Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра административного права, административной деятельности и
управления органами внутренних дел

ДИПЛОМНАЯ РАБОТА

на тему: «Использование современных информационно-телекоммуникационных систем в деятельности полиции»

Выполнил:
Коротков Владислав Сергеевич
(фамилия, имя, отчество)

40.05.02 - Правоохранительная деятельность,
набор 2019 г., 393 учебная группа
(специальность, год набора, № группы)

Руководитель:
кандидат юридических наук, старший
преподаватель кафедры административного
права, административной деятельности и
управления ОВД, майор полиции
(ученая степень, ученое звание, должность)

Кормильцева Светлана Олеговна
(фамилия, имя, отчество)

Рецензент:
Зам. командира ОСБ ДПС Госавтоинспекции
МВД по Республике Марий Эл
подполковник полиции
(должность, специальное звание)

Чемис Дмитрий Викторович
(фамилия, имя, отчество)

Дата защиты: «___» _____2025 г. Оценка_____

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы. Цифровизация общественной и государственной сферы изменила методы и формы функционирования практически всех институтов власти, включая органы внутренних дел. В современных условиях обеспечение общественного порядка, раскрытие преступлений, противодействие экстремизму и терроризму невозможны без применения информационно-телекоммуникационных систем (ИТКС), способных обеспечивать оперативность, точность и масштабируемость полицейской деятельности. Развитие технологий, таких как искусственный интеллект, автоматическая видеоаналитика, биометрическая идентификация, системы мониторинга и прогнозирования, трансформирует содержание оперативно-служебной работы и требует постоянного совершенствования подходов к обеспечению правопорядка.

Согласно данным МВД России, в 2023 году количество преступлений, зарегистрированных с использованием ИТК-технологий, превысило 580 тыс. случаев, что составило более 30 % от всех преступлений экономической направленности. Параллельно продолжилось расширение применения ИТКС в деятельности органов внутренних дел. Например, система «Безопасный город» функционировала в более чем 80 субъектах РФ, охватывая свыше 1,3 млн. камер видеонаблюдения, в том числе более 800 тыс. с функцией распознавания лиц. Единая база данных МВД в 2024 году содержала свыше 6 млрд. единиц информации, включая биометрические и поведенческие параметры, что позволяет в режиме реального времени отслеживать перемещения подозреваемых и анализировать оперативную обстановку[1].

В то же время, по отчётам Счетной палаты и Росфинмониторинга, остаются проблемы, связанные с неравномерностью цифрового оснащения на

[1] Краткая характеристика состояния преступности / Официальный сайт МВД России. Статистика ГИАЦ МВД России. URL: https://www.mvd.ru/Dejatelnost/statistics/reports/ (дата обращения: 20.06.2025).

уровне территориальных отделов МВД, недостаточной защищённостью информации и отсутствием единого протокола межведомственного обмена данными. По итогам проверки 2023 года, более 27 % сотрудников органов внутренних дел отметили затруднения в использовании специализированных ИТК-систем из-за отсутствия должной подготовки, что снижает потенциал цифровых инструментов в повседневной деятельности полиции[1].

Использование ИТКС в деятельности полиции основывается на правовых нормах, технических регламентах и межведомственных соглашениях, регулирующих сбор, обработку, хранение и защиту информации. Современные цифровые платформы позволяют формировать межведомственные базы данных, автоматизировать процедуры реагирования на правонарушения, отслеживать маршруты потенциальных преступников и анализировать поведенческие паттерны на основе больших данных. Вместе с тем наблюдаются трудности, связанные с фрагментарностью ИТ-инфраструктуры, ограничениями в ресурсах, несовершенством нормативной базы и отсутствием единой архитектуры электронного взаимодействия.

Углубление цифровизации государственных институтов требует модернизации вычислительных и телекоммуникационных платформ, способных обеспечивать комплексную поддержку оперативно-служебной деятельности. Применение информационных решений создаёт возможности для повышения результативности административных функций, выполняемых структурами системы внутренних дел. При этом эффективность взаимодействия между территориальными управлениями МВД России во многом зависит от состояния применяемых цифровых средств и юридической определённости процедур их внедрения и эксплуатации.

Таким образом, актуальность выбранной темы обусловлена необходимостью научного осмысления роли информационно-телекоммуникационных систем в системе обеспечения общественной

[1] Информационные сообщения / Официальный сайт Росфинмониторинга. URL: https://www.fedsfm.ru/releases/7185 (дата обращения: 20.06.2025).

безопасности, анализа их влияния на эффективность деятельности полиции, а также выявления организационных и правовых барьеров, препятствующих полноценному использованию современных цифровых решений.

Степень изученности темы исследования. Основы применения современных информационных технологий в деятельности полиции отражены в работах Б.В. Андреева, М.В. Анисифоровой, А.М. Воронова, А.В. Гусева, В.Н. Долинина, И.П.Иванова, В.В. Казакова, И.И. Кирюшина, М.И. Климовой, Я.В. Комельковой, Н.Г. Лабутина, А.Ф. Остряковой, Б.В. Рудакова, В.В. Тимофеева, С.А. Чернякова, Е.Р. Шиковой и др. Труды указанных авторов позволили нам проанализировать использование современных информационно-телекоммуникационных систем в деятельности полиции, выявить их особенности и недостатки.

Объектом исследования выступает деятельность ОВД в цифровой среде по использованию современных информационно-телекоммуникационных систем.

Предметом исследования являются современные информационно-телекоммуникационные системы, используемые в оперативно-служебной и административной деятельности полиции.

Цель дипломной работы - изучение теоретических, правовых и прикладных условий использования информационно-телекоммуникационных систем в деятельности полиции и разработка направлений их совершенствования.

Для достижения сформулированной цели в работе сделана попытка решения следующих основных **задач:**

1) раскрыть понятие и классифицировать информационно-телекоммуникационные системы;

2) изучить компоненты информационной системы органов внутренних дел;

3) проанализировать аравовое регулирование использования информационно-коммуникационных технологий в деятельности полиции;

4) рассмотреть Единую систему информационно-аналитического обеспечения деятельности МВД России;

5) охарактеризовать сервис электронного документооборота;

6) изучить подсистема информационной безопасности;

7) рассмотреть работу федеральной информационной системы Государственной инспекции безопасности дорожного движения МВД России;

8) проанализировать перспективные направления интеграции в процесс охраны общественного порядка и обеспечения общественной безопасности инновационных информационно-телекоммуникационных систем;

9) теоретически обосновать перспективные направления развития единой системы информационно-аналитического обеспечения деятельности МВД России.

Теоретическую основу исследования составили труды ученых в области использование современных информационно-телекоммуникационных систем в деятельности полиции.

Методологическую основу исследования составил диалектический подход к научному познанию общественных отношений, складывающихся при использовании современных информационно-телекоммуникационных систем в деятельности полиции, анализ выявленных факторов, синтез результатов, полученных в ходе исследования, позволивший представить предложения об эффективности использования информации, содержащейся в прикладных сервисах информационно-телекоммуникационных МВД России. К числу специальных методов, примененных в исследовании, относятся метод исследования нормативных правовых актов и документов, метод эмпирического обобщения данных, метод обработки и анализа данных.

Нормативно-правовую базу исследования составляют Конституция РФ, федеральные законы, в частности федеральный закон от 07.02.2011 № 3-ФЗ «О полиции», подзаконные акты МВД России, международные соглашения в сфере информационной безопасности, а также Стратегия цифровой трансформации МВД России до 2030 года и иные подзаконные акты.

Эмпирическая основа исследования - нормативно-правовые акты Российской Федерации, информация, доступная из публикаций, указанных в списке использованной литературы, материалы опроса сотрудников МВД России.

Научная новизна работы выражается в систематизации подходов к внедрению ИТКС в полицейскую деятельность, формировании типологии цифровых решений и обосновании проектных направлений их совершенствования. Предложены меры по расширению использования информационно-телекоммуникационных систем в работе МВД России, с целью оптимизации организации и выполнения регулярных и оперативных задач, выполняемых сотрудниками данного ведомства.

Теоретическая значимость работы заключается в глубоком и системном анализе вопросов использования современных информационно-телекоммуникационных систем в деятельности полиции. Особое внимание уделяется исследованию сервисов Единой системы информационно-аналитического обеспечения деятельности МВД России.

Практическая значимость исследования заключается в возможности использования предложений дипломной работы в процессах реформирования цифровой архитектуры МВД, а также в повышении прозрачности и оперативности взаимодействия полиции с гражданами и иными органами власти.

Структура работы. Дипломная работа состоит из введения, трех глав, разбитых на девять параграфов, заключения, списка использованной литературы и приложений. В первой главе раскрыты теоретико-правовые основы применения информационно-телекоммуникационных систем в органах внутренних дел. Во второй главе осуществлен анализ практики применения информационно-телекоммуникационных систем в деятельности полиции. В третьей главе раскрыты перспективы развития и совершенствования информационно-телекоммуникационных систем в деятельности полиции.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ПОЛИЦИИ

§1. Понятие и классификация информационно-телекоммуникационных систем

Современные подходы к управлению в различных отраслях основываются на систематическом применении цифровых решений. Выполнение аналитических операций, плановых мероприятий, контрольных процедур и итоговой оценки требует функционирования компьютерных систем. Повышенная изменчивость общественных процессов предопределяет необходимость перехода к управлению нового типа, при котором используется обработка значительного объема данных о внутренней и внешней среде, моделируются вероятные сценарии развития и реализуются оперативные меры реагирования. В условиях высокой неопределенности полагаться исключительно на субъективный опыт руководителя или ограниченные ресурсы оказывается недостаточно. Такая ситуация характерна и для организации работы органов внутренних дел, где сложность управленческих задач требует интеграции информации из различных направлений служебной деятельности: от следственных операций до мониторинга патрульных маршрутов. Учет факторов риска и нестабильности предполагает применение технологических решений, обеспечивающих точность и оперативность управленческих процессов. Использование информационно-телекоммуникационных систем позволяет повысить результативность контроля, координации и оценки правоохранительных мероприятий. Эффективное функционирование таких систем зависит от уровня технической оснащённости и структурированной системы информационного сопровождения управленческих процессов.

Отметим, что «ОВД имеют сложную структуру и включают в себя много элементов для выполнения различных функций. Они представлены многоуровневой системой и имеют обширные связи как внутри, так и снаружи системы. Управление этими системами требует регулирования работы так отдельных элементов, так и всей системы в целом. Управление направлено на достижение целей, которые стоят перед системой, создание условий для их выполнения, обеспечение устойчивости структуры и эффективного функционирования, поддержание установленного режима деятельности, сохранение или формирование качественных особенностей системы и выполнение заданных программ работы»[1].

Изучение теории и практики информационных процессов основывается на использовании технических средств для получения информации, сбора их данных, регистрации и передачи по телекоммуникационным каналам. «Информатика определяет правила преобразования информации в автоматизированных системах, разрабатывает методы для алгоритмизации информации, создания языковых средств для общения между человеком и компьютером. Кроме того, информатика и ее подразделы – компьютерные науки, информационные технологии, кибернетика – являются основой для разработки и применения различных интеллектуальных систем, в том числе искусственного интеллекта. Важным направлением развития информатики является оптимизация информационных процессов с целью повышения эффективности и качества работы автоматизированных систем в различных сферах деятельности человека. В этом контексте информатика работает над разработкой новых методов обработки и анализа информации, а также созданием новых программных и аппаратных средств для автоматизации и оптимизации технологических процессов»[2].

---

[1] Маркушин А.Г. Основы управления в органах внутренних дел: учеб. для СПО / А.Г. Маркушин, В.В. Казаков. – 3-е изд., перераб. и доп. – М.: Юрайт, 2020. – С.37.
[2] Там же. С.38.

«Автоматизация – это комплекс мер и действий технического, организационного и экономического характера, которые могут уменьшить или полностью исключить необходимость участия человека в выполнении функций производственных процессов или управления. Автоматизированная информационная система (далее – АИС) – это система, которая создана с применением автоматизации и предназначена для обработки и передачи информации. АИС представляет собой совокупность компьютерной технологии и оператора, которые работают совместно для получения необходимой информации. Она используется для обеспечения информационной поддержки специалистов и оптимизации управления в различных областях жизнедеятельности. Такие системы дают возможность проводить расчеты с разными вариантами, принимать разумные управленческие решения в режиме реального времени, организовывать комплексный учет и анализ, гарантировать достоверность и быстроту доступа к информации, используемой для управления, и многое другое»[1].

Следующие обстоятельства подтверждают обоснованность приведённого утверждения:

- внедрение автоматизированных механизмов обработки документации, в том числе в среде электронных систем документооборота;

- создание специализированных автоматизированных информационных решений, адаптированных к конкретным видам профессиональной деятельности;

- интеграция вычислительной техники и средств телекоммуникации в структуру управления как неотъемлемых компонентов современных организационно-административных моделей[2].

---

[1] Ковалев А.Н. Информационные технологии в правоохранительных органах / А.Н. Ковалев. – М.: Юрайт, 2020. – С.86.

[2] Острякова А.Ф., Митряев И.С. Использование современных технологий в правоохранительных органах / А.Ф. Острякова и др. // Аграрное и земельное право. – 2023. – № 7(223). – С. 60.

Функциональное содержание автоматизированных информационных систем поддаётся структуризации и может быть представлено через совокупность взаимосвязанных компонентов (рис. 1).

Автоматизированная информационная технология формируется на основе совокупности функциональных направлений, каждое из которых определяет отдельный элемент её внутренней организации. В структуру такой технологии входят операции по получению и фиксации сведений, подготовке информационных массивов, их обработке, сохранению в базах данных, а также формированию итоговых сведений. Дополнительно предусматривается передача первичных данных к вычислительным модулям и доставка итогов анализа ответственным лицам, принимающим решения в управленческом контуре.

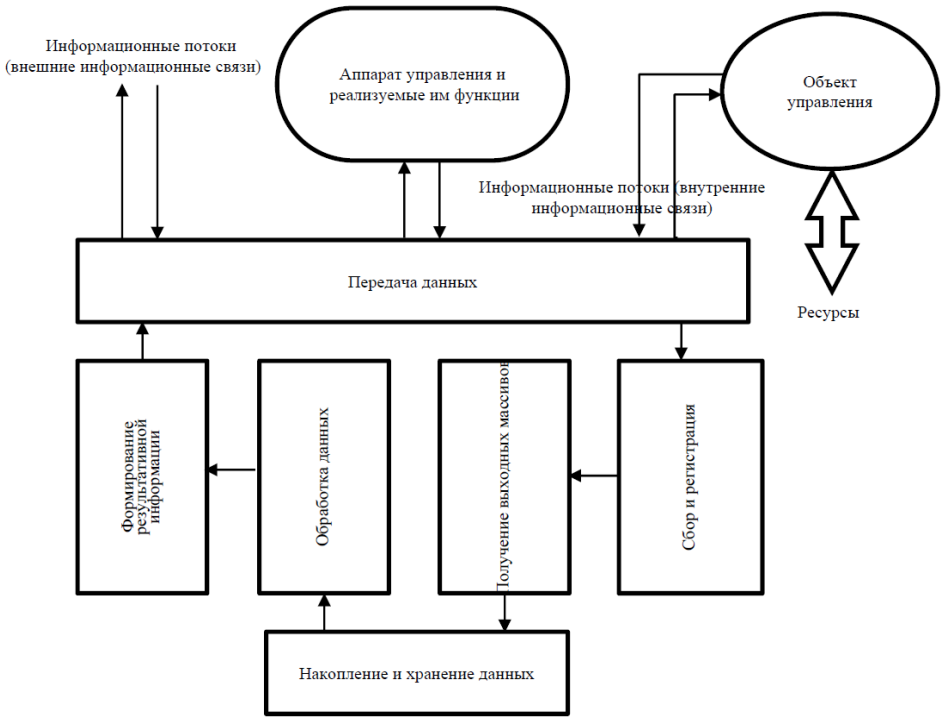

Рис. 1. Функциональная структура АИС[1]

[1] Гюльалиев Т.М., Абакарова О.Г. Развитие и внедрение современных информационных технологий в системе МВД России / Т.М. Гюльалиев и др. // В сборнике: Современные проблемы научной деятельности. Перспективы внедрения инновационных решений. Сборник статей Международной научно-практической конференции. – Уфа, 2022. – С. 36.

Информация, связанная с правовыми положениями, криминологическими наблюдениями или статистическими материалами, в большинстве случаев подвергается специальной трансформации, однако возможны случаи, когда необходимость в преобразовании отсутствует. Последовательность выполнения операций может варьироваться и иногда предполагает повторное применение отдельных действий. Конкретный состав процедур обработки определяется спецификой объекта управления, подлежащего автоматизированной обработке.

Информационно-вычислительные системы (ИВС) являются неотъемлемой частью современной структуры органов внутренних дел и играют ключевую роль в обеспечении эффективности их деятельности. ИВС представляют собой интегрированные комплексы технических средств, программного обеспечения, баз данных и нормативных актов, которые обеспечивают сбор, обработку, хранение и передачу данных. Они позволяют органам внутренних дел эффективно решать широкий спектр задач, включая обеспечение общественной безопасности, раскрытие преступлений, управление оперативной информацией и аналитическую работу.

В рамках МВД России ИВС могут быть классифицированы по функциональной направленности и уровню интеграции. По функциональной направленности системы подразделяются на следующие типы:

1) системы управления и мониторинга - например, система «Безопасный город», интегрирующая в себе элементы видеонаблюдения и автоматической обработки данных для обеспечения правопорядка в городах (Распоряжение Правительства РФ от 3 декабря 2014 г. № 2446-р О Концепции построения и развития аппаратно-программного комплекса «Безопасный город»[1]);

2) системы анализа и прогнозирования - такие системы используются для мониторинга правонарушений и преступлений, а также для выявления тенденций в поведении правонарушителей. Примером является аналитическая

[1] О Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: Распоряжение Правительства РФ от 3 декабря 2014 г. № 2446-р // Российская газета. – 2014. – 11 дек.

платформа МВД России, которая объединяет данные из различных источников для анализа и прогнозирования преступной деятельности (Приказ МВД РФ от 24 октября 2011 г. № 1097 «О совете по созданию Единой системы информационно-аналитического обеспечения деятельности МВД России»[1]);

3) системы обработки и хранения данных - это базы данных, которые используются для централизованного хранения данных о правонарушениях, подозреваемых, криминогенных ситуациях и т.д. К таким системам относится Единая информационная система МВД, которая интегрирует данные из различных региональных подразделений и позволяет оперативно получать необходимую информацию для принятия решений (ст. 10 федерального закона от 07.02.2011 № 3-ФЗ «О полиции»[2]).

Классификация ИВС также включает разделение по уровням их интеграции. На нижнем уровне функционируют локальные ИВС, которые обслуживают отдельные подразделения и территории. Примером являются региональные системы учета и мониторинга. На более высоком уровне находятся интегрированные ИВС, которые обеспечивают обмен данными между различными федеральными и территориальными подразделениями. Единая информационная система МВД России - это пример такой интеграции, которая позволяет на базе общедоступных данных о правонарушениях и преступлениях объединять информацию из различных источников для более комплексного анализа и принятия решений (Паспорт федерального проекта Информационная безопасность (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. № 9))[3].

---

[1] О совете по созданию Единой системы информационно-аналитического обеспечения деятельности МВД России: Приказ МВД РФ от 24 октября 2011 г. № 1097 / Текст приказа официально опубликован не был.

[2] О полиции: федеральный закон от 7 февраля 2011 г. № 3-ФЗ (с изм. от 01 апреля 2025 г.) // Российская газета. – 2011. – №5401; 2025. – №75.

[3] Паспорт федерального проекта Информационная безопасность (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных

Особое внимание в процессе функционирования ИВС уделяется вопросам защиты информации. В связи с обрабатываемыми данными, включая личную информацию граждан и служебную информацию, органы внутренних дел обязаны соблюдать требования безопасности данных. В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], создаются многоуровневые системы защиты, которые включают в себя шифрование данных, системы аутентификации и мониторинга, а также системы аудита и защиты от несанкционированного доступа. Это обеспечивает надлежащую защиту личных данных граждан и служебной информации от внешних угроз и злоупотреблений (Приказ МВД России от 9 ноября 2018 г. № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России»[2]).

Рассмотрим специфику выполнения ключевых процедур преобразования информации в управлении деятельностью ОВД.

