ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

В. В. Антонов, В. Р. Гурьянова, Г. А. Тугузбаев

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Уфа 2023

УДК 351.741.07:002:004(470)(075.8)
ББК 67.401.133.1ф1(2Рос)я73-1
А72

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:
кандидат педагогических наук, доцент В. П. Шумилин
(Орловский юридический институт МВД России имени В. В. Лукьянова);
кандидат технических наук С. В. Смирнов
(Казанский юридический институт МВД России).

Антонов, В. В.
А72 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.– Текст : непосредственный.

ISBN 978-5-7247-1157-9

В учебном пособии рассматриваются новейшие информационно-телекоммуникационные технологии и практические аспекты их использования для обеспечения деятельности органов внутренних, анализируются работы информационно-телекоммуникационных сетей, различные подходы и примеры управления подразделениями с помощью систем информационно-аналитического обеспечения, а также использование методов системной динамики для оценки работы следственных подразделений.

Издание предназначено для обучающихся образовательных организаций МВД России.

УДК 351.741.07:002:004(470)(075.8)
ББК 67.401.133.1ф1(2Рос)я73-1

ISBN 978-5-7247-1157-9

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность применения информационно-телекоммуникационных технологий в управленческой деятельности сохраняется постоянно. Для реализации управленческой деятельности в органах внутренних дел (далее – ОВД) ведется значительная работа по внедрению новых перспективных технологий, поэтому вопросам информационного и технического оснащения правоохранительных органов уделяется основное внимание. На это указывает содержание статьи 11 «Использование достижений науки и техники, современных технологий и информационных систем» Федерального закона от 07.02.2011 № 3-ФЗ «О полиции»[1].

Современные правоохранительные органы не могут обойтись без использования оперативно-справочных, криминалистических и розыскных систем учета, которые необходимы для эффективного расследования уголовных дел. Почти все подразделения правоохранительных органов используют эти системы для получения необходимой информации.

В статье 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] раскрывается понятие информационно-телекоммуникационной сети – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

С развитием информационных технологий преступность стала использовать возможности современных технологий для улучшения своей организации и мобильности. Преступники теперь могут действовать виртуально, скрывая свои действия от правоохранительных органов с помощью специальных программ и шифровальных средств. В то же время техническое оснащение преступников также значительно усовершенствовалось, что позволяет им совершать более сложные и профессиональные преступления, нанося ущерб государству и обществу.

Учебное пособие должно помочь обучающимся в получении знаний в области современных информационных технологий, а также связанных с информационным обеспечением деятельности ОВД и эффективной организацией индивидуального информационного пространства, автоматизацией коммуникационной деятельности, применением информационных ресурсов в профессиональной деятельности, способствующих реализации следующих задач:

---

[1] О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 03.12.2012) // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.

[2] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ч. 1. Ст. 3448.

– изучить состав, функции и конкретные возможности профессионально-ориентированного программного обеспечения, используемого в деятельности ОВД;

– знать актуальные изменения нормативных правовых актов в области защиты государственной тайны и информационной безопасности;

– изучить архитектуру и состав Единой системы информационно-аналитического обеспечения деятельности (далее – ИСОД) МВД России;

– понимать требования информационной безопасности при реализации и использовании информационных технологий в оперативно-служебной деятельности.

Данное учебное пособие предназначено для повышения эффективности работы сотрудников ОВД отечественным программным обеспечением в профессиональной деятельности, оптимизации реализуемых информационных процессов с использованием новых программных и программно-аппаратных комплексов. Пособие поможет обучающимся стать более компетентными в области защиты информации, что является важным элементом работы ОВД в настоящее время. Приобретенные знания и навыки смогут быть применены на практике при проведении оперативно-розыскной и следственной работы, а также при организации и управлении информационными процессами в работе ОВД. Использование отечественных программных продуктов позволит не только повысить эффективность работы, но и защитить государственные интересы в сфере информационной безопасности.

