, регламентирующим процесс развития нейросетей в современной России, является «Национальная стратегия развития искусственного интеллекта до 2030 года», утвержденная указом Президента России № 490 от 10 октября 2019 г. [15]. Данный документ содержит мало норм, непосредственно касающихся именно МВД России, однако на некоторых все же стоит акцентировать внимание.

В главе III п.п. «б» п.19 настоящего указа закреплён в качестве один из основных принципов внедрения систем искусственного интеллекта (ИИ) – принцип безопасности. Данный принцип предполагает собой недопустимость со стороны потенциальных правонарушителей использования ИИ в противоправных целях: например, для причинения вреда гражданам и организациям, права и законные интересы которых охраняются данной Стратегией; неправомерного доступа к информации ограниченного доступа, в том числе касающейся сведений, содержащих государственную тайну или любые персональные данные. Данное положение свидетельствует о приоритетности внедрения систем искусственного интеллекта в систему МВД России, так как все

вышеперечисленное, на наш взгляд, служит еще одним законодательным средством реализации положения п. 1 ч. 1 ст. 1 Федерального закона «О полиции», закрепляющего основным направлением деятельности полиции защиту личности, общества и государства от противоправных посягательств.

Помимо этого, стоит отметить, что п.п. «е» п. 23 упомянутого указа Президента РФ в качестве основной задачи развития искусственного интеллекта в Российской Федерации закрепляет обязательное внедрение доверенных технологий искусственного интеллекта в тех областях его использования, в которых может быть нанесен ущерб безопасности Российской Федерации, в том числе – национальной безопасности, оптимальное состояние защищенности которой обеспечивается путем осуществления полномочий должностными лицами органов предварительного следствия, оперативно-розыскных подразделений органов внутренних дел и органов дознания.

Сегодня в научно-технической разработке искусственного интеллекта в ОВД РФ тестируется множество разнообразных проектов, однако, следует выделить самые перспективные из всех.

В 2023 году заместитель министра внутренних дел В. Д. Шулика утвердил план по внедрению технологий ИИ в деятельность МВД России на 2023-2025 годы. Крупнейшими разработками среди них являются проекты «Клон» и «Конъюнктура». Остановимся на каждом более подробно [29].

«Клон» – это система искусственного интеллекта, главной задачей которого является проверка подлинности изображений, видеозаписей. В частности, стоит отметить, что данная система будет очень полезна для выявления фальсификаций и манипуляций с визуальными материалами, которые в соответствии со ст. 26.2 КоАП РФ являются доказательствами [9].

Система использует различные алгоритмы и методы анализа, такие как:

1. Анализ метаданных: изучение информации о файле, включая дату и время создания, модель камеры, настройки съемки и другие параметры, которые могут помочь определить подлинность.

2. Сравнительный анализ: сравнение исследуемого изображения или видео с оригинальными источниками для выявления несоответствий.

3. Обнаружение артефактов: выявление следов редактирования, таких как неестественные тени, измененные цвета или несоответствия в текстах.

4. Искусственный интеллект и машинное обучение: применение нейронных сетей для обучения на больших объемах данных, что позволяет системе распознавать паттерны, характерные для поддельных изображений и видео.

5. Интерактивная проверка: использование технологий интерактивной проверки для анализа более сложных манипуляций, таких как «deep fakes», где лица и голоса изображаемого человека могут быть подменены.

Говоря об использовании данной системы в деятельности по охране общественного порядка, стоит отметить, что ее функции могут значительно оптимизировать деятельность правоохранительных органов в производстве административного расследования в порядке ст. 28.7 КоАП РФ. Особенно актуально применение системы ИИ «Клон» для проверки материалов по делам о нарушениях законодательства в сфере использования средств массовой информации: например, злоупотребление свободой массовой информации (ст.13.15 КоАП РФ), что по сути является проявлением экстремизма в современных условиях и направлено на дискредитацию Вооруженных сил РФ, что требует соответствующего реагирования.

При расследовании данных правонарушений «Клон» выступит средством оперативного анализа видеоматериалов, изображений, изготовленных и (или) распространенных теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также относящихся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки информационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье.