1. Сбор и фиксация сведений в различных структурных единицах осуществляется с использованием множества методик. Наиболее трудоёмкой считается процедура, реализуемая в рамках автоматизированных систем управления, функционирующих в штабе органа внутренних дел. Здесь производится первичная фиксация данных, отражающих как текущую оперативную обстановку, так и особенности функционирования подразделения в конкретной территориальной зоне. В других подразделениях органов внутренних дел, в том числе дежурных частях, службах тылового, финансового и документационного направления, данный процесс приобретает иную специфику, связанную с оформлением, передачей и архивированием различных

технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. № 9)) / Текст паспорта опубликован не был.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. от 01 апреля 2025 г.) // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3448.

[2] О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России: Приказ МВД России от 9 ноября 2018 г. № 755 // Российская газета. – 2018. – 06 дек.

категорий документов. Устойчивое выполнение задач в сфере охраны общественного порядка требует получения точной, разносторонней и актуальной информации. Сбор таких сведений происходит при приёме заявлений о правонарушениях, поступлении информации от смежных подразделений, формировании статистики по числу предполагаемых участников преступлений, а также по величине нанесённого материального ущерба. Дополнительно фиксируются данные, характеризующие эффективность действий исполнителей, с использованием количественных и качественных показателей. В роли основных носителей данных чаще всего выступают бумажные формы и журналы учёта, после чего информация оцифровывается и переводится в формат, пригодный для хранения и обработки в информационных системах. Использование ручных методов существенно повышает трудозатраты и снижает оперативность документооборота. В связи с этим актуальным становится применение автоматизированных систем. Технические средства позволяют точно измерять показатели, регистрировать данные, сохранять их в памяти устройств и передавать по установленным каналам связи, а также осуществлять прямой ввод в программные комплексы, что обеспечивает возможность дальнейшего анализа и оформления необходимой документации[1].

2. Информация передаётся с использованием различных механизмов: физическая доставка курьерами, почтовое сообщение, отправка по телекоммуникационным линиям связи и иные методы. При этом применение удалённых каналов взаимодействия предполагает использование специализированных технологических решений, что способствует росту затрат и усложнению процедур передачи. «В ОВД предпочтительным вариантом является использование технических средств сбора и регистрации информации, которые автоматически получают данные с датчиков и передают их в компьютер для обработки. Это позволяет повысить достоверность данных и уменьшить

[1] Воронов А.М., Анисифорова М.В. Перспективы внедрения новых информационных технологий в деятельность органов внутренних дел по профилактике правонарушений / А.М. Воронов и др. // Вестник ВИПК МВД России. – 2024. – № 2 (70). – С.41.

трудозатраты. Заметим, что возможна передача первичной информации с места ее возникновения и результатной информации удаленно. Результаты обычно фиксируются на мониторах, информационных панелях и печатающих устройствах. Данные передаются по телекоммуникационным каналам в центр обработки, чаще всего, через компьютер с применением специальных программных и аппаратных средств. Современные телекоммуникационные средства для передачи информации постоянно совершенствуются и развиваются. Они особенно важны для многоуровневых систем внутри одной организации, например, в МВД России. Дистанционная передача информации значительно ускоряет ее обработку и передачу между разными уровнями управления, что является важным преимуществом»[1].

3. Для формирования исходных массивов данных требуется предварительное приведение информации к структурированному виду, позволяющему ввод в вычислительное устройство, сохранение на цифровых носителях или отправку по информационным каналам. Этот этап именуется машинным кодированием. Указанная процедура заключается в трансформации содержательных сведений в формат, воспринимаемый техническими системами и пригодный для размещения на устройствах хранения, таких как твердотельные накопители либо иные виды цифровых носителей. Фиксация информации на машинных носителях может осуществляться как на этапе обработки, так и в рамках отдельного действия. В любом случае сформированные машинные структуры применяются для последующей интерпретации, анализа или исполнения вычислительных операций.

4. Сохранение информации обеспечивает её повторное применение в управленческом или аналитическом контексте. Для выполнения этой задачи требуется наличие постоянного доступа к различным видам данных. До начала обработки сведения подлежат систематическому накоплению и

[1] Долинин В.Н., Пермяков Е.К., Ровнушкин В.Е. Использование компьютерных технологий в правоохранительной деятельности // В сборнике: Технологии XXI века в юриспруденции. Материалы четвёртой международной научно-практической конференции / Отв. редактор: Д.В. Бахтеев. – Екатеринбург, 2022. – С. 67.

структурированию. Организация хранения осуществляется с использованием информационных баз, в которых данные размещаются по заранее установленной логике, определённой в ходе проектирования архитектуры базы. Информация хранится на электронных носителях в форме упорядоченных массивов. Функция хранения тесно связана с необходимостью оперативного поиска нужных сведений. Поисковые процедуры направлены на идентификацию конкретной информации по заданным параметрам, определённым пользователем либо вычислительной системой. Эти процедуры охватывают как выбор уже готовых к применению данных, так и выявление информации, нуждающейся в уточнении или актуализации. Пользователь инициирует поиск посредством формулирования запроса и выбора необходимой формы представления результата. Выполнение операций поиска осуществляется автоматически с целью обнаружения релевантных данных в значительных объёмах хранимой информации.

5. Обработка информации в ОВД происходит на компьютере и обычно осуществляется децентрализовано в местах, где была получена первичная информация. «Для этого создаются автоматизированные рабочие места для специалистов, которые принадлежат определенным службам, таким как дежурная часть, отдел материально-технического снабжения, штаб, отдел делопроизводства и режима и т. д. Однако, существует возможность обработки информации не только автономно, но и в вычислительных сетях с помощью программных средств и информационных массивов, которые позволяют решать различные функциональные задачи. Алгоритмы, реализованные в компьютерных программах, позволяют получать результатные сводки, которые могут быть выведены на экране или напечатаны на бумаге. Для распространения этой информации может быть использована процедура тиражирования или электронной рассылки, которая позволяет доставить данные до нескольких

пользователей. Это удобно, если документ с результатами нужен нескольким людям одновременно»[1].

6. В рамках функционирования автоматизированной системы организационного управления выбор решений осуществляется либо с применением специализированных технических устройств, либо посредством интерпретации информации без опоры на электронные средства. Независимо от подхода, процесс требует выявления наилучшего варианта при стремлении к минимизации временных, трудовых и материальных издержек. Привлечение вычислительной техники способствует углублённому анализу исходных данных и постепенному переходу к автоматизированному формированию решений посредством диалога между пользователем и программным обеспечением. Наиболее результативно в этом направлении работают экспертные платформы и интеллектуальные комплексы, ориентированные на поддержку управленческих процессов.

Таким образом, информационно-вычислительные системы, применяемые в структурах МВД России, обеспечивают повышение результативности и сокращение временных затрат при выполнении задач правоохранительной направленности. Систематизация таких решений позволяет разграничить их по характеру выполняемых функций и степени сопряжённости с другими компонентами. Это создаёт условия для реализации эффективных стратегий обеспечения общественной безопасности и стабильности в административных юрисдикциях.

§2. Компоненты информационной системы органов внутренних дел

[1] Дудченко А.В., Парий М.А. Информационные технологии в правоохранительной деятельности / А.В. Дудченко и др. // Очерки новейшей камералистики. – 2023. – № 2. – С. 16.

Одной из базовых функций органов внутренних дел является системное получение и аналитическая обработка сведений, отражающих характеристики преступной активности и нарушений установленного правопорядка. Это направление охватывает весь спектр управленческой деятельности - от разработки концептуальных решений до реализации конкретных мер, направленных на выявление, пресечение и предупреждение противоправных действий. Все объекты и субъекты, имеющие отношение к расследуемым деяниям, подлежат обязательной фиксации с последующим учётом всех оперативных мероприятий. Таким образом, информационное обеспечение является фундаментом всей структуры управления, а обработка поступающих данных составляет основное содержание деятельности сотрудников.

Информационные ресурсы, используемые в системе управления органов внутренних дел, представляют собой совокупность сведений, предназначенных для подготовки и принятия решений, а также для выполнения функций учёта, анализа, планирования, прогнозирования, контроля и регулирования. Любое сообщение или массив данных, способствующий повышению обоснованности управленческих решений, относится к числу управленческой информации. Потоки таких сведений, циркулирующие в системе МВД России, подразделяются на определённые категории. Первая категория - предписывающая информация. Внутри неё выделяются следующие подгруппы: 1) постановочные материалы, охватывающие приказы, служебные задания, положения оперативных сводок; 2) нормативные документы, включающие законодательные акты, административные постановления, внутренние регламенты, уставы и указания высших органов управления; 3) плановые документы, отражающие текущие и долгосрочные задания, утверждённые для территориальных подразделений. Вторая категория - описательная информация, содержащая сведения об актуальном состоянии объектов, подлежащих

управленческому воздействию, в том числе данные об оперативной обстановке и динамике криминогенных факторов[1].

Функциональная эффективность информационных процессов в системе управления зависит от структуры соответствующих информационных комплексов. Их организация обеспечивает полный цикл - от получения и накопления до анализа и предоставления сведений, необходимых для принятия решений. Информационная система, независимо от формы реализации, охватывает следующие ключевые элементы:

- массивы данных, используемые для реализации управленческих функций;

- процедуры, регулирующие обработку информации: её получение, передачу, преобразование и хранение;

- персонал, осуществляющий поддержку и контроль работы информационной структуры;

- технические устройства, обеспечивающие работу системы;

- каналы и формы взаимодействия, посредством которых осуществляется передача и обмен данными между участниками управленческого процесса[2].

Характеристики системы информационного обеспечения управленческой деятельности могут быть структурированы через этапную модель, отражающую последовательность действий профильных подразделений и отдельных исполнителей. Такая модель демонстрирует переход от одного уровня функционирования к следующему в контексте повышения эффективности управленческого процесса. В данном случае информационное обеспечение выступает в роли ключевого элемента, обеспечивающего устойчивость и результативность управленческой системы. Каждый из этапов требует применения специфических решений и инструментов, связанных с обработкой,

---

[1] Курушин С.А., Яворский М.А. Информационные технологии в оптимизации правоохранительной деятельности / С.А. Курушин и др. // Наука XXI века: актуальные направления развития. – 2022. – № 2-2. – С. 148.

[2] Курушин С.А., Яворский М.А. Информационные технологии в оптимизации правоохранительной деятельности / С.А. Курушин и др. // Наука XXI века: актуальные направления развития. – 2022. – № 2-2. – С. 149.

хранением и передачей данных. Использование цифровых технологий в этих условиях становится необходимым условием для рационализации процессов и повышения качества управленческих решений. Эти этапы схематично могут выглядеть следующим образом (табл. 1).

Таблица 1

Этапы информационного обеспечения управления деятельностью подразделений в ОВД

Этап	**Содержание**	**Целевая направленность**
1	Сбор, обработка, выдача информации	Ответить на вопрос «Что происходит?»
2	Выявление положительных и отрицательных тенденций в состоянии преступности и правоохранительной деятельности	Ответить на вопрос «Почему так происходит?»
3	Прогнозирование противоправной деятельности	Ответить на вопрос «Что будет, если…?»
4	Подготовка обоснованных выводов и рекомендаций по организации правоохранительной деятельности, по борьбе с противоправными действиями	Обеспечить эффективное управление деятельностью ОВД

Для обеспечения соответствия управления в системе органов внутренних дел актуальным стандартам необходимо расширение применения цифровых решений и телекоммуникационной инфраструктуры. Внедрение автоматизированных информационных систем, способных обеспечивать полный цикл работы с управленческой информацией - от её получения до принятия решений, становится обязательным условием повышения эффективности административной деятельности. Комплексная организация информационного сопровождения управления предполагает не только оперативный доступ к данным, но и реализацию аналитических процедур, прогнозных расчётов и подготовку обоснованных управленческих решений.

В настоящее время в практике органов внутренних дел формируется новый этап технологической трансформации, сопряжённый с институциональными изменениями в системе МВД России. Современное регламентирование деятельности сотрудников предусматривает обязательное применение научных разработок, цифровых платформ, сетей связи и других компонентов

телекоммуникационной среды[1]. С этой целью действует единый координационный центр - Департамент информационных технологий, связи и защиты информации, на который возложены функции по организации и контролю мероприятий по внедрению цифровых решений в систему МВД России. Его полномочия определены в соответствии с приказом МВД России от 15 июня 2021 года № 444[2].

Создание единого организационного центра позволило устранить неструктурированное внедрение информационных технологий в деятельность территориальных подразделений, установить унифицированные требования к совместимости систем, а также выстроить логически взаимосвязанную архитектуру цифрового управления. В рамках модернизации были разработаны и внедрены новые технические решения для информационно-справочной системы ОВД, обеспечивающие повышение производительности, оптимизацию доступа к прикладным сервисам и улучшение качества обработки данных. Все указанные меры направлены на усиление функциональной надёжности и эффективности цифровой среды, используемой в оперативной и управленческой работе МВД России.

В настоящее время Департамент информационных технологий, связи и защиты информации МВД России реализует масштабный проект по стандартизации программных решений, применяемых в различных подразделениях ведомства. Основная задача состоит в переходе на единый программный комплекс, охватывающий ключевые направления деятельности, с учётом специфики каждой службы. Разработка и внедрение информационной системы оперативно-диспетчерского управления направлены на создание унифицированного инструмента, обеспечивающего выполнение задач следственных подразделений на всех уровнях – от локального до федерального.

---

[1] О полиции: федеральный закон от 7 февраля 2011 г. № 3-ФЗ (с изм. от 01 апреля 2025 г.) // Российская газета. – 2011. – №5401; 2025. – №75.

[2] Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации МВД России: Приказ МВД России от 15.06.2021 № 444 (с изм. от 31 марта 2025 г.) / Текст приказа официально опубликован не был.

Данное решение предусматривает единую программную платформу с общей базой данных, синхронизированной по структуре и функциональности с задачами различных уровней управления.

Функционирование информационной системы МВД России обусловлено необходимостью повышения эффективности коммуникационных и аналитических процессов в правоохранительных органах. За прошедшие годы сформирована единая цифровая среда, базирующаяся на ведомственной телекоммуникационной платформе, что позволило достичь минимального стандарта технического обеспечения подразделений. В результате создана интегрированная мультисервисная телекоммуникационная сеть, обеспечившая подключение узлов связи всех территориальных единиц министерства к общенациональной информационной структуре.

Внедрение системы ИСОД стало ответом на отсутствие согласованной модели автоматизации, при которой ранее каждое подразделение использовало программные комплексы, ориентированные исключительно на решение узкоспециализированных задач. Программы, разработанные для нужд различных служб – от патрульно-постовой до экономической безопасности, - функционировали изолированно, что исключало возможность обмена данными в едином цифровом пространстве. Отсутствие совместимости между платформами привело к необходимости установки нескольких рабочих станций в рамках одного функционального места, что повышало нагрузку и затрудняло координацию. Современная унифицированная информационная система позволяет устранить подобные ограничения за счёт централизации данных и стандартизации программной архитектуры, обеспечивая непрерывность, согласованность и высокую результативность управленческой и оперативной деятельности.

«Одной из основных целей при разработке информационной системы оперативно-диспетчерского управления МВД России было обеспечение интеграции всех ранее существовавших информационных систем. Это позволило объединить данные и обеспечить эффективную взаимосвязь между

системами, что повысило эффективность работы всей системы в целом. Другой значительной причиной, которая также имеет важное значение, заключается в том, что информационные системы были созданы без учета последних тенденций. Их использование предполагало установку программ на компьютерах пользователей и серверах внутри локальных сетей, а также наличие отдельных центров обработки данных (далее – ЦОД) на региональном уровне. Это приводило к высоким расходам на обслуживание систем, низкой надежности и недостаточному уровню производительности»[1].

ИСОД МВД России представляет собой интегрированный технологический комплекс, состоящий из программного обеспечения, вычислительных модулей и каналов связи, обеспечивающих взаимодействие между функциональными структурами ведомства. Назначением этой системы является автоматизация ключевых процессов, централизованное ведение информационных массивов и упорядоченное распределение доступа к служебным ресурсам. Единая информационная среда формирует условия для взаимодействия между подразделениями, позволяя оперативно использовать обобщённые сведения в рамках координированной деятельности.

Функциональные возможности системы направлены на повышение аналитической точности, улучшение процедур контроля, обеспечение достоверной отчётности и оперативную обработку параметров, отражающих состояние и результативность ведомственной деятельности. Совокупность этих характеристик создаёт условия для эффективной реализации функций государственного управления и предоставления административных услуг при сокращении затрат времени и трудовых ресурсов, связанных с обработкой данных. Работа с компонентами системы осуществляется через ведомственное облачное пространство, структурированное в виде распределённой сети центров

[1] Шикова Е.Р., Клевцов И.А. Информационные технологии в правоохранительной деятельности / Е.Р. Шикова и др. // В сборнике: Право, как искусство добра и справедливости. Сборник научных трудов 3-й Всероссийской научной конференции памяти д.ю.н., профессора О.Г. Лариной. Юго-Западный государственный университет; Союз криминалистов и криминологов; МГЮА имени О.Е. Кутафина. – Курск, 2022. – С. 267.

обработки данных, соединённых в единую цифровую инфраструктуру. Все базовые модули и базы хранятся в этой среде, что обеспечивает устойчивый и централизованный доступ ко всем функциональным компонентам.

Переход к облачной архитектуре потребовал изменения подходов к построению информационно-технической базы Министерства. Вся инфраструктура ведомства была подключена к распределённой системе для обеспечения непрерывного доступа к сервисам. Интенсивность взаимодействия с облачной платформой определялась числом используемых программных решений. Безопасность информационного обмена обеспечивалась путём внедрения технологий шифрования, защищающих каналы передачи. В основу функционирования информационного хранилища положены стандартизированные программные комплексы, обеспечивающие консолидацию и миграцию данных из ранее действующих систем в единое информационное пространство.

«Одним из ключевых компонентов инфраструктуры ИСОД МВД России является система ЦОД, которая создается на нескольких удаленных территориях с целью обеспечения высокого уровня надежности и доступности информационно-телекоммуникационных услуг. Эта система является необходимой для эффективной работы ИСОД МВД России и гарантирует бесперебойную работу информационных ресурсов в любых обстоятельствах. В архитектуре ЦОД используются как проверенные, уже используемые технологии, так и новые, перспективные решения. Обновление системы осуществляется путем замены устаревших компонентов на более современные, при этом не требуется перестройка всей инфраструктуры ЦОД. Кроме того, данная система обеспечивает инвариантность инфраструктуры для решения различных задач, а также возможность внедрения единой централизованной системы управления сетью и сетевой безопасностью. Главной целью является создание единой программно-технической платформы, которая позволит унифицировать решения и обеспечивать доступ к информационным системам и ресурсам МВД России. Также в рамках этой задачи предполагается разработка

программных решений, которые помогут оптимизировать работу территориальных подразделений МВД России, упростят подготовку документов и принятие решений. В результате такой автоматизации сотрудники МВД России смогут быстрее и точнее выполнять свои задачи и вести учет информации о проведенных мероприятиях, что будет очень важно для обеспечения безопасности в стране»[1].

Проектирование программных решений для МВД России ориентировалось на автоматизацию основных направлений деятельности, охватывающих уголовный розыск, предварительное следствие, дознание, исполнение норм административного законодательства, деятельность участковых, дежурных служб, патрульно-постовой полиции, подразделений ГИБДД и иных структур. Реализация таких решений способствует повышению результативности служебных операций и эффективности противодействия преступным действиям.

Центры обработки данных, функционирующие в структуре министерства, используют технологии виртуализации и адаптивного масштабирования, позволяющие динамически распределять ресурсы в зависимости от поступающих запросов. Эти технологические подходы обеспечивают устойчивость системных приложений, доступных исключительно персоналу ведомства, при этом гарантируется высокий уровень защиты при хранении и обработке информационных ресурсов. Применение данной цифровой архитектуры способствует принятию управленческих решений, основанных на обобщённой информации, извлекаемой из актуальных источников. Такой подход обеспечивает возможность анализа текущих процессов, выявления структурных зависимостей, построения прогностических моделей и оценки управляемых ситуаций. В результате происходит совершенствование процедур планирования и оптимизация регламентов управленческого воздействия.

---

[1] Новичихин П.Г. О некоторых проблемах эксплуатации на местах программного обеспечения сервиса обеспечения охраны общественного порядка единой системы информационно-аналитического обеспечения деятельности МВД России / П.Г. Новичихин // Научный портал МВД России. – 2024. – № 1 (65). – С. 69.