ГЛАВА 1. ОБЗОР ИНФОРМАЦИОННЫХ СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

1.1. Основные положения информационного обеспечения управления деятельностью подразделений ОВД

Современное управление в различных секторах требует широкого использования информационных технологий, так как аналитическая работа, планирование, контроль и оценка результатов невозможны без компьютерной техники. Однако с возрастанием динамичности процессов в обществе для принятия эффективных решений необходимо перейти на новый уровень.

Этот уровень управления включает в себя учет большого количества внутренних и внешних факторов, прогнозирование развития ситуации и принятие мгновенных решений. Традиционные методы, такие как интуиция или личный опыт руководителя, а также имеющиеся ресурсы могут быть недостаточными для эффективного управления такими задачами.

Это обстоятельство относится и к управлению деятельностью ОВД, где принятие эффективных управленческих решений требует учета и контроля различных аспектов правоохранительной деятельности в условиях неопределенности и риска. Эти аспекты включают в себя функционирование уголовного розыска, следственные действия, работу дежурной части, патрулирование территории и многое другое.

Более активное использование информационных технологий является эффективным методом для преодоления трудностей в управлении. Для этого нужна соответствующая техническая поддержка и хорошая организация информационного обеспечения управления.

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.

Изучение теории и практики информационных процессов основывается на использовании технических средств для получения информации, сбора их данных, регистрации и передачи по телекоммуникационным ка-

налам. 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.

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.

Условиями, поддерживающими этот тезис, являются:

– повсеместная автоматизация работы с документами, в том числе и в системах электронного документооборота;

– разработка профессионально ориентированных АИС;

– использование в управлении компьютеров и телекоммуникационных систем как основных составных элементов современных организационных структур.

Согласно выполняемым функциям АИС можно представить в виде нескольких составляющих элементов (рис. 1.1).