Система ИИ «Конъюнктура» призвана прогнозировать негативные события и чрезвычайные ситуации, а также моделировать сценарии реагирования на них. В правоохранительной деятельности органов внутренних дел данная система будет достаточно актуальна. Например, данная система может использоваться в деятельности по предупреждению преступлений, а именно: исходя из данных о личности, позволит прогнозировать его возможную модель поведения и выстраивать сценарии реагирования; ссылаясь на текущее состояние общественного порядка может показать, какие районы присоединенных территорий требуют усиленного режима несения службы со стороны подразделений ППСП, а также патрульных ФСВНГ РФ, что снизит риск совершения новых преступных или антиобщественных поведений. Также стоит сказать, что данная система позволит прогнозировать динамику как общей преступности, так и ее отдельных видов. Следует отметить, что нейросети сегодня тестируются в деятельности сотрудников полиции для фиксации административных правонарушений в области дорожного движения.

Из всего вышесказанного следует вывод, что использование нейросетей в органах внутренних дел является очень актуальным направлением деятельности правоохранительных органов. Несмотря на то, что на данный момент эта технология в основном на практике использует такую область действия, как распознавание, ее возможности будут гораздо шире, однако даже в таком формате это значительно облегчает работу органов внутренних дел.

Внедрение в деятельность органов внутренних дел по обеспечению общественной безопасности и охране общественного порядка систем

искусственного интеллекта имеет определенные организационные и правовые проблемные аспекты.

Во-первых, законодательное определение данного явления отсутствует в нашей стране, что можно выделить в качестве первой проблемы в области правового регулирования технологий искусственного интеллекта. В Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг. искусственный интеллект назван в числе основных направлений развития российских информационных и коммуникационных технологий [16]. В Программе «Цифровая экономика Российской Федерации», а также в Национальной программе «Цифровая экономика Российской Федерации» искусственный интеллект перечислен среди основных сквозных технологий, применяемых в различных сферах общественной жизни. Несмотря на это, системы искусственного интеллекта уже используются во многих областях общественной жизни, а законодатель до сих пор не предпринял никаких попыток закрепить внедрение систем ИИ на правовом уровне, что ставит под вопрос законность внедрения данных систем не только в ОВД, но и в других областях.

Во-вторых, организационный аспект заключается в том, что в современном мире, где технологии развиваются с невероятной скоростью, особенно остро стоит вопрос подготовки квалифицированных специалистов в области информационных технологий. Особое внимание следует уделить подготовке юристов, обладающих необходимыми знаниями и навыками для решения сложных правовых задач, возникающих в контексте регулирования искусственного интеллекта. Это направление требует особого внимания, поскольку именно юристы, специализирующиеся на IT-праве, способны обеспечить правовую защиту и регулирование в этой быстро меняющейся сфере [30].

Следовательно, в-третьих, необходимо активизировать усилия по расширению образовательных программ в области юриспруденции, включая внедрение специализированных курсов и направлений, таких как IT-LAW. Это позволит студентам, обучающимся не только в престижных столичных университетах, но и в учебных заведениях регионального уровня, получить актуальные знания и компетенции, необходимые для успешной профессиональной деятельности в области права информационных технологий.

Таким образом, акцент на развитие и внедрение специализированных образовательных программ по IT-LAW не только повысит уровень подготовки будущих специалистов в области юриспруденции, но и внесет значительный вклад в создание правовой базы, способной адекватно реагировать на вызовы, связанные с развитием искусственного интеллекта и других инновационных технологий.

Также стоит внести конкретные предложения по внедрению или замене технического обеспечения рассматриваемой области.

В рамках бюджетного ассигнования на 2024 год предусмотрено выделение средств в размере 106,2 миллиарда рублей на реализацию государственной программы «Безопасный город». Для последующих годов, а именно 2025 и 2026, предусмотрены финансовые планы с объемами финансирования в 98,2 миллиарда рублей и 100,5 миллиарда рублей, соответственно.

Как уже было упомянуто ранее, система «Безопасный город» включает в себя систему интеллектуального видеонаблюдения. В Москве и Санкт-Петербурге чаще всего используются такие видеосерверы, как NVR (Network Video Recorder) и VMS (Video Management System). Данные системы накапливают видеоинформацию большого объема, что позволяет сохранить видеоданные за достаточно большой период времени (чаще всего от 1 года до 3 лет с учетом экономного способа расходования). Стоимость данного оборудования на современном рынке превышает 200 т. р. Безусловно, для городов федерального значения такие устройства необходимы, однако если мы говорим о присоединенных территориях, то на наш взгляд, есть возможность сэкономить государственный бюджет посредством внедрения в новые регионы менее дорогостоящих видеосерверов.