В рамках системы предоставления государственных услуг реализовано межведомственное цифровое взаимодействие. Для обеспечения этого процесса разработаны специализированные приложения, внедрены защищённые каналы связи, функционирующие в пределах единой ведомственной среды. Министерство внутренних дел выступает источником данных в данной модели информационного взаимодействия. Сотрудники, задействованные в предоставлении государственных сервисов, используют специальные программные модули, адаптированные для межведомственного обмена сведениями. «С развитием ИТ-технологий становится все более важным обеспечение безопасности информационных систем и ресурсов МВД России. Это касается в том числе угроз, связанных с кибератаками. Для обеспечения безопасности информационных систем в МВД России работают в соответствии с федеральными и ведомственными правовыми актами, развивают и совершенствуют существующую систему защиты информации. МВД России провело масштабные работы по лицензированию и аккредитации органов внутренних дел в качестве аттестационных органов, которые занимаются оценкой объектов информатизации с точки зрения требований безопасности информации, а также обеспечением необходимой комплектации контрольно-измерительной и поисковой техникой. В настоящее время продолжается обеспечение подразделений МВД России средствами защиты информации»[1].

В системе ИСОД прослеживается курс на унификацию и сопряжение отдельных компонентов цифровой среды, что сопровождается параллельным развитием специализированных решений, предназначенных для выполнения аналитических и управленческих функций в структуре органов внутренних дел. Для решения задач этого уровня используются платформенные продукты класса Business Intelligence, позволяющие формировать прикладные модули для анализа и обработки информации. Одним из направлений работы в данной среде

[1] Новичихин П.Г. О некоторых проблемах эксплуатации на местах программного обеспечения сервиса обеспечения охраны общественного порядка единой системы информационно-аналитического обеспечения деятельности МВД России / П.Г. Новичихин // Научный портал МВД России. – 2024. – № 1 (65). – С.70.

является организация ассоциативного поиска по элементам массивов, размещённых в оперативной памяти. Такой механизм обеспечивает интерактивный режим взаимодействия с данными и предоставляет результаты по мере ввода параметров поиска, что приближает его к функционированию веб-поисковых систем. Анализ информации из разнотипных источников сопровождается визуализацией с применением различных графических форматов - таблиц, диаграмм, сводных блоков, гистограмм, интерактивных календарей и средств пространственной визуализации, включая карты и фильтры. Используемая платформа обеспечивает удалённый доступ к аналитическим инструментам, поддерживая возможность работы в среде браузера. Это расширяет потенциал применения системы в оперативной деятельности, создаёт условия для пространственной мобильности пользователей и способствует совершенствованию методов оценки, визуализации и сопоставления данных в контексте управленческих решений, принимаемых в системе МВД России.

«Платформа BI используется для анализа деятельности службы «02» и дежурной части с использованием данных из внутренних систем, поддерживающих деятельность ведомства. Анализ и оценка работы операторов службы «02» проводится по многим показателям, включая среднее время работы, количество зарегистрированных карточек и среднее время регистрации карточек. По результатам рассмотрения показателей формируются различные рейтинги: рейтинг смен, 10 лучших и 10 худших сотрудников и т.д. Исследуются случаи нарушений закона и жалобы на такие случаи. Анализ проводится по различным параметрам, таким как среднее количество происшествий в разное время суток, количество случаев, зарегистрированных за менее или более двух минут, время регистрации происшествий в зависимости от их типа, а также категории нарушений. Путем анализа ряда показателей можно рассмотреть деятельность операторов и определить, насколько эффективно они работают. Рассмотрение конкретных показателей, связанных с их работой, позволяет оценить, как операторы выполняют свои обязанности и какие изменения могут

быть внесены для улучшения качества работы. Такой анализ помогает контролировать процесс работы операторов и с развитием новых технологий становится все более важным для повышения эффективности бизнеса»[1].

Оценка эффективности функционирования дежурных подразделений органов внутренних дел осуществляется с использованием специализированных аналитических индикаторов, формирующих обобщённое представление об уровне реагирования на инциденты и качестве исполнения обязанностей. В структуру данных показателей входят численность зарегистрированных происшествий, усреднённая продолжительность обработки обращений, классификация правонарушений по категориям, а также доля ложных сообщений по отношению к подтверждённым событиям. Указанные параметры территориально привязаны, что предоставляет возможность проводить сравнительный анализ между различными административными единицами.

Результаты структурных преобразований в системе МВД России привели к существенному укреплению информационного сопровождения оперативной работы. Была развернута многоуровневая телекоммуникационная система на базе ведомственной мультисервисной сети, внедрены централизованные цифровые платформы, включая информационно-справочную систему и центры обработки данных. Созданы территориально распределённые специализированные комплексы. Подходы к нормативно-техническому регулированию автоматизированных информационных систем были пересмотрены, обеспечена унификация требований, с акцентом на интеграцию облачных решений, интеллектуальных функций и аналитических компонентов в рамках единой цифровой среды управления.

Отметим, что в условиях нарастания внешнеполитического давления и необходимости обеспечения технологического суверенитета Российской Федерации, переход федеральных органов исполнительной власти, включая

[1] Новичихин П.Г. О некоторых проблемах эксплуатации на местах программного обеспечения сервиса обеспечения охраны общественного порядка единой системы информационно-аналитического обеспечения деятельности МВД России / П.Г. Новичихин // Научный портал МВД России. – 2024. – № 1 (65). – С.71.

Министерство внутренних дел, на отечественное программное обеспечение стал частью государственной стратегии по импортозамещению в сфере информационно-коммуникационных технологий. Одним из ключевых направлений в данном процессе выступает внедрение операционной системы Astra Linux, сертифицированной ФСТЭК и ФСБ России для обработки информации с различными уровнями конфиденциальности.

Astra Linux представляет собой специализированную операционную систему, разработанную на базе ядра Linux, адаптированную для функционирования в условиях повышенных требований к информационной безопасности. Система обеспечивает реализацию мандатного контроля доступа, защищённую загрузку, изоляцию процессов и расширенные возможности администрирования. Переход МВД на данную платформу осуществляется в рамках Приказа МВД № 362 об использовании российской защищенной системы Astra Linux Special Edition, который был подписан 21 мая 2020 г., однако имеет гриф «Для служебного пользования» и не публиковался. Операционная система Astra Linux была аттестована в качестве госинформсистемы первого класса защищенности 26 мая 2021 г.

На практике внедрение Astra Linux в МВД России осуществляется поэтапно и охватывает следующие направления: 1) автоматизированные рабочие места сотрудников дежурных частей, паспортных подразделений, миграционных служб; 2) серверные комплексы для обработки массивов данных в системах ИСОД, ЕРАП и АРМ «Дежурная часть»; 3) инфраструктура региональных ситуационных центров; 4) мобильные комплексы и ведомственные защищённые ноутбуки.

Таким образом, переход МВД России на Astra Linux отражает системную политику по укреплению технологической независимости и информационной безопасности. Адаптация и интеграция этой платформы в деятельность министерства сопровождаются формированием новых подходов к управлению ИТ-инфраструктурой и повышением защищенности ведомственной цифровой среды.

§3. Правовое регулирование использования информационно-коммуникационных технологий в деятельности полиции

Использование информационно-вычислительных систем в органах внутренних дел Российской Федерации регулируется комплексом законодательных и подзаконных актов, направленных на обеспечение безопасности данных, эффективное функционирование ИВС и соблюдение прав граждан. С момента их внедрения в структуру МВД России, правовое регулирование ИВС претерпело ряд изменений, что обусловлено быстрым развитием цифровых технологий и требованиями к улучшению оперативности и качества работы правоохранительных органов.

Согласно Закону Российской Федерации о поправке к Конституции РФ от 14.03. 2020 г. № 1-ФКЗ к ведению Российской Федерации относится «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных» (пункт «м» статьи 71 Конституции РФ)[1]. Стратегия развития информационного общества на 2017-2030 годы, утвержденная Указом Президента РФ от 09.05.2017 № 203[2], поставила перед органами публичной власти задачи по обеспечению высокого уровня доступности для населения информации и технологий, а также по совершенствованию системы государственных гарантий конституционных прав человека и гражданина в информационной сфере.

---

[1] О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти: Закон Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ // Собрание законодательства РФ. – 2020. – № 11. – Ст. 1416.

[2] О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // Собрании законодательства РФ. – 2017. – № 20. – Ст. 2901.

Одним из ключевых документов, регулирующих использование современных информационно-телекоммуникационных систем в деятельности полиции, является Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции», который определяет общие принципы работы органов внутренних дел и включает положения, касающиеся использования информационных технологий для повышения эффективности работы полиции. В частности, в статье 10 этого закона указано, что МВД России обязано использовать современные информационные технологии для обеспечения безопасности и упрощения взаимодействия с гражданами и другими государственными органами.

Применение информационных технологий в системе полиции предусмотрено положениями статьи 11 Федерального закона «О полиции», где зафиксирована обязанность использования современных технических средств. Цифровая трансформация деятельности органов внутренних дел представляет собой этап функционального развития и структурной оптимизации их работы, направленный на повышение точности, оперативности и координации действий. Основу информационно-технологического обеспечения составляют достижения в сфере вычислительной техники и телекоммуникационной инфраструктуры, обеспечивающие реализацию управленческих, аналитических и оперативных задач в правоохранительной практике.

Кроме того, важную роль в правовом регулировании ИВС играет Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], который устанавливает общие требования к защите данных, используемых в государственных информационных системах, включая правоохранительные органы. Закон ориентирован на повышение уровня защиты персональных данных граждан и служебной информации от несанкционированного доступа, а также на создание

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. от 01 апреля 2025 г.) // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3448.

безопасной среды для обработки и передачи данных в рамках государственных ИТ-систем.

Постановлением Правительства Российской Федерации от 10 октября 2020 года № 1646[1] утверждено Положение о ведомственных программах цифровой трансформации, в котором закреплены процедуры формирования, согласования и внедрения цифровых стратегий федеральными органами исполнительной власти. Документ вводит термин «цифровая трансформация», определяемый как комплекс мероприятий, реализуемых государственным органом с целью преобразования систем управления, а также совершенствования исполнения функций и предоставления услуг посредством применения электронных данных и информационных технологий. Согласно указанному нормативному документу в МВД России разработаны стратегические инициативы цифрового характера, направленные на повышение результативности оперативной, управленческой и сервисной деятельности через внедрение цифровых инструментов. В настоящее время реализуется ведомственная программа цифровой трансформации МВД России на 2023–2025 годы, утверждённая распорядительным актом Министерства внутренних дел от 25 января 2023 года № 1/649[2]. Целевое назначение программы заключается в создании условий для качественного обновления подходов к организации внутренних процессов и обеспечению выполнения возложенных на ведомство полномочий с опорой на цифровую инфраструктуру и технологии обработки данных.

Полиция, как элемент государственной исполнительной системы, реализует свои функции в рамках административно-правовой и уголовно-процессуальной деятельности. При этом переход к цифровой модели

---

[1] О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий, финансовое обеспечение которых осуществляется (планируется осуществлять) за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов: Постановление Правительства РФ от 10 октября 2020 г. № 1646 (с изм. от 18 марта 2025 г.) // Собрание законодательства РФ. – 2020. – № 42 (часть III). – Ст. 6612.

[2] Об утверждении Ведомственной программы цифровой трансформации МВД России на 2023-2025 годы: Распоряжение МВД России от 25.01.2023 № 1/649 / Текст приказа опубликован не был.

управления, продиктованный общественным и государственным запросом, обусловливает необходимость технологического переосмысления организационной и правоприменительной практики. Основанием для внедрения цифровых решений служит часть первая статьи 11 Федерального закона «О полиции», устанавливающая обязанность использования научно-технических достижений, информационных платформ, каналов связи и телекоммуникационных систем в оперативной и управленческой деятельности.

В контексте цифровых преобразований деятельность органов внутренних дел структурируется по ряду ключевых направлений. Одним из приоритетов выступает автоматизация процедур предоставления государственных услуг, реализуемая через интеграцию с Единым порталом государственных услуг и сетью многофункциональных центров. Указанные инструменты обеспечивают удалённый доступ граждан к необходимым сервисам без физического обращения в ведомственные подразделения.

Регламентация указанных процессов осуществлялась на основе нормативных актов МВД России, направленных на повышение результативности исполнения полномочий, в том числе через внедрение электронных форм обслуживания. За период более десяти лет функционирования сформирована устойчивая модель взаимодействия, обладающая высокой степенью структурной устойчивости. Использование цифровых механизмов межведомственной координации позволило достичь качественного изменения характера оказания услуг, выразившегося в росте доступности, улучшении уровня прозрачности и формировании открытого канала взаимодействия между гражданином и полицейскими структурами.

Внедрение информационно-телекоммуникационных систем в практику органов внутренних дел позволило устранить либо существенно сократить проблему очередей при получении государственных услуг. Новая модель взаимодействия между полицией и населением базируется на положениях, закреплённых в статьях 5–11 Федерального закона «О полиции», в которых

сформулированы основные принципы деятельности правоохранительных органов.

Подавляющее большинство государственных функций, реализуемых в системе МВД России, связано с деятельностью миграционных подразделений. Среди них - оформление и продление документов, удостоверяющих личность, регистрация по месту проживания и временного пребывания, оформление гражданства. Значительная часть услуг относится также к сфере деятельности Государственной инспекции по безопасности дорожного движения, включая регистрацию нарушений с помощью средств фотовидеофиксации, применение электронных сервисов обжалования штрафов, контроль за оборотом наркотических веществ и иные направления.

Использование фотовидеофиксации нарушений правил дорожного движения рассматривается как эффективный элемент обеспечения безопасности в транспортной системе. Данный технический инструмент обеспечивает фиксацию фактических обстоятельств событий и служит объективным источником доказательств при документировании административных правонарушений. Применение указанных средств оказывает влияние на снижение числа дорожно-транспортных происшествий. Вместе с тем существует ряд технических и правовых ограничений: автоматические средства фиксации не всегда точно определяют фактического нарушителя, а лицо, зарегистрированное как собственник транспортного средства, не обязательно является участником правонарушения. Установка скрытых технических устройств вызывает вопросы, связанные с правами водителей на осведомлённость о размещении контрольных точек фиксации. С 1 сентября 2024 года вступили в силу изменения, внесённые в Федеральный закон «Об автомобильных дорогах и о дорожной деятельности» [1], предусматривающие обновлённый порядок размещения автоматических систем фиксации нарушений на улично-дорожной сети. Законодательно

[1] Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 8 ноября 2007 г. № 257-ФЗ (с изм. от 20 марта 2025 г.) // Собрание законодательства РФ. – 2007. – № 46. – Ст. 5553.

урегулирован механизм определения мест установки оборудования, что направлено на обеспечение правовой прозрачности и повышение доверия участников дорожного движения к системе контроля.

«В настоящее время полицией стала использоваться технология автоматической идентификации человека по его фото- и видеоизображениям, которая позволяет автоматически идентифицировать или верифицировать человека на фото, видео или вживую. Для распознавания используют нейросети, которые умеют считывать и анализировать уникальные черты человеческого лица, а затем сверять их с базой. Так, система распознавания лиц «FindFace Security», примененная в России в период проведения чемпионата мира по футболу 2018 г., позволила задержать более 180 правонарушителей, часть из которых находилась в федеральном розыске»[1].

В процессе реализации мероприятий по цифровому преобразованию деятельности полиции выявляются отдельные затруднения, препятствующие достижению установленных нормативных ориентиров. Одной из сохраняющихся проблем остаётся утечка персонализированной информации, находящейся в ведомственных информационных ресурсах. Фиксируются случаи неправомерного распространения сведений, в том числе из баз данных, связанных с деятельностью Государственной инспекции безопасности дорожного движения. Источниками подобных инцидентов становятся либо действия сотрудников, обладающих доступом к конфиденциальной информации и нарушающих установленные правила обращения с данными, либо вмешательство посторонних лиц, осуществляющих несанкционированный доступ к цифровым системам. В последнем случае речь идёт о преднамеренных атаках на программно-аппаратную инфраструктуру с целью получения сведений о гражданах и использования этих данных для дальнейшего контроля, наблюдения или иных противоправных целей. Последствием подобных вмешательств становится утечка информации, представляющей

[1] Токарева С.Н. Цифровизация в деятельности органов правопорядка / С.Н. Токарева // Россия: тенденции и перспективы развития. – 2019. – № 14 (2). – С. 590.

государственную, коммерческую или частную ценность[1]. Согласно сведениям Роскомнадзора, в 2024 году произошёл инцидент, в результате которого в открытые источники попали данные о 500 миллионах пользователей, зарегистрированных на территории Российской Федерации[2]. Эти события подтверждают наличие системной угрозы конституционно гарантированному праву на неприкосновенность частной жизни. В условиях таких нарушений утверждение о качественном переходе к цифровому управлению с применением информационных технологий становится преждевременным.

Несмотря на усиление правового механизма в части введения дополнительных мер административного и уголовного характера за нарушение требований по обеспечению безопасности персональных данных, обозначенная проблема не получила эффективного решения. Статистические данные фиксируют устойчивую тенденцию к росту числа правонарушений в этой сфере, что указывает на необходимость пересмотра организационно-технических основ защиты информации в контексте цифровизации государственного управления.

В содержании Концепции цифровой трансформации обозначено несколько приоритетных направлений, среди которых ключевое место занимает формирование среды цифрового доверия. Нарушение требований к защите персональной информации, проявляющееся в случаях утечки данных, оказывает негативное воздействие на реализацию конституционных гарантий, затрагивая как личные, так и имущественные интересы граждан. В подобных обстоятельствах уровень доверия к предоставляемым полицейскими структурами услугам, в том числе через инфраструктуру многофункциональных центров, не демонстрирует положительной динамики. При активной интеграции цифровых решений в правоприменительную деятельность сохраняется разрыв между уровнем технического развития и степенью нормативной и

[1] Бучакова М.А. Персональные данные и их защита в условиях цифровизации общества / М.А. Бучакова // Алтайский юридический вестник. – 2021. – № 2. – С. 44.

[2] Роскомнадзор сообщил об утечке 500 млн данных о россиянах за один раз [Электронный ресурс]. Режим доступа: URL: https://www.rbc.ru/ (дата обращения: 20.06.2025).

организационной готовности, что формирует дисбаланс, способствующий возникновению рисков нарушения прав и свобод человека.

Переход к функционированию в условиях цифровой среды требует от сотрудников органов внутренних дел наличия специфических знаний, ориентированных на работу с информационными технологиями. Исследовательские подходы указывают на необходимость формирования устойчивых цифровых и коммуникативных компетенций у лиц, задействованных в правоохранительной сфере[1]. Обязанности сотрудников полиции уже не ограничиваются выполнением задач в рамках административно-правового и уголовно-процессуального регулирования. Эффективность деятельности в современных условиях требует владения методами работы с цифровыми платформами, обработки и защиты данных, взаимодействия с электронными системами. На фоне технологического обновления зафиксирована проблема кадрового дефицита, отражённая в оценке министра внутренних дел Российской Федерации В.А. Колокольцева. Высокая текучесть кадров затрудняет не только внедрение цифровых средств, но и реализацию традиционных административных процедур, дестабилизируя внутренние организационные процессы[2].

Трансформация системы МВД в цифровом измерении формирует новые направления функциональной деятельности[3]. Реализация поставленных задач требует внедрения целого комплекса решений: профессиональной подготовки сотрудников в сфере информационных технологий, модернизации электронных

---

[1] См.: Мантуров О.С., Ганага В.С. Коммуникативные компетенции сотрудников полиции в цифровом пространстве / О.С. Мантуров и др. // Полицейская деятельность. – 2020. – № 5. – С. 1-17; Челубеева Н.Н., Байдаев М.М. Цифровая трансформация профессиональной подготовки сотрудников ОВД: проблемы и перспективы / Н.Н. Челубеева и др. // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – № 1 (15). – С. 227-234; Коблов Ф.Ч. К вопросу о применении инновационных технологий как способа повышения профессионализма сотрудника органов внутренних дел / Ф.Ч. Коблов // Научно-методический электронный журнал Концепт. – 2016. – т.47 – С.20-24.

[2] Глава МВД заявил о критической нехватке полицейских и следователей [Электронный ресурс]. Режим доступа: URL: https://www.rbc.ru/ (дата обращения: 20.06.2025).

[3] Бучакова М.А., Мушаков В.Е. Оптимизация деятельности российской полиции по защите прав человека в условиях цифровизации / М.А. Бучакова и др. // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2022. – № 4. – С. 11.

ресурсов, ведения постоянного мониторинга интернет-пространства, расширения применения интеллектуальных алгоритмов, включая системы автоматического распознавания лиц для профилактики и пресечения противоправных действий. Эффективное противодействие цифровым угрозам возможно исключительно при условии обновления нормативной базы, с учётом закрепления механизмов, ориентированных на защиту интересов личности, устойчивость общественных институтов и обеспечение безопасности государства.

Современный этап развития показывает, что цифровые технологии в системе полиции находятся на стадии структурного становления. Внедрение осуществляется с высокой интенсивностью, однако масштаб охвата и технологическая сложность требуют дополнительной проработки нормативных и процедурных основ. Отдельные аспекты, включая правовые и организационные положения, требуют дальнейшего уточнения и систематизации в рамках актуализированной цифровой стратегии ведомства.