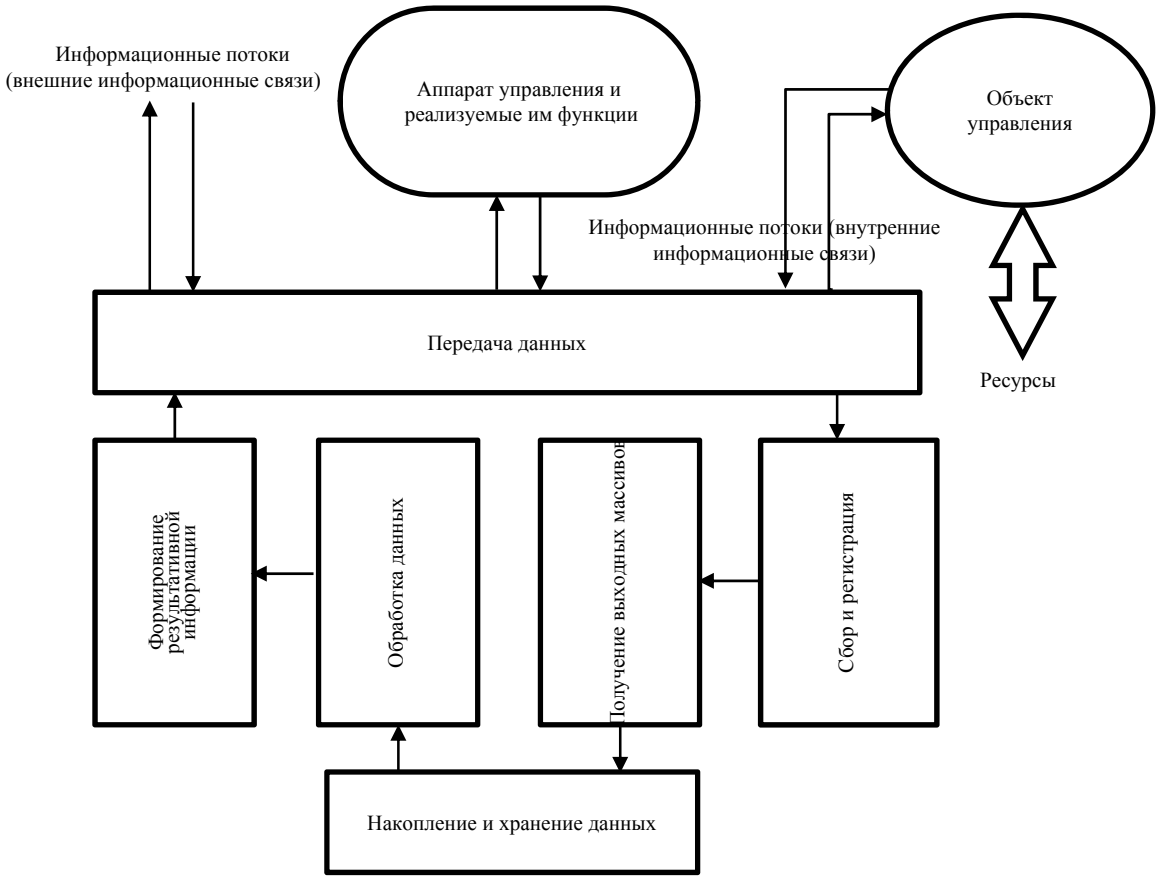

Рис. 1.1. Функциональная структура АИС

Автоматизированная информационная технология имеет различные функциональные направления, из которых определяются ее составляющие структуры. Она включает процессы по сбору и регистрации данных, подготовке информационных массивов, обработке, накоплению и хранению данных, формированию результатной информации, передаче данных от источников к месту обработки, а результатов − к конечным пользователям информации для принятия управленческих решений.

Как и в других случаях, информация юридического, криминологического и статистического характера часто проходит преобразование. Однако иногда этот процесс не требуется. Порядок выполнения процедур может быть разным и включать повторение некоторых из них.

Состав процедур преобразования информации и их выполнение зависят от объекта управления, который используется для автоматизированной обработки данных.

Обсудим специфики выполнения ключевых процедур преобразования информации в управлении деятельностью ОВД.

1. Сбор и регистрация информации для различных организационных объектов выполняются разнообразными способами. Однако наиболее сложный процесс связан с автоматизированными управленческими процессами штабов ОВД, где осуществляется первичная регистрация информации, от-

ражающей состояние деятельности подразделения и криминологической обстановки на его территории. Тем не менее, стоит отметить, что этот процесс также имеет свои особенности в дежурных частях ОВД, подразделениях тылового, финансового и документационного обеспечения, где происходит оформление и передача различных документов.

Для эффективной работы правоохранительных органов необходимо иметь достоверную, полную и своевременную информацию. Сбор и регистрация такой информации происходят в ОВД при регистрации заявлений о преступлениях, приеме информации от других подразделений и подсчете количества подозреваемых и нанесенного материального ущерба. Также в процессе сбора фактической информации осуществляется измерение, подсчет и оценка характеристик работы исполнителей.

Для сбора информации обычно используются носители, такие как документы и журналы, которые затем переносятся в компьютер в виде файлов баз данных или других форматов. Ручная запись в первичные документы приводит к значительной трудоемкости процесса, поэтому автоматизация документооборота является актуальной. Для этого используются технические средства, которые позволяют количественно измерять и регистрировать информацию, накапливать и передавать ее по каналам связи, а также вводить ее непосредственно в компьютер для дальнейшей обработки и формирования документов.

2. Передача информации может осуществляться разными способами, включая курьерскую доставку, пересылку по почте, дистанционную передачу через телекоммуникационные каналы и другие. При этом дистанционная передача данных требует использования специальных технологий, которые могут увеличивать сложность и стоимость процесса. 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 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.

3. Для получения входных массивов необходимо привести исходные данные в формат, пригодный для ввода в компьютер и записи на носители или передачи по каналам связи. Этот процесс называется машинным кодированием.

Машинное кодирование – это процесс преобразования информации в форму, которую машины могут понимать и хранить на своих устройствах. Это делается путем переноса первоначальных данных на машинные носители, такие как жесткие диски или флэш-накопители. Запись информации на машинные носители может быть самостоятельным процессом, или же это может быть результатом обработки данных. В любом случае, итоговые машинные коды используются для того, чтобы компьютер мог обрабатывать эти данные или производить действия на основе этой информации.