Видеосерверы Domination предлагают различные модели для подключения IP-камер, включая решения на 9, 24, 32 и 128 каналов. Эти устройства обеспечивают высокую совместимость с камерами разных производителей и подходят для различных систем видеонаблюдения. Их цена в 1,5 раза меньше тех, которые используются в городах федерального значения и, соответственно, в перспективе внедрить такие видеосерверы в города присоединенных к РФ территорий в целях экономии государственного бюджета и использования новых информационных систем, которые будут выполнять практически такие же функции, что и те, которые используются в городах федерального значения (рис. 1).



Рис. 1. Внешний вид видеосервера Domination

ЗАКЛЮЧЕНИЕ

В заключение, перспективы применения информационных технологий, в частности систем искусственного интеллекта, в охране общественного порядка и обеспечении безопасности на территориях, присоединенных к Российской Федерации, представляют собой важное направление для развития правоохранительных органов.

Правовое положение территорий, присоединенных к Российской Федерации, представляет собой сложный и многогранный вопрос, требующий внимательного анализа и дальнейшего изучения. В условиях текущих геополитических реалий и продолжающихся военных действий правовой статус граждан, проживающих на этих территориях, становится особенно актуальным. Введение военного положения и переходного периода создает специфические условия, в которых права и обязанности жителей новых субъектов адаптируются к законодательству Российской Федерации, однако сохраняют некоторые особенности, связанные с прежним правовым режимом.

Современное состояние внедрения интеллектуальных и интегрированных систем безопасности в России демонстрирует значительный прогресс в обеспечении общественной безопасности и охраны правопорядка. Системы, такие как «Безопасный город» и «Сфера», представляют собой комплексные решения, которые, благодаря высокотехнологичным компонентам и интеграции с биометрическими реестрами, обеспечивают оперативное выявление и реагирование на угрозы. Высокая точность идентификации и автоматизация процессов мониторинга позволяют правоохранительным органам эффективно справляться с вызовами, связанными с террористическими угрозами и преступной деятельностью.

Однако, несмотря на достигнутые успехи, необходимо учитывать постоянно эволюционирующие угрозы, такие как использование беспилотных летательных аппаратов, и соответствующим образом адаптировать системы безопасности. Важно, чтобы интегрированные системы обладали достаточной гибкостью и мощностью для автоматического обнаружения и нейтрализации новых типов угроз.

Дальнейшее развитие и совершенствование интегрированных систем безопасности, включая их технические и организационные аспекты, является критически важным для повышения уровня защиты стратегически важных объектов и обеспечения безопасности граждан в условиях быстро меняющейся обстановки. Интеграция интеллектуальных алгоритмов и автоматизация процессов будут способствовать созданию более безопасной городской среды, где правоохранительные органы смогут эффективно выполнять свои функции и обеспечивать защиту общественного порядка.

Федеральные конституционные законы, определяющие порядок интеграции новых территорий, демонстрируют стремление к обеспечению прав граждан и их социальной защиты. Тем не менее, необходимо учитывать, что правовой статус этих граждан может быть охарактеризован как специальный административно-правовой, учитывая введенные ограничения и особенности правового регулирования.

Внедрение таких технологий, как системы «Клон» и «Конъюнктура», может значительно повысить эффективность работы МВД России, способствуя более точному анализу и прогнозированию правонарушений, а также оперативному реагированию на них. Однако, несмотря на очевидные преимущества, существует ряд организационных и правовых проблем, включая отсутствие четкого законодательного регулирования в сфере использования ИИ. Это подчеркивает необходимость разработки специализированных образовательных программ в области IT-права для подготовки квалифицированных специалистов, способных решать возникающие правовые задачи. Кроме того, оптимизация бюджетных расходов на техническое обеспечение правоохранительных органов, в том числе использование более доступных технологий видеонаблюдения, может стать ключевым фактором в эффективном внедрении информационных систем на новых территориях.