Таким образом, правовое регулирование использования информационно-вычислительных систем в МВД России представляет собой совокупность законов, постановлений и приказов, направленных на улучшение работы полиции с использованием современных цифровых технологий, а также на обеспечение безопасности данных и защиту прав граждан.

ГЛАВА 2. АНАЛИЗ ПРАКТИКИ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТИ ПОЛИЦИИ

§1. Единая система информационно-аналитического обеспечения деятельности МВД России

В 2012 г. согласно приказу МВД России от 30 марта 2012 г. № 205 «Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012-2014 годах»[1] было принято решение о создании Единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России), которая представляет собой комплекс взаимосвязанных цифровых решений, направленных на обработку, структурирование, накопление, хранение и аналитическое использование данных, получаемых в ходе оперативно-служебной деятельности органов внутренних дел. Система предназначена для поддержки управленческих решений, оперативного реагирования, криминологического анализа и информационного взаимодействия между территориальными и центральными подразделениями МВД.

ИСОД функционирует как вертикально интегрированная многоуровневая система, охватывающая всю структуру МВД России. Она аккумулирует массивы данных, поступающих из различных подсистем: автоматизированных рабочих мест (АРМ) сотрудников, оперативных сводок, реестров правонарушений, аналитических отчётов, миграционных баз, систем видеонаблюдения, а также из других государственных информационных систем при наличии межведомственных соглашений.

---

[1] Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах: Приказ МВД России от 30.03.2012 № 205 / Текст приказа официально опубликован не был.

ИСОД МВД России функционирует как интегрированный комплекс автоматизированных информационных решений, программно-аппаратных модулей, технических систем и каналов передачи данных, предназначенных для поддержки процессов, связанных с выполнением служебных задач органов внутренних дел. Данная структура формирует унифицированное информационное пространство, обеспечивающее доступ подразделений министерства к централизованным ресурсам. Использование системы позволяет:

1) реализовывать электронные каналы взаимодействия между ведомственными структурами с соблюдением принципов разграничения полномочий при обращении к данным;

2) оптимизировать процедуры принятия управленческих решений за счёт подготовки аналитических и статистических отчётов, основанных на достоверных и актуализированных сведениях, с возможностью оперативной интерпретации ключевых показателей деятельности;

3) повышать эффективность исполнения государственных задач, минимизируя временные и трудовые ресурсы, необходимые для обработки информационных потоков в рамках предоставления административных сервисов.

«ИСОД МВД России обеспечивает круглосуточный доступ к информационным ресурсам сотрудников полиции практически в любой точке страны. Ключевым элементом ведомственной технологической инфраструктуры является единая система ЦОД, которая начала функционировать 28 февраля 2014 г. и позволила унифицировать применяемые проектно-технические решения, а также эффективно управлять данными, обеспечивая их защиту и регламентированный доступ к ресурсам»[1].

Для обеспечения бесперебойной работы сервисов и объектов ИСОД МВД России, их технической поддержки и обслуживания сформирован единый центр

[1] Аврутин Р.Ю., Габова О.С., Шихалов А.О. Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России: учебно-практическое пособие / Р.Ю. Аврутин и др. – Санкт-Петербург: СПбУ МВД России, 2023. – С.56.

эксплуатации. В качестве основного аналитического ресурса ИСОД применяются так называемые информационные карты (инфокарты), содержащие агрегированные сведения о субъектах правонарушений, событиях, объектах, временных и территориальных признаках. Эти инфокарты используются для анализа криминальных рисков, построения временных цепочек, выявления повторяемости событий и зон повышенной опасности.

Рассмотрим архитектуру ИСОД МВД России. Система состоит из нескольких функциональных подсистем, таких как: 1) ИМТС МВД России; 2) подсистема базового информационно-технологического обеспечения, включающая в свой состав подсистему автоматизированного рабочего места (далее – АРМ) пользователей и систему ЦОД; 3) подсистема автоматизации прикладных задач; 4) подсистема информационной безопасности; 5) подсистема мониторинга и управления; 6) подсистема навигационно-информационного обеспечения мониторинга и управления силами и средствами МВД России; 7) подсистема информационно-аналитической поддержки принятия решений по направлениям деятельности МВД России; 8) подсистема информационно-аналитического обеспечения деятельности оперативно-технических подразделений ОВД. Подсистемы 3-8 имеют непосредственное отношение к пользователю и реализуются в составе прикладных сервисов ИСОД.

Функциональные прикладные сервисы, поддерживающие текущую деятельность структур МВД России, охватывают следующие компоненты:

1) сервис электронной почты МВД России (СЭП) - автоматизированная система передачи текстовых сообщений, обеспечивающая документоориентированную коммуникацию между сотрудниками центрального аппарата, территориальных подразделений, а также служащими и работниками организаций, выполняющих задачи в рамках компетенции органов внутренних дел. СЭП позволяет осуществлять как внутриведомственный обмен, так и взаимодействие с внешними адресатами через электронные каналы связи;

2) система электронного документооборота (СЭД) - цифровой инструмент, направленный на оптимизацию процессов, связанных с обработкой

управленческой документации и представлением документов, обладающих юридической значимостью. СЭД способствует упорядочиванию административных операций и ускоряет процедуру согласования;

3) система видеоконференцсвязи МВД России (СВКС-М) - средство оперативного информационного взаимодействия, предназначенное для повышения скорости обработки управленческих сведений и принятия решений. Система обеспечивает возможность проведения совещаний и консультаций между структурными единицами в режиме реального времени;

4) сервис управления доступом к информационным ресурсам МВД России (СУДИС) - централизованный механизм разграничения полномочий и идентификации субъектов, работающих в ИСОД. Сервис реализует:

- аутентификацию пользователей и сервисов;

- ведение реестров пользователей;

- назначение и отзыв прав доступа;

- регистрацию событий, связанных с обеспечением информационной безопасности;

- обеспечение подписи электронных документов с использованием электронной подписи;

5) ведомственный информационно-справочный портал (ВИСП) - внутренняя цифровая платформа информационного сопровождения управленческой деятельности, предназначенная для пользователей ИСОД МВД России. Портал формирует единое информационное пространство, поддерживает структурирование контента, систематизацию внутренних и межведомственных сведений, а также способствует ускорению доступа к служебной информации. Через ВИСП доступны:

- сведения о структуре министерства;

- справочные данные контактного характера;

- объявления о мероприятиях и нововведениях, касающихся ИСОД;

- актуальная служебная информация.

Работа с ВИСП осуществляется при наличии зарегистрированной учётной записи в СУДИС;

6) официальный интернет-сайт МВД России - публичный ресурс, предназначенный для внешнего информационного обеспечения граждан и организаций. Сайт предоставляет данные о структуре министерства, его руководстве, правовых актах, регулирующих деятельность органов внутренних дел, а также сведения о территориальных подразделениях, в том числе контактную информацию участковых и адреса отделений полиции.

Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России – это:

1) СЦУО – сервис централизованного учета оружия;

2) ФИС ГИБДД-М – сервис федеральной информационной системы Госавтоинспекции;

3) «Следопыт-М» – информационно-поисковый сервис;

4) СОДЧ – сервис обеспечения деятельности дежурных частей;

5) СООП – сервис обеспечения охраны общественного порядка;

6) СПГУ – сервис предоставления государственных услуг;

7) «Ксенон-2» – сервис объединенной поисковой федеральной системы генетической идентификации;

8) ИБД-М – сервис интегрированных банков данных централизованных учетов (модернизированный);

9) «Ретроспектива» – программный комплекс формирования и ведения единого банка данных подразделений архивной информации ОВД;

10) СОМТО – сервис обеспечения деятельности подразделений материально-технического обеспечения МВД России;

11) СОПС – сервис оформления проезда сотрудников МВД России и военнослужащих Росгвардии;

12) СОЭБ – сервис обеспечения экономической безопасности;

13) ЦИАДИС – централизованная интегрированная автоматизированная дактилоскопическая информационная система МВД России;

14) СОДИ – сервис обеспечения оперативно-служебной деятельности НЦБ Интерпола МВД России;

15) СОКД – сервис обеспечения кадровой деятельности;

16) СОШП – сервис обеспечения деятельности организационно-штатных подразделений;

17) СОДПП – сервис обеспечения деятельности правовых подразделений системы МВД России;

18) САПД УЗС – сервис автоматизированной проверки документов, лиц и транспортных средств на объектах учетно-заградительной системы подразделений МВД России;

19) Сервисы ГУВМ – сервис Главного управления по вопросам миграции МВД России;

20) ЦАФАП – сервис для автоматизации деятельности центров автоматизированной фиксации административных правонарушений в области дорожного движения.

Перечень действующих прикладных сервисов, функционирующих в рамках Информационной системы обеспечения деятельности МВД России, не носит окончательного характера. Структура ИСОД МВД России подвергается регулярному обновлению: внедряются новые цифровые модули, актуализируется функционал ранее интегрированных решений, происходят изменения в их наименованиях. Получение достоверной информации о текущем составе сервисов возможно посредством обращения к официальному ресурсу ИСОД, функционирующему в закрытом ведомственном контуре. Основной состав компонентов ИСОД, а также положения, регламентирующие эксплуатацию телекоммуникационной сети, закреплены в служебных нормативных документах, доступ к которым ограничен в соответствии с режимом конфиденциальности.

Несмотря на наличие широкого спектра доступных информационных сервисов, непосредственную практическую ценность для сотрудников оперативных подразделений представляют лишь те источники, содержание

которых соотносится со специфическими направлениями оперативно-розыскной деятельности. Учитывая характер выполняемых задач, приоритетное значение имеют информационные блоки, способные обеспечить актуальные сведения, подлежащие последующему включению в оперативную разработку. В связи с этим необходимо рассмотреть структуру и содержание ресурсов, используемых оперативным составом для выполнения должностных обязанностей в рамках информационного сопровождения оперативно-служебной деятельности.

1. Информационно-поисковый сервис «Следопыт-М» (ИПС «Следопыт-М») «разработан и внедрен в состав ИСОД для использования непосредственно в интересах оперативных подразделений МВД России и предназначен для поиска, сбора, обработки и представления информации, получаемой из включенных в состав сервиса разнородных информационных систем и баз данных, используемых в оперативных подразделениях МВД России на федеральном, межрегиональном, региональном и территориальном уровнях. Внедрение ИПС «Следопыт-М» призвано повысить эффективность информационного обеспечения деятельности оперативных подразделений МВД России за счет снижения трудозатрат и сокращения времени на получение необходимых сведений путем формирования единого поискового запроса, сбора, обработки информации, досье в рамках унифицированного интерфейса и статистической отчетности»[1].

2. Информационно-поисковая система «Сервис ИСОД МВД России «Незаконный оборот наркотиков» (Сервис «НОН») предназначена для обеспечения инструментальной и информационной поддержки деятельности сотрудников оперативных подразделений центрального аппарата и территориальных органов МВД России, отвечающих за организацию раскрытия и расследования преступлений в сфере незаконного оборота наркотиков. Областью применения Сервиса «НОН» являются следующие виды оперативно-

[1] Искалиев Р.Г., Телков А.В. К вопросу о противодействии преступлениям экономической и коррупционной направленности, совершаемым с использованием IT-технологий / Р.Г. Искалиев и др. // Закон и право. – 2021. – № 11. – С. 118.

служебной деятельности подразделений ГУНК МВД России и территориальных органов МВД России на региональном и районном уровнях:

- выявление, предупреждение, пресечение и раскрытие преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров путем поиска, систематизации и анализа информации, полученной путем взаимодействия с интегрированными сервисами ИСОД МВД России (СООП, СОДЧ, ИБД-Ф, ФИС ГИБДД-М, СПО «Мигрант», АС «Российский паспорт», ПТК «Розыск-Магистраль»), базовыми сущностями единого списка физических лиц (ЕСФЛ) и нормативно-справочной информации (НСИ);

- обеспечение централизованного учета и контроля структурными подразделениями органов внутренних дел за исполнением лицами обязанности, возложенной судьями в порядке части 2.1 статьи 4.1 Кодекса об административных правонарушениях Российской Федерации[1] (далее - КоАП РФ);

- осуществление контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров, а также реализация мер по противодействию их незаконному обороту;

- учет, поиск и анализ оперативно значимой информации, содержащей сведения о потребителях наркотических средств, преступниках и правонарушителях в сфере незаконного оборота наркотиков;

- формирование статистических и аналитических отчетов установленной формы, в том числе в графической форме[2].

3. Сервис обеспечения экономической безопасности (СОЭБ) предназначен для реализации функций ввода, накопления, обработки и анализа оперативно-

---

[1] Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30 декабря 2001 г. № 195-ФЗ (с изм. от 21 апреля 2025 г.) // Собрание законодательства РФ. – 2002. – №1 (ч. 1). – Ст. 1.

[2] Черняков С.А., Горбатенко С.Л. Возможности использования сервисов Единой системы информационно-аналитического обеспечения деятельности МВД России в оперативно-разыскной деятельности органов внутренних дел / С.А. Черняков и др. // Проблемы правоохранительной деятельности. – 2023. – № 4. – С. 53.

служебной, аналитической и оперативно-разыскной информации в Главное управление экономической безопасности и противодействия коррупции МВД России (далее – ГУЭБиПК МВД России), а также в подразделениях экономической безопасности и противодействия коррупции (далее – ЭБиПК) территориальных органов внутренних дел МВД России на региональном и районном уровнях[1].

«Сервис СОЭБ выполняет следующие функции и задачи: автоматизирует процесс учета и регистрации информации о результатах оперативно-служебной деятельности ГУЭБиПК МВД России подразделений ЭБиПК территориальных органов МВД России; обеспечивает информационное взаимодействие ГУЭБиПК МВД России с Экспертно-криминалистическим центром МВД России (далее - ЭКЦ МВД России) и подразделениями ЭБиПК территориальных органов МВД России в сфере борьбы с преступностью экономической и коррупционной направленности; осуществляет обработку, анализ и хране-ние данных, получаемых в процессе оперативно-служебной деятельности ГУЭБиПК МВД России и подразделений ЭБиПК территориальных органов МВД России; формирует единый банк данных, где содержится информация о результатах оперативно-служебной деятельности ГУЭБиПК МВД России, подразделений ЭБиПК территориальных органов МВД России и сведения, поступающие из ЭКЦ МВД России о фальшивых денежных знаках»[2].

4. Сервис интегрированных банков данных централизованных учетов (ИБД-М) предназначен для повышения эффективности оперативно-служебной деятельности ОВД по формированию, ведению и использованию массивов централизованных оперативно-справочных, криминалистических и разыскных учетов ОВД. Сервис ИБД-М включает в себя следующие подсистемы, возможности которых могут быть использованы сотрудниками оперативных

---

[1] Родивилина В.А. Развитие информационного обеспечения деятельности МВД России / В.А. Родивилина // Криминалистика: вчера, сегодня, завтра. – 2025. – № 1. – С. 51.

[2] Фастович Г.Г. Правовое регулирование информационно-аналитической работы органов МВД России: теоретико-правовой аспект / Г.Г. Фастович // Право и государство: теория и практика. – 2023. – № 4(220). – С. 76.

подразделений: Интегрированный банк данных; Обработчик запросов; Сведения ФСБ; ФР-Оповещение; ОСК; АБД-Центр; Криминал-И; Оружие; Автопоиск; Антиквариат; Номерные вещи; Паспорт-Центр; АСВ-РИФ; Реестр задержанных; Государственная защита[1].

5. Сервис централизованного учета оружия (СЦУО) предназначен для централизованного учета и контроля за оборотом нарезного боевого, служебного и гражданского оружия, гранатометов, реактивных пехотных огнеметов, переносных зенитно-ракетных и противотанковых комплексов на территории Российской Федерации. В состав СЦУО включены представляющие интерес для оперативных подразделений МВД России подсистема ЦСМ СЦУО и подсистема «АИПС «Оружие-МВД», которая, в свою очередь, имеет в составе комплекса модули: Физические лица; Юридические лица; Иностранцы; Частные охранники; Бланки; Наградное оружие[2].

6. Сервис для автоматизации деятельности центров автоматической фиксации административных правонарушений «Паутина» (Сервис «Паутина») предназначен для совершенствования деятельности ОВД по фиксации, предупреждению, пресечению и раскрытию преступлений и правонарушений, выявлению похищенных или находящихся в угоне транспортных средств, транспортных средств участников дорожного движения, скрывшихся с мест дорожно-транспортных происшествий[3].

7. Сервисы управления Главного управления по вопросам миграции (сервисы по вопросам миграции) предназначены для обеспечения деятельности полиции в сфере миграции, а также их взаимодействия с соответствующими органами государственной власти Российской Федерации и организациями.

---

[1] Романов А.Ю. Информационные сервисы МВД России / А.Ю. Романов // Специальные информационные технологии: сборник докладов межведомственной научно-практической конференции. – М., 2017. – С. 19.

[2] Веселова Я.А. Применение ИСОД в органах внутренних дел / Я.А. Веселова // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сборник материалов конференции. – Воронеж, 2022. – С. 23.

[3] Майоров В.И. Совершенствование использования технических средств фотовидеофиксации нарушений правил дорожного движения на основе цифровых технологий / В.И. Майоров // Безопасность дорожного движения. – 2023. – № 3. – С. 44.

«Сервисы по вопросам миграции включают в себя следующие интегрированные подсистемы, возможности которых могут быть использованы в практической деятельности сотрудниками оперативных подразделений:

- автоматизированная система аналитической отчетности государственной информационной системы миграционного учета (АСАО ГИСМУ): предназначена для фиксации и учета событий, происходящих с участием иностранных граждан на территории России, получения полной, достоверной и своевременной информации об иностранных гражданах, пересекающих государственную границу Российской Федерации, обеспечения системы регистрационного учета граждан Российской Федерации, системы ведения адресно-справочной работы, системы межведомственного взаимодействия по доступу к учетным данным и организации обмена информацией;

- центральный банк данных по учету иностранных граждан и лиц без гражданства «Мигрант-1» (АС ЦБД УИГ «Мигрант-1»): предназначен для учета иностранных гражданах и лиц без гражданства, временно или постоянно проживающих на территории России;

- Единый информационный ресурс регистрационного и миграционного учета (ЕИР РМУ): предназначен для формирования единого федерального информационного регистра, содержащего сведения о населении, а также для формирования соответствующих выгрузок сведений;

- программное предохранительное обеспечение «Территория» (ППО «Территория»): предназначена для реализации функции регистрации и снятия с регистрационного учета по месту пребывания в электронном виде гражданина Российской Федерации, а также постановки на миграционный учет и снятие с миграционного учета иностранных граждан и лиц без гражданства по месту пребывания»[1].

ИСОД МВД России занимает особое значение в аналитической деятельности МВД. Система аккумулирует разнородные данные, включая

[1] Матросова Л.Д. Использование автоматизированных баз данных в учебном процессе / Л.Д. Матросова // Наука и практика. – 2023. – № 2. – С. 135.

сведения о преступлениях, лицах, находящихся в розыске, криминогенной обстановке в регионах. На базе ИСОД формируются информационные массивы для прогнозирования угроз и построения моделей реагирования. Функционирование прикладных сервисов, входящих в состав информационно-справочной системы органов внутренних дел, осуществляется на основе унифицированных технологических и программных регламентов, ориентированных на выполнение специализированных задач. Такая унификация обеспечивает совместимость модулей и упрощает их внедрение в структуру ИСОД МВД России.

Доступ к элементам системы организован посредством ведомственного облачного решения, построенного на базе виртуализированной платформы с территориально распределённой архитектурой центров обработки данных. В этом цифровом контуре размещаются все прикладные модули и соответствующие базы данных, используемые в оперативно-служебной деятельности. В целях реализации проекта произведена оптимизация конфигурации информационно-мультимедийной телекоммуникационной структуры МВД, обеспечивающая прямое подключение всех территориальных подразделений к облачной платформе с сохранением необходимого уровня пропускной способности.

Практические итоги внедрения системы подтверждают её значимость: в 2024 г. по данным МВД России, свыше 40 процентов расследованных преступлений категорий тяжёлой и средней степени тяжести сопровождались использованием аналитических данных, сформированных с применением инструментов ИСОД[1]. Такой результат позволяет рассматривать систему как важный элемент повышения результативности оперативно-розыскной деятельности.

[1] Краткая характеристика состояния преступности / Официальный сайт МВД России. Статистика ГИАЦ МВД России. URL: https://www.mvd.ru/Dejatelnost/statistics/reports/ (дата обращения: 20.06.2025).