4. Хранение и сохранение информации необходимо для ее повторного использования. Для этого требуется иметь постоянный доступ к информации различных видов. Для этого данные необходимо накапливать и комплектовать до их обработки. Этот процесс преобразования данных осуществляется при помощи информационных баз, где данные располагаются в определенном порядке, который устанавливается в процессе проектирования базы данных. Информация может храниться на различных машинных носителях в виде информационных массивов.

Хранение и накопление данных неразрывно связаны с требованием поиска необходимой информации. Поиск данных подразумевает поиск конкретной информации на основе критериев, заданных пользователем или компьютерной системой. Это может включать как поиск информации, готовой к использованию, так и информации, которая требует корректировки или обновления. Пользователь может составить запрос на поиск нужных данных и выбрать форму их представления. Этот процесс выполняется автоматически и имеет своей целью найти нужную информацию в большом объеме данных, хранимых в системе.

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.

6. В процессе принятия решений в автоматизированной системе организационного управления специалист может использовать технические средства или основываться на анализе полученной информации без их помощи. В любом случае задача принятия решения является сложной, так как необходимо выбрать оптимальное решение, минимизируя потери ресурсов, таких как время, труд, материальные затраты и т. д.

Использование компьютеров в этом процессе позволяет улучшить качество анализа данных и постепенно перейти к автоматизации процесса выработки оптимального решения через взаимодействие пользователя с вычислительной системой. В этом помогают экспертные системы и системы поддержки принятия решений, основанные на современных технологиях.

1.2. Компоненты информационной системы ОВД

Один из основных аспектов работы управления внутренних дел – это сбор и анализ информации относительно преступлений и нарушений правил поведения. Это относится ко всем уровням работы − от выработки стратегических решений до конкретных действий по обнаружению и раскрытию преступлений и предотвращению правонарушений. Кроме того, существует строгая необходимость документирования всех характеристик объектов и субъектов преступлений, а также действий сотрудников в отношении этих объектов и субъектов. Следовательно, в работе управления внутренних дел и его сотрудников информационный аспект играет ключевую роль, и основная часть работы каждого сотрудника связана с обработкой информации.

Управленческая информация в ОВД – это информация или данные, которые были, используются или могут использоваться для принятия управленческих решений, а также для учета, анализа, планирования, прогнозирования, регулирования и контроля в ОВД. Это могут быть любые сообщения или данные, которые могут помочь управляющим в принятии основных управленческих решений в организации.

Данная информация (например, циркулирующая в управлениях МВД России) делится на следующие виды:

1) задающая (предписывающая, прескриптивная):

– постановочная (распоряжения руководства, пункты планов работ, информация оперативных сводок и т. д.);

– нормативная (указы, законы, постановления органов государственной власти и местной администрации, директивы, приказы, указания, решения коллегии МВД России, положения о подразделениях территориальных органов, должностные уставы, наставления и т. д.);

– плановая (текущие и перспективные планы работы территориальных подразделений ОВД);

2) осведомляющая (дескриптивная) – данные о текущем состоянии объекта управления ОВД – оперативной обстановке.

Содержание этого вида информации определяется информационными блоками и элементами, составляющими оперативную обстановку.

Это прежде всего два крупных блока:

– внешние условия, факторы среды функционирования;

– внутренние условия (параметры территориального подразделения ОВД).

В свою очередь, каждый из этих блоков имеет по два составляющих элемента:

1) информационный элемент оперативной обстановки, определяемой внешними условиями, включает в себя:

– информацию о состоянии правопорядка и законности; преступности и иных правонарушениях, лицах, их совершивших; других явлениях в обществе: пьянстве, наркомании, психических и венерических заболеваниях; самоубийствах, чрезвычайных происшествиях, этнических конфликтах; крупных авариях, террористических актах и т. д. (элемент представлен, например, в формах статистической отчетности);

– информацию о среде функционирования ОВД: о природно-географических и демографических условиях; социальном, экономическом, политическом, культурном развитии региона; национальной структуре; миграционных процессах; доходах населения; наличии безработицы (в том числе скрытой); ценах; потреблении промышленных и продовольственных товаров, в том числе вино-водочных изделий;

2) информационный элемент оперативной обстановки, определяемой внутренними условиями, представлен:

– информацией о самих ОВД: их структуре, штатах, кадрах, расстановке сил и средств, технической оснащенности, состоянии дисциплины и законности, социальной защите личного состава;

– информацией о результатах оперативно-служебной, в том числе управленческой, деятельности.