Таким образом, комплексный подход к внедрению информационных технологий, включая правовое регулирование, подготовку кадров и оптимизацию ресурсов, способен существенно улучшить состояние общественной безопасности в России.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный текст Конституции РФ, включающий новые субъекты Российской Федерации - Донецкую Народную Республику, Луганскую Народную Республику, Запорожскую область и Херсонскую область, опубликован на Официальном интернет-портале правовой информации // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

2. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

3. О науке и государственной научно-технической политике : Федеральный закон от 23 августа 1996 г. № 127-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

4. О связи : Федеральный закон от 07 июля 2003 г. № 126-ФЗ (ред. от 08.08.2024) (с изм. и доп., вступ. в силу с 01.09.2024) // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

5. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления : Федеральный закон от 09 февраля 2009 г. № 8-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

6. Об электронной подписи : Федеральный закон от 06 апреля 2011 г. № 63-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

7. О коммерческой тайне : Федеральный закон от 29 июля 2004 г. № 98-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

8. О полиции: Федеральный закон от 07 февраля 2011 г. № 3-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

9. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 декабря 2001 г. № 195-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

10. Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме : постановление Правительства Российской Федерации от 08 июня 2011 г. № 451

// Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

11. О Концепции правовой информатизации России : указ Президента Российской Федерации от 28 июня 1993 г. № 966 // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

12. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

13. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 05 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

14. Национальная стратегия развития искусственного интеллекта на период до 2030 года : указ Президента Российской Федерации № 490 от 10 октября 2019 г. – URL: <http://www.kremlin.ru>.

15. Стратегия развития информационного общества в Российской Федерации на 2017-2030 гг. : указ Президента Российской Федерации от 09 мая 2017 г. № 203 // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.

16. Прогноз научно-технологического развития Российской Федерации на период до 2030 года – Москва, 2013. – URL: <http://government.ru>.

17. Окинавская хартия глобального информационного общества от 21 июля 2000 г. – URL: <http://www.kremlin.ru>.

18. Андреева С. И. Правовой статус военнослужащего в условиях Специальной военной операции // Вестник магистратуры. – 2022. – № 11-2 (134). – С. 69–70.

19. Неверов А. Я. Военная служба в Российской Федерации в период проведения Специальной военной операции // Заметки ученого. – 2023. – № 10. – С. 32–36.

20. Бахрах Д. Н., Российский Б. В., Стариков Ю. Н. Административное право : учебник для вузов. – Москва : Норма, 2005. – 800 с.

21. Пастухов П. С. Правовые аспекты использования информационных технологий для обеспечения общественной безопасности и общественного порядка // Вестник Прикамского социального института. – 2016. – № 3(75). – URL: <https://cyberleninka.ru/>.

22. Ловцов Д. А., Ниесов В. А. Актуальные проблемы создания и развития единого информационного пространства судебной системы России // Информационное право. – 2013. – № 5. – С. 13–18.

23. Дейнеко А. Г. Информационно-правовой комментарий к поправкам в Конституцию Российской Федерации // Труды по интеллектуальной собственности. – 2021. – Т. 37, № 1/2. – С. 9–10.

24. Мантуров О. С., Ганага В. С. Формирование цифровой компетентности у сотрудников полиции // Полицейская деятельность. – 2020. – № 5.

25. Виталий Шулика принял участие в Межведомственной научно-практической конференции «Искусственный интеллект на службе полиции». – URL: <https://мвд.рф/>.

26. Путешествие в мир искусственного интеллекта : конференция. – URL: <http://www.kremlin.ru>.

27. Клон и Конъюнктура: МВД РФ анонсировало внедрение ИИ в правоохранительную деятельность к 2025 году. – URL: <https://www.securitylab.ru>.

28. Козлов Д. В. Развитие юридической профессии в контексте роботизации. Анализ ситуации и прогноз на будущее / Тарасова А. Е. Европейская Конвенция по правам человека (ЕКПЧ) и Российское прав. 20 лет вместе. Бизнес и права человека в условиях цифровой экономики, искусственного интеллекта, новых международных вызовов : сборник статей. – Москва : Русайн, 2018. – С. 157.

29. URL:<https://www.consultant.ru>.

30. URL:<https://pravo.gov.ru>.

Учебное издание

Евгения Михайловна Абросимова

Сергей Анатольевич Гречаный

Ольга Владимировна Толстых

Дарья Алексеевна Сошнев

Юлия Сергеевна Никитина

**ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
В ОХРАНЕ ОБЩЕСТВЕННОГО ПОРЯДКА
И ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ
НА ТЕРРИТОРИЯХ, ВНОВЬ ПРИСОЕДИНЕННЫХ В СОСТАВ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Методические рекомендации

В авторской редакции

Компьютерный набор Д. А. Сошневой

Объем 0,6 МБ

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