Таким образом, Единая система информационно-аналитического обеспечения деятельности МВД России служит фундаментом для перехода органов внутренних дел к цифровой модели управления, обеспечивая объективность, полноту и актуальность данных, необходимых для принятия управленческих и оперативных решений. Формирование единого цифрового пространства в системе ОВД способствует модернизации всех направлений оперативно-служебной деятельности. Современные ИТКС позволяют не только фиксировать и обрабатывать данные о правонарушениях, но и формировать предпосылки для прогнозирования, автоматического анализа и целенаправленного реагирования. Эффективность их применения оценивается по показателям раскрываемости преступлений, скорости реагирования, снижению уровня повторной преступности, степени аналитической точности и полноты информационного обмена.

§2. Подсистема информационной безопасности

Значение информационных потоков, обрабатываемых в рамках ИСОД МВД России, предопределяет приоритетность вопросов, связанных с их защищённостью. В системе реализована подсистема обеспечения информационной безопасности (ПОИБ), включающая комплекс современных защитных механизмов. Архитектура ПОИБ построена на принципах централизованного управления, постоянного протоколирования событий, связанных с безопасностью, оперативной реакции на потенциальные угрозы, а также проведения регулярных проверок с целью выявления уязвимостей в структуре ведомственной информационно-технологической среды на всех её уровнях.

Правовые основы функционирования подсистемы информационной безопасности заложены в Федеральном законе от 27.07.2006 № 149-ФЗ «Об

информации, информационных технологиях и о защите информации»[1], а также в Федеральном законе от 26.07.2006 № 152-ФЗ «О персональных данных»[2]. Кроме того, регламентирующие положения закреплены в Приказе МВД России от 9 ноября 2018 г. № 755, которым утверждены вопросы обращения со служебной информацией ограниченного распространения в системе МВД России[3]. Эти нормативные акты определяют требования к организационным, программно-техническим и криптографическим мерам, обязательным к применению в системах МВД.

Структурно подсистема информационной безопасности МВД России охватывает следующие направления:

- организация контроля доступа, включая идентификацию и аутентификацию пользователей по многофакторной схеме;

- применение сертифицированных межсетевых экранов, антивирусной защиты и средств обнаружения вторжений, в том числе в подсетях, обрабатывающих сведения, составляющие государственную тайну;

- шифрование информации при передаче и хранении, с использованием криптосредств, одобренных ФСБ России;

- системы мониторинга, журналирования и анализа событий информационной безопасности, применяемые на центральных и региональных уровнях;

- реагирование на инциденты ИБ, включая разработку планов восстановления и регулярное проведение учебных тревог.

Основной задачей ПОИБ является обеспечение для информации: конфиденциальности, целостности и доступности; защиты; достоверности; непрерывности обработки.

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. от 01 апреля 2025 г.) // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3448.

[2] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (с изм. от 28 февраля 2025 г.) // Собрании законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3451.

[3] О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России: Приказ МВД России от 9 ноября 2018 г. № 755 // Российская газета. – 2018. – 06 дек.

В состав ПОИБ входят средства защиты инфраструктуры, средства защиты сервисов и средства защиты АРМ сотрудников МВД России. Несомненно, что наибольшее значение для обеспечения информационной безопасности ИСОД МВД России имеет эффективность системы защиты АРМ. В ее составе выделяют ряд базовых средств (рис. 2).

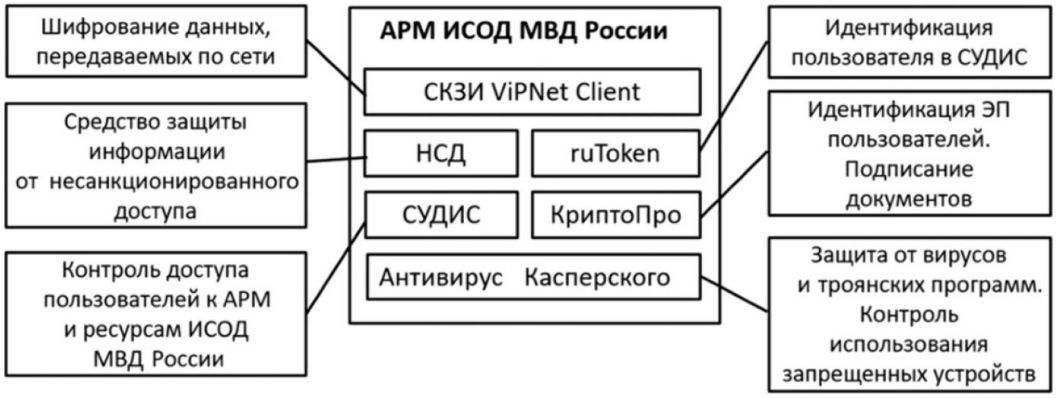

Рис. 2. Состав системы защиты АРМ ИСОД МВД России

СУДИС выполняет функции централизованного контроля над пользовательскими правами и параметрами взаимодействия с цифровыми сервисами системы. СУДИС обеспечивает унифицированный механизм аутентификации, регистрацию инцидентов безопасности, контроль за распределением и изменением полномочий субъектов доступа, включая как физических пользователей, так и сервисные компоненты системы. Предоставление прав доступа к функционалу осуществляется с использованием электронной подписи. Указанная система входит в состав базовой инфраструктуры защиты информации, являясь составным элементом архитектуры обеспечения безопасности ИСОД МВД России.

«Учитывая, что основные уязвимости информационных систем обусловлены недекларированными возможностями зарубежного программного обеспечения, СУДИС является собственным отечественным программным обеспечением, реализующим функционал защиты от несанкционированного

доступа к информации в части идентификации и аутентификации пользователей ИСОД МВД России. В целях минимизации угроз проникновения в информационные системы вредоносного кода в рамках ПОИБ ИСОД МВД России сформирована инновационная технологическая инфраструктура антивирусной защиты на основе антивируса Касперского, на сегодняшний день не имеющая в стране аналогов по масштабности. К указанной системе подключены пользовательские АРМ и серверное оборудование. Антивирус Касперского обеспечивает защиту от вредоносного программного обеспечения, от почтового спама, позволяет сохранять целостность информации, проводить инвентаризацию программного и аппаратного обеспечения, контролировать использование внешних съемных устройств. Антивирус является обязательным элементом любой современной информационной системы»[1].

На информационные ресурсы МВД России фиксируется устойчиво высокий уровень кибератак, что указывает на особую значимость ИТ-инфраструктуры данного ведомства. В ответ на выявленные угрозы, в сотрудничестве с Федеральной службой безопасности разработан специализированный сегмент государственной системы обнаружения, предотвращения и нейтрализации последствий компьютерных атак - СОПКА МВД, обеспечивающий реагирование на инциденты в информационном пространстве

«КриптоПро позволяет применять электронную подпись при работе с сервисами ИСОД МВД России, а именно идентифицировать пользователей по электронной подписи (доступ в систему, доступ к сервисам ИСОД МВД России), производить подписание электронных документов в СЭД. Без использования КриптоПро работа с электронной подписью в ИСОД МВД России невозможна. Порядок изготовления ключа электронной подписи, получения сертификата

[1] Вермеенко Я.С. Современное состояние и перспективы развития ИСОД МВД России / Я.С. Вермеенко // Академическая мысль. – 2021. – № 3 (16). – С. 75.

ключа проверки электронной подписи, а также процедура отзыва сертификата определены в регламенте Удостоверяющего центра МВД России»[1].

«Рутокен (ruToken) обеспечивает хранение электронной подписи сотрудника МВД России на его персональном идентификаторе, позволяет входить в систему и сервисы ИСОД МВД России без дополнительного ввода логина и пароля, производить блокировку АРМ при извлечении идентификатора. Использование ruToken с записанной на нем электронной подписью обеспечивает доступ к сервисам ИСОД МВД России»[2].

«Средство криптографической защиты информации (далее – СКЗИ) ViPNet Client обеспечивает защиту информации при ее передаче по каналам связи, защиту от сетевых атак на уровне АРМ, позволяет обмениваться информацией по открытым каналам связи с использованием шифрования. В связи с территориальной распределенностью объектов МВД России, а также в соответствии с требованиями ФСБ России защита каналов связи является обязательной. С учетом территориально распределенной инфраструктуры ИСОД МВД России на базе ИМТС МВД России сформирована VPN-сеть с использованием криптографических средств линейки ViPNet. Указанные средства были своевременно приобретены и переданы в соответствии с потребностями в территориальные органы МВД России. В состав комплекса СКЗИ входят ViPNet Administrator, ViPNet StateWatcher, ViPNet Client, а также программно-аппаратные комплексы ViPNet Coordinator HW 1000 и ViPNet Coordinator HW 2000. Во всех территориальных органах МВД России организован защищенный VPN-канал до ЦОД МВД России и развернуты центры управления региональными защищенными сетями»[3].

---

[1] Кирюшин И.И., Иванов И.П., Тимофеев В.В., Жмурко Д.Ю. Использование технологии блокчейна в правоохранительной деятельности / И.И. Кирюшин и др. // Полицейская деятельность. – 2024. – № 1. – С.31.

[2] Там же.

[3] Воронов А.М., Анисифорова М.В. Перспективы внедрения новых информационных технологий в деятельность органов внутренних дел по профилактике правонарушений / А.М. Воронов и др. // Вестник ВИПК МВД России. – 2024. – № 2 (70). – С.43.

Техническую реализацию подсистемы ИБ обеспечивают департамент информационных технологий МВД России, региональные службы ИБ, а также взаимодействующие подразделения ФСБ и ФСТЭК России.

Внедрение ОС Astra Linux Special Edition в МВД России обеспечивает техническую поддержку мандатного контроля доступа, защищённой загрузки, разграничения прав пользователей и аудита действий. Системы работают в рамках закрытых контуров с ограничением внешнего сетевого взаимодействия, что снижает вероятность проникновения вредоносного кода и внешнего воздействия.

Проблемы подсистемы информационной безопасности связаны с:

- недостаточной защищенностью региональных серверов, особенно в подразделениях с устаревшей техникой;

- неоднородностью внедрённых решений, обусловленной различиями в технической оснащённости;

- отсутствием единой системы автоматического реагирования на инциденты во всех регионах;

- кадровым дефицитом в области ИБ на местах, особенно в отдалённых территориальных управлениях.

Таким образом, подсистема информационной безопасности МВД России представляет собой многоуровневую систему, интегрированную во все информационные процессы ведомства и обеспечивающую функционирование критически важных цифровых сервисов в условиях высокого уровня угроз. Функционирование информационно-телекоммуникационных систем МВД России обусловлено необходимостью обработки большого объёма персональных, служебных и оперативных данных, значительная часть которых относится к категории ограниченного доступа. Это определяет приоритетное значение подсистемы информационной безопасности, являющейся структурным элементом всей цифровой инфраструктуры МВД России и обеспечивающей защиту информации от несанкционированного доступа, утечки, искажения и уничтожения. Эффективность её работы требует постоянной модернизации,

унификации программно-аппаратных решений, а также совершенствования нормативной базы и подготовки профильных специалистов.

§3. Сервис электронного документооборота

Современная система электронного документооборота (ЭДО) МВД представляет собой совокупность программных и организационных средств, обеспечивающих автоматизированное создание, регистрацию, передачу, согласование, подписание и хранение документов в цифровом формате. Внедрение ЭДО в структуру МВД направлено на повышение эффективности делопроизводства, сокращение сроков рассмотрения обращений, снижение бумажного документооборота и обеспечение прозрачности управленческих процедур.

Функционирование системы ЭДО осуществляется в рамках Паспорта национальной программы «Цифровая экономика Российской Федерации» (утв. 24 декабря 2018 г. № 16)[1], а также в соответствии с положениями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»[2], устанавливающего юридическую значимость электронных документов, подписанных усиленной квалифицированной электронной подписью. В МВД России ЭДО внедряется с учетом требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с соблюдением норм конфиденциальности, целостности и доступности служебной информации.

---

[1] Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16) / Текст паспорта официально опубликован не был.

[2] Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (с изм. от 21 апреля 2025 г.) // Собрание законодательства РФ. – 2011. – № 15. – Ст. 2036.

Технической основой электронного документооборота в МВД выступает система «СЭД МВД России» (Система электронного документооборота МВД РФ), интегрированная с другими внутренними и межведомственными цифровыми платформами: ИСОД, порталом «Госуслуги», системой «Межведомственный электронный взаимодействие» (СМЭВ) и единой биометрической системой. Работа СЭД организована на базе защищенных каналов связи, с разграничением доступа по уровням допуска, использованием средств криптографической защиты информации, сертифицированных ФСБ России[1].

В практической плоскости СЭД МВД реализует:

- электронную регистрацию входящих и исходящих писем;

- автоматизированную маршрутизацию поручений по структуре МВД;

- электронное визирование и подписание документов;

- контроль исполнения сроков и формирование отчётности;

- архивное хранение документов в соответствии с требованиями Федерального закона от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»[2].

В основу проектирования системы электронного документооборота (СЭД) положен принцип сервисно-ориентированной архитектуры (SOA), предполагающий структурирование информационной системы на функционально изолированные, стандартизированные и взаимозаменяемые сервисные компоненты. Каждый такой компонент функционирует автономно либо в составе иных программных решений, с возможностью последующего выделения для независимого использования.

СЭД решает задачи, направленные на:

---

[1] Харитонова С.А. Организационно-правовые проблемы использования системы электронного документооборота в системе МВД / С.А. Харитонова // Молодой ученый. – 2024. – № 35 (482). – С. 121.

[2] Об архивном деле в Российской Федерации: Федеральный закон от 22 октября 2004 г. № 125-ФЗ (с изм. от 13 декабря 2024 г.) // Собрание законодательства РФ. – 2004. – № 43. – Ст. 4169.

- обеспечение полноты и своевременности информационной поддержки управленческих решений в структуре МВД России;

- повышение эффективности делопроизводственной и административной деятельности, осуществляемой территориальными подразделениями и подведомственными организациями;

- развитие механизмов юридически значимого электронного документооборота между структурными единицами;

- формирование унифицированного информационного пространства документационного обеспечения органов внутренних дел;

- рационализацию движения документов на различных уровнях системы МВД;

- стандартизацию работы с электронными материалами при сохранении управляемости, доступности и защищённости информационных ресурсов;

- реализацию непрерывного контроля за прохождением документации и усиление дисциплины исполнения служебных обязанностей;

- обеспечение защищённого канала обмена документами в рамках функционирования СЭД;

- организацию безопасного хранения данных и ограничение доступа к информации, включая обязательное протоколирование действий пользователей и применение электронной подписи.

Система электронного документооборота функционирует как инструмент комплексной обработки различных категорий документов. В перечень обрабатываемых материалов входят входящие корреспонденции, обращения граждан, нормативные правовые документы, приказы и иные управленческие акты. Система осуществляет их регистрацию, контроль исполнения, формирование архивных записей. Имеется возможность получения сведений из внешних источников, включая платформы межведомственного электронного документообмена и официальный ресурс МВД России.

Функциональность СЭД охватывает механизмы поиска по зарегистрированным документам, использование справочных классификаторов,

формирование отчётной документации и создание дел в соответствии с утверждённой номенклатурой.

Архитектура СЭД содержит несколько категорий сервисов:

- интеграционные компоненты обеспечивают синхронизацию процессов документооборота между подразделениями МВД, формируя единое информационное пространство;

- документационные модули предназначены для автоматизации деятельности сотрудников, ответственных за ведение делопроизводства, включая регистрацию, маршрутизацию и контроль документов;

- мобильные решения адаптированы для планшетных устройств, с целью упрощения вынесения руководящих решений и направления поручений.

Пользователь при авторизации в СЭД получает доступ к интерфейсу, соответствующему его должностной роли - будь то руководитель, делопроизводитель или исполнитель. Выбор сервиса «Документы» позволяет перейти к карточкам регистрации, содержащим полную информацию о каждом документе. Интерфейс обеспечивает просмотр содержимого, контроль за прохождением и доступ к истории обработки.

Эксплуатация СЭД регламентирована требованиями, закреплёнными в Инструкции по делопроизводству в органах внутренних дел Российской Федерации (утверждена приказом МВД России от 2 сентября 2024 г. № 515[1]). Применение данной системы ограничивается административными задачами, связанными с внутренним документооборотом и формированием юридически значимых записей.

Особенность функционирования системы СЭД МВД заключается в наличии режима обработки сведений ограниченного доступа. Документооборот, связанный с государственной тайной, реализуется в рамках специального защищённого сегмента, доступ к которому возможен только при наличии

[1] Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации: Приказ МВД России от 2 сентября 2024 г. № 515 / Официально приказ опубликован не был.

соответствующих допусков и средств защиты (включая мандатную модель разграничения доступа, реализованную на базе ОС Astra Linux Special Edition).

Согласно данным Министерства цифрового развития, связи и массовых коммуникаций РФ, к концу 2024 года доля внутренних служебных документов МВД, оформленных в электронном виде, превысила 85 % от общего объёма делопроизводства. В ведомстве функционирует более 140 тыс. автоматизированных рабочих мест, оборудованных СЭД и обеспечивающих сквозную цифровую обработку документов во всех территориальных органах[1]. Тем не менее, на этапе внедрения зафиксированы отдельные трудности, в частности: необходимость переподготовки кадров, проблемы миграции архивных данных из устаревших систем, несогласованность внутренних регламентов между подразделениями. Для устранения этих затруднений в МВД России действует рабочая группа по мониторингу хода цифровизации документооборота, координируемая Главным управлением информационных технологий МВД РФ.

Таким образом, система электронного документооборота в МВД России представляет собой важнейший элемент цифровой трансформации управления ведомством. Она способствует сокращению сроков принятия решений, упрощает межведомственное взаимодействие и обеспечивает юридическую значимость и защиту информации в электронном формате.

§4. Федеральная информационная система Государственной инспекции безопасности дорожного движения МВД России

[1] Харитонова С.А. Организационно-правовые проблемы использования системы электронного документооборота в системе МВД / С.А. Харитонова // Молодой ученый. – 2024. – № 35 (482). – С. 122.

Приказом МВД России от 05.02.2016 № 60 «О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции»[1] с целью совершенствования информационного обеспечения подразделений Госавтоинспекции и иных подразделений ОВД было принято решение о необходимости введения в эксплуатацию с 01.08.2016 специального программного обеспечения федеральной информационной системы Госавтоинспекции (далее - Система, ФИС «ГИБДД-М») на базе инфраструктуры единой системы информационно-аналитического обеспечения деятельности МВД России. ФИС ГИБДД-М разработано в интересах Главного управления по обеспечению безопасности дорожного движения МВД России и предназначено для обеспечения деятельности подразделений Госавтоинспекции, а также их взаимодействия с соответствующими органами государственной власти и организациями.

Федеральная информационная система «ГИБДД-М» ориентирована на решение ряда технологических и организационных задач, связанных с совершенствованием деятельности подразделений Государственной инспекции безопасности дорожного движения. К приоритетным направлениям функционирования системы относится обеспечение цифрового сопровождения административных процедур, регламентирующих регистрацию транспортных средств, оформление водительских удостоверений, а также доступ к сведениям о правонарушениях, зафиксированных в административном порядке.

Дальнейшее развитие системы направлено на стандартизацию архитектуры автоматизированных решений, применяемых в подразделениях ГИБДД, с приведением их к современным требованиям по устойчивости, доступности и целостности обрабатываемых данных. Наряду с этим реализуется задача интеграции с иными ведомственными платформами в целях

---

[1] О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции: Приказ МВД России от 5 февраля 2016 г. № 60 / Текст приказа официально опубликован не был.

формирования единого информационного массива, поддерживающего внутреннее взаимодействие в структуре МВД России.

Среди технических целей - формирование универсальной модели представления данных, на базе которой функционирует система, а также обеспечение непрерывной работы в режиме синхронной обработки запросов. Механизмы реализации проекта предполагают снижение совокупных затрат на проектирование, эксплуатацию и техническое сопровождение программных комплексов, применяемых в деятельности подразделений ГИБДД.

В состав специального программного обеспечения ФИС ГИБДД-М входят пять подсистем:

1. Подсистема «Транспортные средства» автоматизирует регистрацию транспортных средств и прицепов, обеспечивает предоставление государственной услуги и поддерживает межведомственный обмен сведениями.

Функционал системы охватывает: приём и обработку заявлений на регистрационные действия и изменения данных; заверение информации с использованием электронной подписи уполномоченного сотрудника; поиск сведений о транспортных средствах и истории их регистрационных операций; формирование реестра с данными о выданных документах, паспортах ТС, номерах и регистрационных действиях; сохранение решений об отказах с цифровой подписью; проверку на ограничения по регистрации, фактам розыска, утрате, распределению или недействительности спецпродукции, с фиксацией даты, времени и исполнителя проверки; подготовку и печать необходимого пакета регистрационных документов; верификацию серий и номеров специальных бланков на соответствие и наличие по базе подсистемы «Специальная продукция»; автоматическую регистрацию использованных и испорченных бланков спецпродукции, применённых при регистрационных действиях. Доступ к системе предоставляется инспекторам регистрационно-экзаменационных отделений ГИБДД, уполномоченным на проведение регистрационных операций с транспортом и прицепами.