В территориальных органах непосредственно составляется только одна из форм отчета, представляющая собой элемент такого типа, – форма 1-А «Оперативная статистическая информация о состоянии преступности и результатах выявления и раскрытия преступлений», которая направляется в вышестоящие подразделения. Этим занимаются сотрудники штаба, ответственные за учетно-регистрационную работу в данном подразделении;

3) вспомогательная (ориентирующая) информация:

– справочные данные о районе: экономические, демографические, географические, административно-территориальные и т. д.;

– справочные данные о дислоцированных на обслуживаемой территории подразделениях ОВД и т. д.;

– организационная документация (телефонные справочники, схемы оповещения, сведения о районных органах управления и т. д.);

– служебная научно-методическая информация (материалы семинаров-совещаний, аналитические справки, отчеты и т. д.);

4) рабочая информация, в которую входят переработанные фрагменты задающей, ориентирующей и вспомогательной информации.

Эффективное использование информации, ее доступность и полезность связаны с информационными системами, которые обеспечивают реализацию процессов сбора, хранения, обработки и выдачи информации, необходимой для успешной работы субъектов и объектов управления.

Состав информационной системы в наиболее общем виде содержит следующие компоненты:

– информация, которая обеспечивает выполнение одной или нескольких функций управления;

– методы и процедуры обработки информации (сбор, передача, хранение и преобразование информации);

– персонал, призванный поддерживать функционирование информационной системы;

– технические средства;

– коммуникации, реализующие направления и процесс обмена информацией.

Для более ясного представления основных характеристик информационного обеспечения управленческой деятельности можно представить его в виде последовательно переходящих из одного в другой этап деятельности соответствующих служб и отдельных сотрудников с целью улучшения и оптимизации процесса. В этом контексте информационное обеспечение рассматривается как критическое звено для обеспечения правильного функционирования процесса управления, где каждый отдельный этап имеет свои особенности и требует соответствующего подхода в направлении оптимизации с помощью информационных технологий и инструментов. Эти этапы схематично могут выглядеть следующим образом (табл. 1.1).

Таблица 1.1

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?»

Окончание таблицы 1.1

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 соответствия современным требованиям управления в ОВД необходимо шире использовать информационные и телекоммуникационные технологии, внедрять АИС, которые обеспечивают полный цикл обработки управленческой информации. Организация эффективной системы информационного обеспечения является неотъемлемой частью современного управления и включает в себя не только обеспечение оперативного доступа к информации, но и анализ, прогнозирование и подготовку оптимальных решений.

1.3. Современное состояние и тенденции развития информационных технологий в ОВД

В последнее время в деятельности ОВД выделяют новый этап внедрения ИТ. Он связан с реформированием системы МВД России. Современное требование к сотрудникам ОВД – это обязанность использовать в своей деятельности «достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру»[1].

В этих целях создан единый центр, осуществляющий координацию работ по продвижению ИТ в системе МВД России. Департамент информационных технологий, связи и защиты информации МВД России (далее – ДИТСиЗИ МВД России) как раз и является таким центром. Благодаря его работе можно отметить такие положительные тенденции, как ликвидация хаотичного внедрения ИТ в деятельность ОВД, формулирование единых требований к совместимости информационных систем.

В последние времена МВД России добилось успехов в разработке новых технических решений для ИСОД. Были созданы новые системы обработки данных, которые позволяют использовать информационные системы и прикладные сервисы ИСОД с более высокой производительностью и эффективностью. Все мероприятия направлены на улучшение функциональности и качества ИСОД МВД России.

[1] О полиции : Федеральный закон от 07 февраля 2011 № 3-ФЗ (ред. от 03.12.2012) // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.

Сегодня ДИТСиЗИ МВД России проводит сложный комплекс мероприятий для перевода всех подразделений МВД России на единое программное обеспечение по ключевым направлениям работ. Целью создания и использования информационной системы оперативно-диспетчерского управления в МВД России является обеспечение унификации процессов: все следственные отделы, работающие на разных уровнях (локальном, региональном, межрегиональном и федеральном), должны использовать одно прикладное приложение. Оно должно быть адаптировано к особенностям задач, выполняемых на каждом уровне управления, и обеспечивать единую базу данных.

Для лучшего понимания обращаемся к краткому описанию особенностей ИСОД МВД России и объясняем, почему создание и использование данной системы в настоящее время и в будущем являются крайне актуальными и практически значимыми.

В ОВД за последние годы проведена значительная работа по развитию информационной инфраструктуры. Была создана единая информационно-телекоммуникационная система ОВД на основе ведомственной инфраструктуры и обеспечен базовый уровень технического оснащения подразделений ОВД. В дальнейшем в результате проведенных работ появилась интегрированная мультисервисная телекоммуникационная система (далее – ИМТС) МВД России, к которой подключили узлы связи подразделений системы МВД России.

Главной причиной введения ИСОД МВД России стало отсутствие единой системы и стандартов внедрения автоматизированных систем. Ранее были созданы различные программные решения для отдельных служб, таких как полиция, уголовный розыск и экономическая безопасность, каждое из которых выполняло свои задачи. Однако для эффективной работы необходимо было иметь общую информационную базу для всех структур. Получение данных из разных систем оказалось затруднительным из-за несовместимости форматов и требовало установки нескольких компьютеров на одном рабочем месте.

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 обслужи-

вание систем, низкой надежности и недостаточному уровню производительности.

ИСОД МВД России – это комплекс систем обработки информации, программ и технических устройств, связывающих все разделы МВД России и необходимых для эффективного выполнения задач служебной деятельности. Её главной целью является автоматизация основных видов деятельности МВД России, централизованное хранение и обработка данных.

Сотрудники ИСОД МВД России, каждое подразделение которых имеет доступ к единому источнику информации, могут взаимодействовать друг с другом, благодаря чему обеспечивается правильное сопоставление доступа к информационным ресурсам. Важной особенностью является то, что система позволяет повысить эффективность принимаемых решений, улучшить качество отчетов и проводить оперативный и своевременный анализ ключевых показателей деятельности МВД России на основе грамотно составленных отчетов и актуальных данных. Другой значимый результат состоит в более эффективном выполнении государственных функций и предоставлении государственных услуг благодаря уменьшению времени и трудоемкости операций по обработке информации.

Сотрудники ИСОД МВД России получают доступ к необходимым компонентам и работают с ними на основе ведомственного облака. Это облако представляет собой распределенную систему ЦОД, которые связаны между собой. Таким образом, все базовые приложения и базы данных для ИСОД МВД России размещаются в этом облаке.

Для функционирования ведомственного облака МВД России была необходима перестройка организации ИТ-инфраструктуры. Все объекты МВД России были непосредственно подключены к облаку, чтобы обеспечить быстрый доступ к его сервисам. Скорость доступа определялась количеством прикладных решений, используемых на каждом объекте. Для обеспечения безопасности передаваемых данных соответствующие каналы закрывались с помощью шифрования. Для формирования единого хранилища информации использовались типовые программные решения и данные загружались из уже действующих информационных систем.

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 со-

временные, 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.

Основное внимание в разработке программного обеспечения было уделено автоматизации ключевых направлений деятельности МВД России, таких как уголовный розыск, предварительное следствие, дознание, исполнение административного законодательства, работа участковых уполномоченных, дежурных частей, патрульно-постовой службы полиции, ГИБДД и других. Это позволяет сотрудникам МВД России эффективно и оптимально выполнять свои обязанности, а также повышает эффективность борьбы с преступностью.

ЦОД МВД России применяет передовые технологии виртуализации и динамического масштабирования для оптимизации производительности в зависимости от количества и типа запросов пользователей. Эти технологии обеспечивают максимальную гибкость и масштабируемость приложений, которые могут использоваться исключительно сотрудниками МВД России с гарантией на обеспечение безопасности хранения и обработки информационных ресурсов.