2. Подсистема «Водительские удостоверения» автоматизирует процессы учета прав на управление транспортными средствами, оформления удостоверений и экзаменационной деятельности Госавтоинспекции. Обеспечивается выполнение регламентов и межведомственный обмен данными при оказании госуслуг.

Основные функции подсистемы: регистрация и обработка заявлений на получение водительских удостоверений с возможностью печати; предоставление сведений о статусе удостоверений; поиск и просмотр данных по удостоверениям; создание электронного реестра выданных документов с заверением квалифицированной подписью. ФИС «ГИБДД-М» формирует доступный для печати реестр по форме, предусмотренной приказом МВД России от 13.05.2009 № 365 «О введении в действие водительского удостоверения»[1]; аннулирование ранее выданных или утраченных удостоверений при замене; проверка заявлений с учетом розыска лиц, документов, административных нарушений, включая учет смены персональных данных; загрузка фото с веб-камеры для персонализации удостоверения; проверка специальных бланков по базе на соответствие форме и наличию; автоматическая регистрация использованных или испорченных бланков в подсистеме «Специальная продукция». Работа с подсистемой обеспечивает соблюдение установленных требований при учёте, оформлении и выдаче водительских документов.

3. Подсистема «Специальная продукция» предназначена для учета и контроля специальных бланков, передаваемых в органы Госавтоинспекции и таможенные структуры. Система регистрирует поступление, распределение, использование и утрату продукции, включая автоматическое формирование перечней недействительных экземпляров. Перечень продукции, определённый приказом МВД России от 27.04.2002 № 390[2], охватывает документы и

---

[1] О введении в действие водительского удостоверения: Приказ МВД РФ от 13 мая 2009 г. № 365 (с изм. от 9 января 2024 г.) // Российская газета. – 2009. – № 132.

[2] О разработке и утверждении образцов специальной продукции, необходимой для допуска транспортных средств и водителей к участию в дорожном движении: Приказ МВД РФ от 27 апреля 2002 г. № 390 (с изм. от 15 августа 2012 г.) // Российская газета. – 2002. – № 89.

регистрационные знаки, необходимые для допуска водителей и транспортных средств к движению. К ним относятся: водительские удостоверения; временные разрешения; паспорта транспортных средств; регистрационные свидетельства; паспорта шасси; справки на номерные агрегаты; регистрационные знаки, включая «ТРАНЗИТ»; международные водительские удостоверения.

Функциональные возможности подсистемы: регистрация данных при получении бланков от изготовителей; фиксация передачи продукции в органы Госавтоинспекции; учёт выдачи юридическим лицам; отражение использования при оформлении документов в рамках предоставления государственных услуг; внесение сведений при порче с одновременным включением в реестр утрат; оформление уничтожения с регистрацией сведений об изъятии; фиксация приёмки продукции для последующей утилизации. Реестр, формируемый системой, содержит информацию о потерянных, уничтоженных, похищенных или забракованных экземплярах, в том числе о документах и регистрационных знаках.

4. Подсистема «Административные правонарушения» служит для цифрового сопровождения делопроизводства по нарушениям в сфере дорожного движения. Система поддерживает взаимодействие с ФССП и Федеральным казначейством, упрощая обработку данных и контроль исполнения.

Функциональные модули обеспечивают: ввод сведений на каждом этапе делопроизводства; поиск и просмотр данных по делам; проверку лиц и транспортных средств по розыскным учетам ФИС «ГИБДД-М»; печать документов, необходимых в рамках административного производства; передачу информации о штрафах в ГИС ГМП через СМЭВ; получение сведений об оплате из ГИС ГМП с автоматическим сохранением; направление документов в ФССП для возбуждения исполнительного производства по неоплаченным штрафам; прием информации от ФССП о ходе принудительного исполнения; автоматическую сверку бланков с данными из подсистемы «Специальная продукция»; регистрацию израсходованных и испорченных бланков; формирование отчетности на основании зарегистрированных нарушений и

выполненных запросов; контроль сроков и автоматическое оформление материалов при просрочке оплаты. Все данные о нарушениях вносятся должностными лицами Госавтоинспекции. В случае фиксации нарушений автоматическими средствами, информация заносится после вынесения постановления в порядке статьи 28.6 КоАП РФ[1].

Корректировка сведений по жалобам осуществляется вручную. При внесении данных система сверяет информацию с базой розыска, проводит двусторонний обмен сведениями о начислениях и оплатах между ФИС «ГИБДД-М» и ГИС ГМП. При начислении штрафа данные автоматически поступают в ГИС ГМП. После оплаты информация возвращается обратно, что позволяет системе зафиксировать исполнение наказания.

Сотрудники полиции используют сведения о правонарушениях при оперативной работе и анализе повторных нарушений, что повышает эффективность надзорной деятельности.

5. Подсистема «Получение и предоставление сведений» служит для организации обмена данными между ФИС «ГИБДД-М» и внешними информационными структурами. Система поддерживает интеграцию с сервисами ИСОД МВД России, федеральными и региональными информационными системами, муниципальными платформами и организациями, исполняющими государственные или муниципальные функции.

Функциональные модули обеспечивают: автоматическую загрузку данных о транспортных средствах, находящихся в розыске; импорт сведений о лицах, объявленных в федеральный розыск; передачу информации в иные подсистемы МВД России. Доступ к модулю осуществляется через вкладку «Запросы» на стартовой странице интерфейса ФИС «ГИБДД-М». Внедрение специализированного программного обеспечения упростило межведомственный и межрегиональный обмен сведениями, повысив эффективность работы

[1] Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30 декабря 2001 г. № 195-ФЗ (с изм. от 21 апреля 2025 г.) // Собрание законодательства РФ. – 2002. – №1 (ч. 1). – Ст. 1.

Госавтоинспекции. Система продолжает развиваться: функциональность оптимизируется, дополняются новые элементы и инструменты.

Работа с подсистемами выстраивается по единому сценарию: пользователь выбирает необходимое действие (например, регистрация автомобиля, аннулирование водительского удостоверения), затем заполняет форму соответствующими данными. Внедрение сервисов ИСОД МВД России сопровождается созданием детальных инструкций, адаптированных под различные категории пользователей. Методические материалы систематически обновляются в связи с расширением функционала.

ФИС «ГИБДД-М» обеспечивает полный цикл обработки запросов и межведомственного обмена внутри структуры Госавтоинспекции. Сотрудники в реальном времени получают сведения о регистрации транспортных средств, ограничениях на управление и пр. Граждане имеют доступ к информации о наложенных административных штрафах и данных об их оплате.

«Детальное описание технологии работы с прикладными сервисами ИСОД МВД России доступно на соответствующем портале, где для каждого сервиса в разделе «Документы» представлены подробные инструкции и регламенты по использованию всех видов программного обеспечения. Конечно, развитие и совершенствование сетевой инфраструктуры ИСОД в части, относящейся к ИМТС МВД России, продолжается и основывается на передовых технологиях, учитывающих основные принципы построения и объединения телекоммуникационных сетей, как технических, так и экономических. К ним относятся:

1) принцип структурности – разбиение телекоммуникационных систем на части и подсистемы, каждая из которых выполняет строго определенные функции и снабжена стандартизованным интерфейсом для взаимодействия с другими подсистемами и сетевым оборудованием;

2) принцип универсальности – построение телекоммуникационных систем с заданными и зафиксированными в стандартах наборами основных технических характеристик;

3) принцип избыточности – обеспечение быстрой адаптации ИМТС МВД России для удовлетворения конкретных потребностей и возможности, не останавливая деятельности пользователей, вносить организационные и технические изменения;

4) принцип иерархичности – создание единой телекоммуникационной системы, систем администрирования и мониторинга, единого адресного пространства в соответствии со структурой и составом ОВД, их подчиненностью и принятой технологией информационного обмена;

5) принцип этапности – пространственно-временное изменение и развитие системы телекоммуникаций и обеспечение ее статусности в каждый момент времени;

6) принцип управляемости – контроль за действиями и процессами и целенаправленность системы. Контроль должен быть предсказуемым, а целенаправленность поддерживается для максимального удовлетворения потребностей пользователей;

7) принцип информативности – опережение спроса (потребностей), что в ИМТС МВД России реализуется на основе создания широкополосных каналов, максимального использования информационной емкости, оптимального распределения информации во времени и пространстве, равномерной загрузки сети»[1].

«Дальнейшее развитие ведомственной инфокоммуникационной платформы является одним из стратегических направлений деятельности МВД России и ведется в рамках совершенствования единой системы информационно-аналитического обеспечения деятельности МВД России. К первоочередным направлениям можно отнести следующие: 1) повышение эффективности функционирования инфокоммуникационных систем в оперативно-служебной деятельности ОВД; 2) создание инфокоммуникационных систем, являющихся

[1] Иншаков М.И. Правовые и организационные аспекты ресурсного обеспечения информационных технологий в органах внутренних дел / М.И. Иншаков // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2021. – № 21-2. – С. 60.

универсальной транспортной средой для передачи информации в интересах всех подразделений ОВД и обеспечивающих, в том числе, мобильный доступ к ведомственным базам данных»[1].

Функционирование инфокоммуникационной платформы МВД требует системной работы по обеспечению информационной безопасности. В этой связи утверждены типовые модели угроз и нарушителей ИСОД МВД, направленные на защиту данных в ведомственных системах. Доступ к сервисам организован через персональные идентификаторы и сертификаты электронной подписи с распределением полномочий.

Цель цифровой трансформации ОВД - формирование внутренней среды взаимодействия на базе единой аналитической платформы. Для этого внедряются интеграционные сетевые решения, обеспечивающие бесперебойную работу ИМТС в составе ИСОД с заданным уровнем технологической устойчивости.

Инфраструктура ОВД достигла высокого уровня развития. Существенным шагом стало внедрение ИСОД МВД - архитектурно завершенной системы с набором сервисов, ориентированных на задачи структур МВД. Построение платформы учитывает дальнейшее расширение информационных связей, рост производительности ИМТС и повышение доступности цифровых функций для сотрудников.

Подведем некоторые итоги второй главы дипломной работы.

1. Применение телекоммуникационных решений в оперативной работе органов внутренних дел осуществляется через Единую систему информационно-аналитического обеспечения МВД. Эта система формирует интегрированную цифровую среду, охватывающую все подразделения министерства, обеспечивает рациональное распределение задач, ускоряет доступ к данным для управленческих звеньев и повышает эффективность обмена сведениями в границах национальной телекоммуникационной инфраструктуры. Все

[1] Комелькова Я.В. Применение информационных технологий в правоохранительной деятельности / Я.В. Комелькова // StudNet. – 2022. – № 5. – С. 26.

рассмотренные платформы соответствуют требованиям Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который устанавливает обязательные нормы по защите данных, функционирующих в государственных ИС. Таким образом, применение ИТК-систем в практике МВД позволяет централизовать управление, обеспечить прозрачность процессов, повысить качество принятия решений и оперативность реагирования на угрозы общественной безопасности. Однако эффективность использования платформ зависит от уровня их интеграции, технической оснащенности, подготовки кадров и нормативного регулирования.

2. В начале 2020 года МВД России инициирована комплексная замена зарубежных программных платформ, основанных на MS Windows, на российскую операционную систему «Astra Linux». Одновременно организовано обучение пользователей и администраторов основам работы с новым программным обеспечением.

3. Эффективность использования современных информационно-телекоммуникационных систем в деятельности полиции» напрямую зависит от степени их интеграции, устойчивости каналов связи, уровня подготовки сотрудников, унификации форматов данных и наличия единого протокола информационного взаимодействия. Проблемы, выявленные в ходе контрольно-ревизионных мероприятий, касаются фрагментарности архитектуры платформ, недостаточной защищенности информации, отсутствия резервных каналов в удаленных территориях.

Таким образом, практическое применение современных информационно-телекоммуникационных систем в деятельности полиции демонстрирует положительную динамику в вопросах обеспечения общественного порядка, раскрытия преступлений, сокращения временных и организационных затрат. При этом эффективность систем требует дальнейшего технологического и нормативного совершенствования.

ГЛАВА 3. ПЕРСПЕКТИВЫ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТИ ПОЛИЦИИ

§1. Перспективные направления интеграции в процесс охраны общественного порядка и обеспечения общественной безопасности инновационных информационно-телекоммуникационных систем

Организация деятельности по охране порядка и обеспечению безопасности населения опирается на внедрение цифровых решений, способствующих повышению эффективности работы подразделений полиции, несущих службу в составе тактических нарядов. При этом, наибольший научно-практический интерес представляют 10 наиболее перспективных направлений интеграции в процесс ООП и ООБ инновационных цифровых систем и технологий, позволяющих обеспечить дальнейшее поступательное совершенствование работы полиции в изучаемой сфере ее деятельности.

1. Разработка алгоритмических решений, обеспечивающих обработку значительных массивов визуальной информации с технических средств наблюдения и иных источников, направлена на идентификацию лиц и фиксацию отклоняющегося поведения. Применение технологий машинного обучения и инструментов анализа больших данных позволяет выявлять потенциально опасные действия, а также осуществлять прогнозирование возможных нарушений правопорядка. Визуальный мониторинг служит одним из основных механизмов предупреждения противоправных деяний в общественных пространствах. Анализ видеозаписей осуществляется вручную или с использованием автоматизированных средств. В первом случае контроль осуществляется оператором, что требует значительных временных ресурсов и не всегда обеспечивает необходимую точность. Второй подход предполагает

применение программных средств, базирующихся на алгоритмах искусственного интеллекта, позволяющих распознавать образы, проводить сопоставление с базами данных и выявлять лиц, представляющих потенциальную угрозу. Благодаря автоматизации удаётся существенно повысить скорость и точность обработки данных, что обеспечивает оперативную реакцию правоохранительных органов. Важной функцией систем интеллектуального видеонаблюдения выступает распознавание лиц. Современные алгоритмы способны одновременно обрабатывать множество изображений и идентифицировать совпадения с информацией, содержащейся в специализированных регистрах. Эти алгоритмы функционируют в режиме реального времени, обеспечивая мгновенную передачу сведений о зафиксированных лицах. Интеграция видеоаналитических систем с архитектурой комплекса технических средств, таких как «Безопасный город», расширяет возможности автоматического контроля. Взаимодействие с системами контроля доступа способствует предупреждению несанкционированного проникновения на охраняемые территории. Фиксация нарушений, сопряжённых с несоблюдением административных предписаний в общественной среде, осуществляется посредством интеллектуальных средств видеоаналитики[1]. Применение этих технологий способствует своевременному реагированию на угрозы, что повышает эффективность превентивных мер, направленных на поддержание правопорядка.

2. Применение беспилотных летательных систем, включая дроны, обеспечивает оперативное наблюдение за урбанизированными и пригородными территориями, где традиционные методы патрулирования затруднены в результате транспортной перегрузки, плотной застройки, инженерных ограничений или ограниченного доступа к частным объектам. Использование автоматизированных воздушных платформ позволяет осуществлять контроль за участками с высокой плотностью населения и фиксировать информацию при

[1] Колупаева Т.А. Использование информационных технологий в правоохранительной деятельности / Т.А. Колупаева // Молодой ученый. – 2024. – № 22 (312). – С. 267.

ограниченных возможностях наземного перемещения. Беспилотные комплексы применяются для наблюдения за труднодоступными природными и лесными массивами, расположенными вне пределов муниципальных образований. Такие технические средства обеспечивают дистанционное сканирование ландшафта и предоставляют визуальные сведения в реальном масштабе времени, что позволяет оперативно принимать решения при осуществлении охраны общественного порядка[1].

Технологические возможности беспилотных платформ позволяют проводить визуальное картографирование, выявлять скопления людей, отслеживать подозрительное поведение в условиях плотной застройки и минимизировать риски несвоевременного реагирования сотрудников правоохранительных органов. Эти аппараты повышают эффективность наблюдения за городской средой и способствуют предупреждению правонарушений. В соответствии с положениями пункта 3 статьи 11 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции», использование беспилотных средств воздушного, наземного и водного типа разрешено в деятельности органов внутренних дел. Закон закрепляет право на применение таких комплексов для фиксации обстоятельств преступлений, правонарушений и происшествий, в том числе в общественных местах, а также для регистрации действий сотрудников, исполняющих служебные обязанности. Введение дронов в практику правоприменения способствует формированию доказательной базы, улучшает контроль за соблюдением законности и повышает уровень прозрачности при выполнении полицейских функций.

Органы внутренних дел вправе обеспечивать защиту территорий и объектов, находящихся в их ведении, с применением технических средств, включая беспилотные летательные аппараты (БЛА). Указанное полномочие закреплено в пункте 25 части 1 статьи 13 Федерального закона «О полиции».

---

[1] Шевцов А.В. Применение некоторых современных информационных технологий в процессе организации охраны общественного порядка и обеспечения общественной безопасности / А.В. Шевцов, В.А. Милёхин // Экстремальные ситуации, конфликты, социальное согласие. сборник материалов XXV Международной научно-практической конференции. – М., 2023. – С. 294.

Законодатель также предоставляет право использовать в служебной деятельности (пункт 33 части 1 статьи 13) информационные системы, аппаратуру для фото-, аудио- и видеозаписи, специализированные комплексы, не наносящие ущерба гражданам и окружающей среде. Пункт 40 части 1 той же статьи определяет возможность пресечения работы БЛА в случае угрозы безопасности граждан, имущества, сотрудников органов внутренних дел. Это возможно в районах проведения следственных мероприятий, оперативных действий, массовых мероприятий и прилегающих зонах. Закон допускает использование методов подавления сигналов, перехвата управления, повреждения или физического уничтожения аппаратов. Соответствующий порядок принятия решений и круг уполномоченных должностных лиц регулируется приказом МВД России[1]. Статья 21, пункт 12 части 1, закрепляет право применять специальные технические средства для остановки действия БЛА. Кроме того, пункт 15 части 2 той же статьи указывает на наличие специализированных устройств в арсенале полиции, предназначенных для противодействия использованию таких средств. Закон также допускает применение табельного оружия в целях нейтрализации беспилотных платформ (пункт 5 части 3 статьи 23).

Эксплуатация БЛА в целях охраны общественного порядка и обеспечения безопасности населения ограничена требованиями по охране жизни и соблюдению прав субъектов. Использование дронов в местах массового скопления людей требует учета рисков, связанных с возможными нарушениями правопорядка и неприкосновенности частной жизни. Эффективное применение таких технологий предполагает соблюдение баланса между мерами обеспечения безопасности и юридическими гарантиями граждан. С учетом возможностей БЛА, их внедрение рассматривается как одно из наиболее перспективных направлений развития технического сопровождения в деятельности полиции.

---

[1] Об утверждении Порядка принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий и Перечня должностных лиц, уполномоченных на принятие такого решения: Приказ МВД России от 30 апреля 2020 г. № 252 // Российская газета. – 2020. – 27 авг.

3. Оснащение патрульных транспортных средств специализированным оборудованием, обеспечивающим автоматизированное считывание регистрационных знаков, навигацию и доступ к централизованным базам данных о правонарушениях, позволяет повысить результативность контроля за общественным порядком. Технологические решения, основанные на применении интеллектуальных систем, обеспечивают автоматическую фиксацию нарушений и реализацию оперативных мер реагирования в реальном времени. Их внедрение способствует улучшению оперативной деятельности подразделений, задействованных в обеспечении правопорядка и общественной безопасности. Применение подобных комплексов требует соблюдения стандартов по защите информации, исключающей несанкционированное использование персональных данных, полученных в процессе мониторинга. Персональные сведения, зафиксированные с помощью указанных систем, допустимо применять исключительно в рамках деятельности, связанной с охраной общественного порядка. Условием эффективности данных технологий выступает соблюдение юридических норм, обеспечивающих неприкосновенность частной жизни и прозрачность процедур сбора и хранения информации.

Интеграция интеллектуальных модулей с информационными массивами, содержащими сведения о правонарушениях, включая данные о штрафах, мерах административного воздействия и судебных постановлениях, осуществляется в соответствии со статьями 11 и 17 Федерального закона «О полиции». Такая синхронизация расширяет функциональные возможности распознающих систем, позволяя использовать их для установления фактов правонарушений, контроля доступа в охраняемые зоны и рационального распределения ресурсов органов правопорядка. Система автоматического считывания номерных знаков представляет собой пример практического применения цифровых инструментов в процессе обеспечения общественной безопасности. Эти технологии задействуются для идентификации транспортных средств, контроля дорожного движения и управления доступом на территориальные объекты с ограниченным

режимом[1]. Перспективы развития этих решений предполагают их дальнейшее усовершенствование, направленное на повышение точности, скорости обработки и степени интеграции с иными элементами инфраструктуры правоохранительной системы.