Использование данной системы управления позволяет повысить эффективность принятия решений менеджерами. Это достигается путем анализа сводной информации, основанной на актуальных данных об объекте управления, а также поиска закономерностей, прогнозирования развития ситуации и ее характеристики. В конечном итоге использование этой системы помогает оптимизировать процесс планирования управляющих мероприятий.

Межведомственное электронное взаимодействие при оказании государственных услуг не осталось без внимания со стороны МВД России. Здесь разработаны и зарегистрированы электронные сервисы, программное обеспечение и защищенные каналы связи, где МВД России является поставщиком данных. Работники, непосредственно участвующие в предоставлении государственных услуг, получили доступ к специальному про-

граммному обеспечению для межведомственного электронного взаимодействия.

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. Также была организована подготовка специалистов в области технической защиты информации на базе образовательных учреждений МВД России, в рамках которых изучались вопросы обеспечения безопасности информации в подразделениях МВД России.

В сфере информационной безопасности ОВД решаются задачи по защите информации, информационных ресурсов и систем от утечки, несанкционированного доступа, взлома, модификации, копирования и т. д. Кроме того, в настоящее время важными требованиями являются разработка системы информационной безопасности ОВД с использованием облачной архитектуры и создание системы мониторинга состояния информационной безопасности. При этом акцент делается на использовании отечественных средств и систем защиты информации.

В документах, которые регулируют информационную безопасность в органах внутренних дел, определены основные направления, которые являются наиболее существенными и актуальными в свете современного состояния и развития информационно-коммуникационных технологий.

К таковым относятся:

– выявление, оценка, прогнозирование и ликвидация новых угроз информационной безопасности ОВД;

– модернизация программных, программно-технических и технических средств защиты, в том числе криптографической;

– реализация эффективной системы доступа к информационным ресурсам и информационным системам ОВД;

– обеспечение информационной безопасности при межведомственном информационном взаимодействии с федеральными органами государственной власти;

– организация защиты информации в информационных системах ЦОД от несанкционированного доступа и деструктивных воздействий;

– обеспечение защищенного доступа пользователей к информационным ресурсам ЦОД.

Для успешной реализации стратегий повышения безопасности информационных систем в полиции крайне важно инвестировать в обучение и повышение уровня компетенции сотрудников, работающих в области защиты данных. Это является ключевым условием для достижения поставленных целей и векторов развития в этой сфере.

Одной из главных задач МВД России является обеспечение общественной безопасности. В связи с этим МВД России активно работает над внедрением инновационных технологий в работу полицейских подразделений и совершенствованием технического обеспечения, чтобы обеспечить более эффективный контроль ситуации и быстрое реагирование на происшествия.

Введение системы мобильного доступа к информационным ресурсам на базе АПК «Барс» в наружные подразделения полиции является примером использования современных технологий в этой области. Эта система позволяет полицейским получать оперативную и правдивую информацию о гражданах, автомобилях и лицах, которые находятся в розыске, из информационных систем МВД России. Это помогает не только в расследовании преступлений «по горячим следам», но и в предотвращении несанкционированного доступа к конфиденциальной информации и обеспечении безопасности.

В ИСОД МВД России наблюдается тенденция интеграции информационных ресурсов и систем, однако разработка и использование средств ИТ для решения специфических задач в ОВД также является перспективным направлением развития ИТ.

Для решения аналитических задач можно использовать программную платформу класса Business Intelligence (далее – BI), которая позволяет разработать прикладные решения для обработки данных. Например, можно создать систему ассоциативного поиска и обработки данных в оперативной памяти, а также извлекать и объединять информацию из разных источников.

Ассоциативный поиск и обработка данных в оперативной памяти осуществляются по всем элементам массива данных. Это напоминает работу интернет-поисковика: если ввести слово или фразу в строку поиска, то система начнет показывать результаты уже по мере их набора. Таким образом, пользователь может получить нужную информацию быстро и эффективно.