4. Применение технологии распределённых реестров, основанной на архитектуре блокчейн, рассматривается в качестве эффективного инструмента формирования защищённых цифровых систем контроля за состоянием общественного порядка. Использование данной технологии обеспечивает сохранность, достоверность и устойчивость информации, исключая возможность её изменения без авторизованного следа в журнале транзакций. Такая система повышает уровень доверия к операциям, связанным с фиксацией и обработкой сведений, имеющих значение для обеспечения общественной безопасности. Технологическая структура блокчейн-фреймворков обеспечивает создание непрерывных зашифрованных цепочек данных, каждая из которых содержит уникальные идентификаторы и сохраняет неизменность записей. Эти характеристики позволяют использовать децентрализованные платформы в целях автоматизированного мониторинга и документирования правонарушений, а также контроля доступа к зафиксированным событиям. В условиях цифровой трансформации правопорядочной деятельности указанный подход способствует формированию высокоэффективных механизмов обеспечения прозрачности в процессе администрирования и координации мер по поддержанию общественной безопасности. Системы на основе блокчейн-технологий обладают потенциалом к интеграции в существующие цифровые среды Министерства внутренних дел и иных субъектов правоохранительной инфраструктуры, создавая распределённые среды хранения данных, устойчивые к вмешательству извне. Их использование позволяет существенно снизить риски несанкционированного доступа, модификации или удаления сведений,

[1] Крупина М.А. Административно-правовые аспекты использования прикладных сервисов единой системы информационно-аналитического обеспечения деятельности МВД России / М.А. Крупина // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2023. – № 2. – С. 140.

критически значимых для реализации функций правоохранительной деятельности.

5. Разработка приложений для мобильных устройств, которые позволяют гражданам сообщать о правонарушениях и подозрительной активности, а также предоставлять информацию о своем местоположении и времени обращения. «Геофенсинг позволяет пользователям таких мобильных устройств и приложений к ним сообщать о правонарушениях, а также определять свое местоположение и время обращения. Геофенсинг – это технология, которая использует GPS-позиционирование и Wi-Fi сигналы для определения местоположения мобильных устройств. Она позволяет отслеживать перемещение людей и объектов в реальном времени, а также анализировать их поведение. Эта технология используется в различных сферах, включая ООП и ООБ. Например, геофенсинг может помочь субъектам управления НП быстрее реагировать на противоправные проявления и обеспечивать безопасность на массовых мероприятиях. В транспортной сфере геофенсинг помогает оптимизировать работу НП с учётом трафика движения пассажирского и грузового транспорта. Основная возможность геофенсинга – это определение местоположения объекта или человека. Геофенсинг также позволяет контролировать соблюдение ПДД и предотвращать нарушения»[1].

6. Применение технологий виртуализации социальных взаимодействий в городском пространстве и иных общественно значимых локациях, включая объекты транспортной инфраструктуры, используется при подготовке сотрудников полиции к реагированию в различных ситуациях, связанных с обеспечением правопорядка. Имитационные цифровые среды создаются на основе технологий виртуальной и дополненной реальности, предоставляя возможность моделирования различных нарушений и отработки тактических действий в условиях, приближённых к реальным. Использование VR- и AR-

[1] Токбаев А.А., Аверина Е.А. Использование современных средств технического контроля при охране общественного порядка и обеспечении общественной безопасности / А.А. Токбаев и др. // Школа будущего. – 2024. – № 1. – С.73.

решений в системе служебной подготовки позволяет реализовать сценарное обучение личного состава правоохранительных структур, направленное на повышение готовности к действиям в условиях неопределённости. Такие среды обеспечивают возможность многократного воспроизведения разнообразных поведенческих ситуаций в контролируемой цифровой форме, где анализируются реакции сотрудников, оценивается корректность применяемых мер и степень соответствия установленным алгоритмам служебного реагирования. Виртуализированные модели сообществ применяются при исследовании социального поведения в нестандартных ситуациях, которые невозможно смоделировать в физическом пространстве. Создание экспериментальных цифровых групп позволяет изучать процессы взаимодействия внутри социальных кластеров, включая поведение в условиях массовых мероприятий, чрезвычайных ситуаций, а также в период социально-эпидемиологических ограничений. Такие подходы способствуют расширению методологических возможностей анализа динамики общественного поведения, адаптации обучающих алгоритмов и корректировке нормативов профессиональной подготовки сотрудников органов правопорядка.

7. «Интеграция устройств IoT (интернет вещей) в систему мониторинга состояния правопорядка в общественных местах, чтобы обеспечить сбор данных о правонарушениях, а также контроль их доступа в определенные общественные местах. Интернет вещей в общественных местах позволяет с достаточно высокой точностью определить местонахождение лиц, имеющих опыт совершения противоправных деяний. Это позволяет не допустить со стороны таких лиц иные посягательства на охраняемые законом правоотношения в общественных местах, а также в прилегающем к ним жилом секторе и объектах социального назначения. Интеграция устройств Интернета вещей (IoT) в систему мониторинга общественного порядка может значительно улучшить уровень безопасности и контроля в городе и административно-территориальном образовании. Устройства IoT могут собирать данные с различных источников, таких как видеокамеры, датчики движения, системы распознавания лиц и многие

другие, и передавать их в режиме реального времени на серверы для анализа. В этом эссе рассматривается, как интеграция IoT устройств может улучшить систему мониторинга общественного порядка»[1].

8. Разработка специализированных «Интернет голосовых помощников», способных обрабатывать запросы граждан на предмет мониторинга правопорядка и оказывать помощь в решении проблем. Голосовые помощники (ассистенты) могут в режиме реального времени обрабатывать многочисленные запросы пользователей, поступающие с их мобильных телефонов (смартфонов), а также со стационарных устройств экстренной связи «гражданин-полиция», помогая тем самым разрешению самых различных ситуационных задач, возникающих в процессе мониторинга состояния правопорядка на обслуживаемых полицией территориях.

9. «Применение методов прогнозирования и проактивного мониторинга, таких как анализ данных, социальных медиа и других источников информации, для предотвращения возможных нарушений до их возникновения. Проактивный мониторинг эффективное средство системного анализа данных, социальных сетей и других источников с помощью специальных математических алгоритмов. Он так же позволяет результативно выявлять и пресекать намерения совершить определённые (этим алгоритмом) противоправные проявления в наиболее значимых с точки зрения обеспечения правопорядка сферах правоотношений. В этой связи проактивный мониторинг медиапространства становится все более важным в современном мире, где информация распространяется с невероятной скоростью»[2].

10. Вовлечение граждан и сообществ в мониторинг правопорядка через краудсорсинговые платформы и мобильные приложения, которые позволят сообщать о нарушениях и предоставлять обратную связь. «Краудсорсинг

---

[1] Бураева Л.А. Роль информационных технологий в обеспечении общественного порядка и общественной безопасности / Л.А. Бураева, Т.М. Шогенов // Социально-политические науки. – 2024. – Том IX. – С. 192.

[2] Воронов А.М., Анисифорова М.В. Перспективы внедрения новых информационных технологий в деятельность органов внутренних дел по профилактике правонарушений / А.М. Воронов и др. // Вестник ВИПК МВД России. – 2024. – № 2 (70). С. 157.

реализуется посредством активного привлечения граждан с высоким уровнем социальной ответственности перед обществом, являющихся деятельными и энергичными пользователями вышеуказанных мобильных приложений и самых различных социальных сетей. Такой метод может использоваться для обучения нарядов полиции новым методам и технологиям, а также для повышения их профессиональных навыков. Это важно в условиях быстрого развития технологий и появления новых форм противоправных проявлений»[1].

Интеграция цифровых решений в систему обеспечения общественного порядка и безопасности способствует сокращению времени реагирования на противоправные действия и нештатные ситуации. Внедрение современных информационных механизмов в практику оперативной деятельности способствует совершенствованию компетенций сотрудников правоохранительных органов, задействованных в обеспечении правопорядка. Использование технологических средств управления и мониторинга позволяет повысить эффективность функционирования органов внутренних дел при выполнении задач в сфере охраны общественной безопасности.

§2. Перспективные направления развития единой системы информационно-аналитического обеспечения деятельности МВД России

В процессе цифровой трансформации органов внутренних дел реализуется комплекс мероприятий, направленных на оснащение ведомственных подразделений высокотехнологичными средствами информатизации и обеспечивающими безопасность информационных ресурсов решениями. За последние годы осуществлена масштабная модернизация в сфере применения

[1] Яворский М.А. Использование цифровых технологий в административно-юрисдикционной деятельности правоохранительных органов / М.А. Яворский, Е.А. Саблина Е.А., М.С. Цымбалюк // Право и практика. – 2022. – № 2. – С. 75.

телекоммуникационных и вычислительных технологий, сформирована унифицированная система учётов различной направленности - оперативно-справочного, экспертно-криминалистического, розыскного характера - и внедрён ряд специализированных программных комплексов, способствующих росту эффективности функционирования ведомства.

Функционирующая в настоящее время система информационно-аналитического обеспечения МВД России представляет собой многокомпонентную структуру, охватывающую базы данных, средства анализа информации и современные коммуникационные платформы[1]. Задачи, определённые в стратегии развития ИСОД на 2020 год[2], выполнены. Достигнуты заявленные показатели по повышению результативности аналитической деятельности, снижению затрат за счёт цифровизации процессов и обеспечению устойчивости технологической инфраструктуры. Завершены этапы, касающиеся унификации разрозненных информационных систем, правовой регламентации цифрового взаимодействия, внедрения механизмов защиты информации, перехода на отечественное программное и аппаратное обеспечение, усовершенствования дата-центров и создания новых прикладных решений[3].

Таким образом, формирование и совершенствование интегрированной информационно-коммуникационной системы МВД России выступило основой для повышения результативности ведомственной деятельности. Выполнение установленных целей и задач привело к росту технологического потенциала

---

[1] Кубасов И.А. Проблемные вопросы и направления развития единой системы информационно-аналитического обеспечения деятельности МВД России / И.А. Кубасов // Охрана, безопасность, связь. – 2022. – № 5-3. – С. 210.

[2] Основные направления дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы: утв. исполняющим обязанности Министра внутренних дел РФ генералом полиции Российской Федерации В.А. Колокольцевым от 21 января 2020 г. // Специализированная территориально распределенная система СТРАС «Юрист» [Электронный ресурс]. Режим доступа: https://ви.мвд.рф/ (дата обращения: 20.06.2025).

[3] Проведение анализа выполнения Плана реализации основных направлений дальнейшего развития ИСОД МВД России на период с 2020 по 2024 год (дорожная карта) и подготовка предложений по внесению изменений в Основные направления дальнейшего развития ИСОД МВД России на период с 2020 по 2024 год: отчет о научно-исследовательской работе. Шифр «Рубикон». Гос. регистрация № 01231813. – М.: ФКУ НПО «СТиС» МВД России, 2024.

ведомства, а также к улучшению качества государственных функций, в том числе в дистанционном формате.

Необходимость последующего развития системы обусловлена влиянием различных факторов, поддающихся классификации на социальные, технические и организационные. В социальном аспекте потребность в адаптации приоритетов развития информационной платформы определяется изменением запроса со стороны как служащих системы внутренних дел, так и населения. Современные пользователи ожидают высокой скорости предоставления данных и доступа к услугам через цифровую среду. Продолжение работы над расширением функциональности информационной системы должно соответствовать этим ожиданиям, обеспечивая реализацию сервисов, ориентированных на интересы граждан.

Расширение цифровых механизмов управления и внедрение технологических инноваций в процесс оказания государственных услуг способствует укреплению уровня открытости административных процедур, формированию условий для объективной отчётности и усилению доверия общества к системе МВД России[1].

С позиции технологического прогресса необходимость пересмотра приоритетов развития ИСОД МВД России обусловлена динамикой внедрения современных цифровых решений, как в отечественной, так и в международной практике. Применение искусственного интеллекта, средств анализа массивов информации, робототехнических комплексов и облачных платформ обеспечивает высокий уровень обработки данных, совершенствует процедуры принятия управленческих решений, усиливает меры по обеспечению правопорядка и укрепляет информационную защищенность ведомства[2].

---

[1] Новичихин П. Г. О некоторых проблемах эксплуатации на местах программного обеспечения сервиса обеспечения охраны общественного порядка единой системы информационно-аналитического обеспечения деятельности МВД России / П.Г. Новичихин // Научный портал МВД России. – 2024. – № 1 (65). – С. 69.

[2] Кубасов И.А. Цифровой двойник: технология, революционизирующая методы работы предприятий / И.А. Кубасов // Первая миля. – 2023. – № 2 (110). – С. 74.

С учётом организационной специфики актуальность обновления стратегических ориентиров информационной системы МВД России определяется требованиями текущих и перспективных задач, стоящих перед подразделениями. Используемые программные продукты часто характеризуются избыточной стоимостью обслуживания и функциональной неэффективностью, не соответствуя требованиям вновь сформированных структур. Продолжение модернизации ИСОД обеспечит создание специализированных решений, реструктуризацию существующих процессов и улучшение координации между функциональными уровнями ведомства.

В качестве ключевых направлений модернизации ИСОД МВД России целесообразно рассматривать:

- организацию оперативного доступа сотрудников к данным в различных форматах (аудио, видео, текст, графика) с учётом разграничения прав пользования;

- использование интеллектуальных программных решений для выявления скрытых взаимосвязей и улучшения качества принимаемых решений;

- снижение временных затрат при выполнении повторяющихся задач через автоматизацию рутинных процессов;

- развитие механизмов межведомственного информационного обмена с федеральными структурами и гражданами при оказании услуг, в том числе через цифровые платформы;

- усиление защиты информационной инфраструктуры органов внутренних дел, включая меры по противодействию киберугрозам.

Для достижения стратегических ориентиров в области трансформации информационной системы МВД России требуется выполнение комплекса взаимосвязанных задач, обеспечивающих технологическую устойчивость и эффективность управленческих решений. Во-первых, необходимо обеспечить интеграцию ведомственных информационных массивов в единую цифровую архитектуру. Это создаст общее пространство оперативного взаимодействия, упрощающее доступ к информации и сокращающее время на получение

аналитических данных. Во-вторых, требуется разработать программные комплексы, способные обрабатывать массивы информации из разнородных источников. Применение таких решений позволит устанавливать скрытые корреляции, тем самым повышая результативность деятельности должностных лиц в рамках реализуемых полномочий. В-третьих, актуальной задачей становится внедрение комплекса высокотехнологичных решений: аналитических платформ с элементами машинного обучения, распределённых реестров (блокчейн), иммерсивных систем (AR/VR), автономных комплексов, сетей умных устройств, а также геоинформационных решений. Применение этих инструментов обеспечит автоматизацию процессов и позволит повысить качество управленческих решений[1]. В-четвёртых, требуется усилить меры защиты цифровой инфраструктуры МВД России, предусматривающие не только сохранность данных, но и устойчивость к внешним угрозам, включая обеспечение кибербезопасности.

Сложившиеся геополитические условия и стремительное расширение цифрового пространства определяют необходимость усиления мер по обеспечению устойчивости информационной инфраструктуры в системе внутренних дел. Повышение уровня защищённости информационных ресурсов становится структурообразующим элементом стратегии технологической трансформации ведомства.

Для реализации приоритетных задач в этой области целесообразно:

1) углубить подготовку специалистов, задействованных в обеспечении правопорядка, в сфере противодействия цифровым угрозам;

2) установить регламентированные процедуры защиты ограниченного доступа к данным, минимизирующие вероятность несанкционированного вмешательства и утраты информации;

---

[1] Кубасов И. А., Щетников А. В. О реализации федерального проекта «Искусственный интеллект» Национальной программы «Цифровая экономика Российской Федерации» в сфере внутренних дел // Цифровая трансформация системы МВД России: сборник научных статей по материалам Международного форума: в 2 ч. / под ред. И. Г. Чистобородова. Ч. 1. – М.: Академия управления МВД России, 2022. – С. 425.

3) применить криптографические механизмы при передаче и хранении сведений, обеспечивающие сохранность содержимого и устойчивость к перехвату;

4) разработать программные решения, направленные на идентификацию попыток нарушения целостности систем и их активную нейтрализацию;

5) внедрить цикл плановых проверок текущих механизмов защиты, предусматривающий выявление и устранение уязвимостей в кратчайшие сроки;

6) использовать системы персональной идентификации, основанные на биометрических параметрах, в целях исключения несанкционированного доступа к техническим средствам и массивам данных.

Комплексная реализация указанных направлений развития информационно-аналитической инфраструктуры МВД России обеспечит устойчивость цифровой среды, модернизирует механизм предоставления государственных функций, улучшит доступ к услугам и укрепит доверие граждан к работе ведомства.

Подведем некоторые итоги третьей главы дипломной работы.

Одной из центральных проблем выступает фрагментарность и слабая интеграция используемых платформ. Несмотря на наличие ИСОД МВД, АРМ «Дежурная часть» и других модулей, их архитектурная несовместимость и отсутствие единого ядра приводят к дублированию данных, затруднённому межведомственному обмену и снижению аналитической точности.

Значительным препятствием становится недостаточная правовая регламентация использования искусственного интеллекта, биометрических технологий и автоматической видеоаналитики в повседневной служебной деятельности. Несмотря на наличие общих положений в законодательстве (Федеральный закон «О полиции»; Федеральный закон «О персональных данных»), отсутствует единый подзаконный акт, регламентирующий допустимые методы использования интеллектуальных алгоритмов в оперативных целях. Это сдерживает масштабное применение предикативной аналитики и интеллектуальных решений в правоохранительной практике.

Таким образом, несмотря на положительные результаты цифровизации МВД России, реализация ИТКС сопровождается комплексом организационно-правовых, технологических и кадровых ограничений. Решение обозначенных проблем требует комплексного подхода: модернизации инфраструктуры, подготовки кадров, унификации правового регулирования и совершенствования архитектуры цифровых платформ.

ЗАКЛЮЧЕНИЕ

В ходе исследования использования современных информационно-телекоммуникационных систем в деятельности полиции России была проведена комплексная оценка их влияния на эффективность работы правоохранительных органов, а также выявлены ключевые проблемы и перспективы дальнейшего развития этой области.

1. Система внутренних дел, обладая функцией обеспечения общественной безопасности и правопорядка, занимает центральное место в структуре исполнительной власти. В условиях цифровой трансформации её деятельность требует правового регулирования применения новых технологий. Федеральные нормативные акты предусматривают использование в служебной практике передовых технических решений, информационных ресурсов и цифровых платформ. Внедрение автоматизированных средств анализа, хранения и обработки данных способствует организации координированной и продуктивной работы сотрудников, устранению рутинных процедур и ускорению обработки сведений, имеющих значение для исполнения оперативных задач. Цифровая трансформация позволяет объединять информационные потоки, формировать аналитические выборки, осуществлять контроль за полнотой и точностью сведений, а также устранять обнаруженные ошибки в краткие сроки.

2. В 2012 году утверждён нормативный документ, закрепляющий основы построения интегрированной информационно-аналитической системы МВД России. Этот комплекс охватывает совокупность автоматизированных решений, технических платформ, каналов связи и средств обработки, направленных на оптимизацию всех направлений деятельности ведомства. Архитектура системы ориентирована на автоматизацию типовых процедур, формирование структурированного массива данных, обеспечивающего доступ к хранимой информации с возможностью просмотра, анализа и корректировки. Предусматривается взаимодействие через электронные каналы, что

способствует снижению временных затрат при формировании отчётной документации и повышает обоснованность решений, принимаемых в рамках управленческой компетенции.

ИСОД выполняет следующие функции: 1) автоматизированного сбора и фильтрации данных о криминальной обстановке; 2) структурированного хранения информации о правонарушениях, участниках преступлений, уголовных делах, розыскных мероприятиях; 3) генерации прогнозно-аналитических моделей с целью предотвращения преступлений; 4) обеспечения единых стандартов аналитической работы в масштабах всей системы МВД. На текущем этапе система внедрена во всех территориальных органах МВД России. Доступ к ИСОД имеют должностные лица, наделённые соответствующими полномочиями, с соблюдением требований разграничения доступа и криптографической защиты данных.

3. В структуре ИСОД МВД России реализован комплекс компонентов, обеспечивающих работу специализированных цифровых инструментов. Среди них: 1) система централизованной обработки данных МВД России (СЦОД), предназначена для размещения в ней информационных систем и прикладных сервисов обеспечения повседневной и оперативно-служебной деятельности подразделений МВД России на вычислительных мощностях ИСОД МВД России; 2) интегрированная мультисервисная телекоммуникационная сеть МВД России, предназначена для создания универсальной телекоммуникационной транспортной среды, позволяющей обеспечить предоставление комплекса услуг связи подразделениям МВД России; 3) подсистема обеспечения информационной безопасности, представляющая собой совокупность аппаратных, программных и технических средств обеспечения комплексной информационной безопасности в рамках ИСОД МВД России и включающая в себя прикладной сервис управления доступом; 4) информационная система взаимодействия с гражданским обществом и иными государственными органами, обеспечивающая процессы информирования населения, исполнения государственных функций, осуществления межведомственных коммуникаций,

сбора и анализа информации, оценки результативности предоставления государственных услуг, а также мониторинга соответствия деятельности установленным регламентам; 5) каталог прикладных цифровых решений, классифицированных по назначению.

Инструменты, входящие в данную систему, подразделяются на две функциональные категории: средства, поддерживающие регулярную административную деятельность, и инструменты, предназначенные для обеспечения выполнения оперативно-служебных мероприятий. Первая группа охватывает все подразделения ведомства. Вторая применяется в зависимости от задач конкретных направлений ведомственной работы.

4. Интеграция и унификация действующих информационно-аналитических ресурсов на базе защищённых облачных платформ и алгоритмов обработки больших массивов данных с применением программных средств искусственного интеллекта создаёт предпосылки для углубления цифрового взаимодействия между различными структурами системы обеспечения правопорядка. Формирование единой архитектуры обмена данными способствует повышению качества межведомственной координации в области противодействия преступности и обеспечивает систематизацию процессов обработки информации в цифровом формате.

Развитие системы информационного сопровождения административной деятельности органов внутренних дел приобретает статус одного из приоритетов в контексте повышения результативности профилактических и правоохранительных мероприятий. Научно выверенная стратегия, реализуемая Министерством внутренних дел Российской Федерации в сфере цифровизации оперативной и служебной деятельности, предусматривает формирование комплексных хранилищ информации с возможностью коллективного доступа, охватывающих федеральный и субъектовый уровни. Применение современных решений в области телекоммуникаций, идентификационных систем и биометрических механизмов обработки данных повышает эффективность информационного обмена, ускоряет реагирование на оперативные события и

позволяет достичь нового уровня организации аналитической и поисковой работы.

5. Разработка и внедрение автоматизированных систем в контуре органов внутренних дел требует учета технологической совместимости используемого оборудования, соблюдения установленных регламентов, стандартов и подготовки персонала к работе в новых условиях. Информационные платформы, соответствующие функциональным требованиям ведомства, увеличивают продуктивность работы сотрудников, обеспечивают мгновенное получение доступа к массивам данных и способствуют сокращению времени на реализацию процедурных задач. Процесс интеграции автоматизированных средств информационной поддержки в структуру деятельности органов правопорядка рассматривается как значимый вектор совершенствования институциональной среды. Такой подход к организации оперативной деятельности способствует повышению уровня общественной защищенности.

Использование цифровых решений в повседневной и специальной служебной деятельности сотрудников позволяет качественно выполнять функции, связанные с хранением, поиском, трансляцией и документированием сведений, а также поддерживать необходимый уровень внутриорганизационной коммуникации. Прогнозируемым направлением развития системы МВД выступает дальнейшее перемещение информационных процессов в электронную среду. Эта стратегия направлена на расширение функционального охвата служебных задач при одновременном снижении ресурсных затрат.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

а) Законы, нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации: Принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ от 04.10.2022 № 8-ФКЗ) // Собрание законодательства РФ. – 2022. – № 41. – Ст. 6933.

2. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30 декабря 2001 г. № 195-ФЗ (с изм. от 21 апреля 2025 г.) // Собрание законодательства РФ. – 2002. – №1 (ч. 1). – Ст. 1.

3. Об архивном деле в Российской Федерации: Федеральный закон от 22 октября 2004 г. № 125-ФЗ (с изм. от 13 декабря 2024 г.) // Собрание законодательства РФ. – 2004. – № 43. – Ст. 4169.

4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. от 01 апреля 2025 г.) // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3448.

5. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (с изм. от 28 февраля 2025 г.) // Собрании законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3451.

6. Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 8 ноября 2007 г. № 257-ФЗ (с изм. от 20 марта 2025 г.) // Собрание законодательства РФ. – 2007. – № 46. – Ст. 5553.

7. О полиции: федеральный закон от 7 февраля 2011 г. № 3-ФЗ (с изм. от 01 апреля 2025 г.) // Российская газета. – 2011. – №5401; 2025. – №75.

8. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (с изм. от 21 апреля 2025 г.) // Собрание законодательства РФ. – 2011. – № 15. – Ст. 2036.

9. Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23 июня 2016 г. N 182-ФЗ (с изм. от 8 августа 2024 г.) // Собрание законодательства РФ. – 2016. – № 26 (часть I). – Ст. 3851.

10. О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти: Закон Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ // Собрание законодательства РФ. – 2020. – № 11. – Ст. 1416.

11. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // Собрании законодательства РФ. – 2017. – № 20. – Ст. 2901.

12. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 г. № 490 (с изм. от 15 февраля 2024 г.) // Собрание законодательства РФ. – 2019. – N 41. – Ст. 5700.

13. О Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: Распоряжение Правительства РФ от 3 декабря 2014 г. № 2446-р // Российская газета. – 2014. – 11 дек.

14. О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий, финансовое обеспечение которых осуществляется (планируется осуществлять) за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов: Постановление Правительства РФ от 10 октября 2020 г. № 1646 (с изм. от 18 марта 2025 г.) // Собрание законодательства РФ. – 2020. – № 42 (часть III). – Ст. 6612.

15. О разработке и утверждении образцов специальной продукции, необходимой для допуска транспортных средств и водителей к участию в дорожном движении: Приказ МВД РФ от 27 апреля 2002 г. № 390 (с изм. от 15 августа 2012 г.) // Российская газета. – 2002. – № 89.

16. О введении в действие водительского удостоверения: Приказ МВД РФ от 13 мая 2009 г. № 365 (с изм. от 9 января 2024 г.) // Российская газета. – 2009. – № 132.

17. О совете по созданию Единой системы информационно-аналитического обеспечения деятельности МВД России: Приказ МВД РФ от 24 октября 2011 г. № 1097 / Текст приказа официально опубликован не был.

18. Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах: Приказ МВД России от 30.03.2012 № 205 / Текст приказа официально опубликован не был.

19. О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции: Приказ МВД России от 5 февраля 2016 г. № 60 / Текст приказа официально опубликован не был.

20. О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России: Приказ МВД России от 9 ноября 2018 г. № 755 // Российская газета. – 2018. – 06 дек.

21. Об утверждении Порядка принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий и Перечня должностных лиц, уполномоченных на принятие такого решения: Приказ МВД России от 30 апреля 2020 г. № 252 // Российская газета. – 2020. – 27 авг.

22. Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации МВД России: Приказ МВД России от 15.06.2021 № 444 (с изм. от 31 марта 2025 г.) / Текст приказа официально опубликован не был.

23. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022–2024 годы: распоряжение МВД России от 11 января 2022 г. № 1/37 / Текст распоряжения официально опубликован не был.

24. Об организационных вопросах профилактики правонарушений в системе МВД России: Приказ МВД России от 29 сентября 2022 г. № 715 / Текст приказа официально опубликован не был

25. О некоторых организационных вопросах деятельности ОВД по профилактике правонарушений: Приказ МВД России от 24 августа 2023 г. № 619 / Текст приказа официально опубликован не был.

26. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2023-2025 годы: Распоряжение МВД России от 25.01.2023 № 1/649 / Текст распоряжения официально опубликован не был.

27. Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации: Приказ МВД России от 2 сентября 2024 г. № 515 / Официально приказ опубликован не был.

28. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16) / Текст паспорта официально опубликован не был.

29. Паспорт федерального проекта Информационная безопасность (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. № 9)) / Текст паспорта опубликован не был.

30. ГОСТ Р 59853–2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие Приказом Росстандарта от 19.11.2021 № 1520-ст). – М.: ФГБУ «РСТ», 2021.

б) Монографии, учебники, учебные пособия:

1. Аврутин Р.Ю., Габова О.С., Шихалов А.О. Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России: учебно-практическое пособие / Р.Ю. Аврутин и др. – Санкт-Петербург: СПбУ

МВД России, 2023. – 210 с.

2. Антонов В.В. Актуальные вопросы информационного обеспечения органов внутренних дел: учебное пособие / В.В. Антонов, В.Р. Гурьянова, Г.А. Тугузбаев. – Уфа: Уфимский ЮИ МВД России, 2023. – 48 с.

3. Ковалев А.Н. Информационные технологии в правоохранительных органах / А.Н. Ковалев. – М.: Юрайт, 2020. – 186 с.

4. Маркушин А.Г. Основы управления в органах внутренних дел: учеб. для СПО / А.Г. Маркушин, В.В. Казаков. – 3-е изд., перераб. и доп. – М.: Юрайт, 2020. – 224 с.

5. Майстренко А.В., Майстренко Н.В. Информационные технологии в науке, образовании и инженерной практике: учебное пособие / А.В. Майстренко и др. – Тамбов: ФГБОУ ВПО «ТГТУ», 2014. – 159 с.

в) Статьи, научные публикации:

1. Бураева Л.А. Роль информационных технологий в обеспечении общественного порядка и общественной безопасности / Л.А. Бураева, Т.М. Шогенов // Социально-политические науки. – 2024. – Том IX. – С. 192-197.

2. Бучакова М.А. Персональные данные и их защита в условиях цифровизации общества / М.А. Бучакова // Алтайский юридический вестник. – 2021. – № 2. – С. 44-48.

3. Бучакова М.А., Мушаков В.Е. Оптимизация деятельности российской полиции по защите прав человека в условиях цифровизации / М.А. Бучакова и др. // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2022. – № 4. – С. 11-16.

4. Вермеенко Я.С. Современное состояние и перспективы развития ИСОД МВД России / Я.С. Вермеенко // Академическая мысль. – 2021. – № 3 (16). – С. 75-80.

5. Веселова Я.А. Применение ИСОД в органах внутренних дел / Я.А. Веселова // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сборник материалов конференции. – Воронеж,

2022. – С. 23-27.

6. Воронов А.М., Анисифорова М.В. Перспективы внедрения новых информационных технологий в деятельность органов внутренних дел по профилактике правонарушений / А.М. Воронов и др. // Вестник ВИПК МВД России. – 2024. – № 2 (70). – С.40-44.

7. Глухов Н.В. Роль цифровизации в деятельности правоохранительных органов / Н.В. Глухов // Технологии XXI века в юриспруденции: материалы Третьей международной научно-практической конференции. – Екатеринбург, 2024. – С. 441-445.

8. Гюльалиев Т.М., Абакарова О.Г. Развитие и внедрение современных информационных технологий в системе МВД России / Т.М. Гюльалиев и др. // В сборнике: Современные проблемы научной деятельности. Перспективы внедрения инновационных решений. Сборник статей Международной научно-практической конференции. – Уфа, 2022. – С. 36-40.

9. Долинин В.Н., Пермяков Е.К., Ровнушкин В.Е. Использование компьютерных технологий в правоохранительной деятельности // В сборнике: Технологии XXI века в юриспруденции. Материалы четвёртой международной научно-практической конференции / Отв. редактор: Д.В. Бахтеев. – Екатеринбург, 2022. – С. 67-71.

10. Дудченко А.В., Парий М.А. Информационные технологии в правоохранительной деятельности / А.В. Дудченко и др. // Очерки новейшей камералистики. – 2023. – № 2. – С. 16-21.

11. Иншаков М.И. Правовые и организационные аспекты ресурсного обеспечения информационных технологий в органах внутренних дел / М.И. Иншаков // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2021. – № 21-2. – С. 60-65.

12. Искалиев Р.Г., Телков А.В. К вопросу о противодействии преступлениям экономической и коррупционной направленности, совершаемым с использованием IT-технологий / Р.Г. Искалиев и др. // Закон и право. – 2021. – № 11. – С. 118-123.

13. Кирюшин И.И., Иванов И.П., Тимофеев В.В., Жмурко Д.Ю. Использование технологии блокчейна в правоохранительной деятельности / И.И. Кирюшин и др. // Полицейская деятельность. – 2024. – № 1. – С.31-35.

14. Коблов Ф.Ч. К вопросу о применении инновационных технологий как способа повышения профессионализма сотрудника органов внутренних дел / Ф.Ч. Коблов // Научно-методический электронный журнал Концепт. – 2016. – т.47 – С.20-24.

15. Колупаева Т.А. Использование информационных технологий в правоохранительной деятельности / Т.А. Колупаева // Молодой ученый. – 2024. – № 22 (312). – С. 267-272.

16. Комелькова Я.В. Применение информационных технологий в правоохранительной деятельности / Я.В. Комелькова // StudNet. – 2022. – № 5. – С. 26-31.

17. Крупина М.А. Административно-правовые аспекты использования прикладных сервисов единой системы информационно-аналитического обеспечения деятельности МВД России / М.А. Крупина // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2023. – № 2. – С. 140-145.

18. Кубасов И.А. Проблемные вопросы и направления развития единой системы информационно-аналитического обеспечения деятельности МВД России / И.А. Кубасов // Охрана, безопасность, связь. – 2022. – № 5-3. – С. 210-215.

19. Кубасов И. А., Щетников А. В. О реализации федерального проекта «Искусственный интеллект» Национальной программы «Цифровая экономика Российской Федерации» в сфере внутренних дел // Цифровая трансформация системы МВД России: сборник научных статей по материалам Международного форума: в 2 ч. / под ред. И. Г. Чистобородова. Ч. 1. – М.: Академия управления МВД России, 2022. – С. 425-430.

20. Кубасов И.А. Цифровой двойник: технология, революционизирующая методы работы предприятий / И.А. Кубасов // Первая

миля. – 2023. – № 2 (110). – С. 74-80.

21. Курушин С.А., Яворский М.А. Информационные технологии в оптимизации правоохранительной деятельности / С.А. Курушин и др. // Наука XXI века: актуальные направления развития. – 2022. – № 2-2. – С. 148-152.

22. Левчунец И.В., Максимов А.В., Метельков А.Н. Абстрактная и формальная модели безопасности при информационно-техническом взаимодействии автоматизированных систем / И.В. Левчунец и др. // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2020. – № 3. – С. 100-107.

23. Мантуров О.С., Ганага В.С. Коммуникативные компетенции сотрудников полиции в цифровом пространстве / О.С. Мантуров и др. // Полицейская деятельность. – 2020. – № 5. – С. 1-17.

24. Матросова Л.Д., Кислицин И.А. Инструменты для поиска оперативно-значимой информации по открытым источникам / Л.Д. Матросова и др. // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2022. – № 4 (93). – С. 65-72.

25. Матросова Л.Д. Использование автоматизированных баз данных в учебном процессе / Л.Д. Матросова // Наука и практика. – 2023. – № 2. – С. 135-140.

26. Майоров В.И. Совершенствование использования технических средств фотовидеофиксации нарушений правил дорожного движения на основе цифровых технологий / В.И. Майоров // Безопасность дорожного движения. – 2023. – № 3. – С. 44-49.

27. Новичихин П.Г. О некоторых проблемах эксплуатации на местах программного обеспечения сервиса обеспечения охраны общественного порядка единой системы информационно-аналитического обеспечения деятельности МВД России / П.Г. Новичихин // Научный портал МВД России. – 2024. – № 1 (65). – С. 69-73.

28. Острякова А.Ф., Митряев И.С. Использование современных технологий в правоохранительных органах / А.Ф. Острякова и др. // Аграрное и

земельное право. – 2023. – № 7(223). – С. 58-62.

29. Родивилина В.А. Развитие информационного обеспечения деятельности МВД России / В.А. Родивилина // Криминалистика: вчера, сегодня, завтра. – 2025. – № 1. – С. 51-56.

30. Романов М.С. и др. Воздействие цифровизации на деятельность органов МВД России / М.С. Романов, А.Я. Дидюк, Н.М. Трифоненко, Д.В. Солодянкин // Юридическая наука. – 2022. – № 7. – С. 48-53.

31. Романов А.Ю. Информационные сервисы МВД России / А.Ю. Романов // Специальные информационные технологии: сборник докладов межведомственной научно-практической конференции. – М., 2017. – С. 19-24.

32. Токарева С.Н. Цифровизация в деятельности органов правопорядка / С.Н. Токарева // Россия: тенденции и перспективы развития. – 2019. – № 14 (2). – С. 590-595.

33. Токбаев А.А., Аверина Е.А. Использование современных средств технического контроля при охране общественного порядка и обеспечении общественной безопасности / А.А. Токбаев и др. // Школа будущего. – 2024. – № 1. – С.73-78.

34. Фастович Г.Г. Правовое регулирование информационно-аналитической работы органов МВД России: теоретико-правовой аспект / Г.Г. Фастович // Право и государство: теория и практика. – 2023. – № 4(220). – С. 76-81.

35. Челубеева Н.Н., Байдаев М.М. Цифровая трансформация профессиональной подготовки сотрудников ОВД: проблемы и перспективы / Н.Н. Челубеева и др. // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – № 1 (15). – С. 227-234.

36. Черняков С.А., Горбатенко С.Л. Возможности использования сервисов Единой системы информационно-аналитического обеспечения деятельности МВД России в оперативно-разыскной деятельности органов внутренних дел / С.А. Черняков и др. // Проблемы правоохранительной деятельности. – 2023. – № 4. – С. 53-58.

37. Шевцов А.В. Применение некоторых современных информационных технологий в процессе организации охраны общественного порядка и обеспечения общественной безопасности / А.В. Шевцов, В.А. Милёхин // Сборник материалов XXV Международной научно-практической конференции. – М., 2023. – С. 294-300.

38. Яворский М.А. Использование цифровых технологий в административно-юрисдикционной деятельности правоохранительных органов / М.А. Яворский, Е.А. Саблина Е.А., М.С. Цымбалюк // Право и практика. – 2022. – № 2. – С. 75-81.

г) Электронные ресурсы:

1. Глава МВД заявил о критической нехватке полицейских и следователей [Электронный ресурс]. Режим доступа: URL: https://www.rbc.ru/ (дата обращения: 20.06.2025).

2. Информационные сообщения / Официальный сайт Росфинмониторинга. URL: https://www.fedsfm.ru/releases/7185 (дата обращения: 20.06.2025).

3. Краткая характеристика состояния преступности / Официальный сайт МВД России. Статистика ГИАЦ МВД России. URL: https://www.mvd.ru/Dejatelnost/statistics/reports/ (дата обращения: 20.06.2025).

4. Основные направления дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы: утв. исполняющим обязанности Министра внутренних дел РФ генералом полиции Российской Федерации В.А. Колокольцевым от 21 января 2020 г. // Специализированная территориально распределенная система СТРАС «Юрист» [Электронный ресурс]. Режим доступа: https://ви.мвд.рф/ (дата обращения: 20.06.2025).

5. Проведение анализа выполнения Плана реализации основных направлений дальнейшего развития ИСОД МВД России на период с 2020 по 2024 год (дорожная карта) и подготовка предложений по внесению изменений в

Основные направления дальнейшего развития ИСОД МВД России на период с 2020 по 2024 год: отчет о научно-исследовательской работе. Шифр «Рубикон». Гос. регистрация № 01231813. – М.: ФКУ НПО «СТиС» МВД России, 2024.

6. Роскомнадзор сообщил об утечке 500 млн данных о россиянах за один раз [Электронный ресурс]. Режим доступа: URL: https://www.rbc.ru/ (дата обращения: 20.06.2025).

ПРИЛОЖЕНИЕ

Приложение 1

Структура ИСОД МВД России

Приложение 2

Характеристика информационно-телекоммуникационных систем, применяемых в МВД России

№	Название системы	Назначение	Особенности применения
1	АСУ «Дежурная часть»	Регистрация сообщений, учет происшествий, контроль сроков реагирования	Интеграция с региональными базами, автоматизация документооборота
2	«Безопасный город»	Видеонаблюдение, аналитика, автоматизация реагирования	Работа в режиме реального времени, интеграция с системами экстренных служб
3	Паспортно-визовый сервис МВД России	Миграционный учет, контроль пребывания иностранных граждан	Проверка гражданства, регистрационные действия
4	ИСОД МВД России	Анализ преступности, хранение сводок, прогнозирование	Централизация аналитических данных, формирование отчетности