Если необходимо извлечь информацию из разных источников и объединить ее, то для представления данных применяется множество графических элементов. Среди них могут быть таблицы, сводные таблицы, диаграммы, графики, гистограммы, календари, слайдеры и интеграция с онлайн-картами и прочее. Платформа позволяет пользователям с необходи-

мыми правами анализировать отчеты в любом месте, где есть доступ к браузеру.

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.

Для оценки работы дежурной службы используются специальные аналитические показатели, которые отражают общую картину ее деятельности и качество реагирования на инциденты. Эти показатели включают количество происшествий, среднее время их обработки, рейтинг правонарушений и соотношение ложных и подтвержденных вызовов. Важно отметить, что многие из этих показателей связаны с конкретными территориями, на которых дежурная служба действует, что позволяет проводить анализ работы в различных административных округах.

Аналитика и статистика являются очень важными и востребованными направлениями, заинтересованными аппаратом управления. Особенно важным является решение задач, связанных с анализом деятельности подразделений через автоматизацию составления отчетности. Этот класс задач включает в себя такие важные операции, как анализ уголовной статистики и оперативных данных, таких как количество возбужденных/отказанных уголовных дел и анализ уголовных дел по конкретным статьям. Также важны данные, связанные с работой ГИБДД, такие как учет краж транспортных средств по маркам автомобилей, время суток и территориальному признаку.

Использование инструментов BI позволяет решать вопросы управления кадрами, например, контролировать количество сотрудников на территориях с высокой преступностью. Он также помогает улучшить профилак-

тические меры, выделять группы наиболее уязвимых к преступлениям и сосредоточивать усилия на их предупреждении и предотвращении.

В результате широкомасштабных реформирований МВД России, значительных успехов было достигнуто в сфере информационной поддержки деятельности ОВД. В частности, была создана современная информационно-телекоммуникационная инфраструктура на базе ИМТС МВД России, были внедрены ИСОД МВД России и ЦОД, а также были разработаны специализированные территориально распределенные системы. Нормы и стандарты, регулирующие требования к новым и существующим АИС, на основе облачных технологий были унифицированы, акцент в требованиях к АИС и технологиям был смещен в сторону аналитических и интеллектуальных функций.

Вопросы для самоподготовки

1. Какое информационное обеспечение используется в органах внутренних дел?
2. Какие компоненты входят в информационную систему ОВД?
3. Какие существуют тенденции развития информационных технологий в органах внутренних дел?
4. Каким образом информационные технологии помогают управлять деятельностью подразделений в ОВД?
5. Какие программные средства используются в органах внутренних дел?

ГЛАВА 2. СЕРВИСЫ ИСОД МВД РОССИИ

2.1. 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 информационной системы ЦОД для информационно-аналитической поддержки деятельности подразделений МВД России.

Сегодня ИСОД МВД России представляет собой совокупность используемых в ОВД автоматизированных систем обработки информации, программно-аппаратных комплексов и комплексов программно-технических средств, а также систем связи и передачи данных, необходимых для эффективного обеспечения служебной деятельности МВД России.

Система является единым источником информации для всех подразделений МВД России. Она позволяет:

− организовывать электронное взаимодействие между ними и предоставлять разграничение доступа к информационным ресурсам;

− более эффективно принимать решения за счет улучшения качества подготавливаемых отчетов, основанных на актуальных и достоверных данных, обеспечения оперативного и своевременного анализа ключевых показателей деятельности МВД России;

− повышать качество выполнения государственных функций и предоставления государственных услуг за счет снижения временных затрат и трудоемкости операций по обработке информации.

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.

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

Рассмотрим архитектуру ИСОД МВД России. Система состоит из нескольких функциональных подсистем, таких как:

---

[1] Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012-2014 годах : приказ МВД России от 30 марта 2012 г. № 205. Доступ из справ.-правовой системы «КонсультантПлюс».

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.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД России:

1) сервис электронной почты МВД России (далее – СЭП). Предназначен для автоматизации процессов обмена электронными сообщениями, образующимися в ходе деятельности сотрудников, федеральных государственных гражданских служащих и работников центрального аппарата МВД России, территориальных органов, а также иных подразделений и организаций, созданных для выполнения задач и осуществления полномочий, возложенных на ОВД. При этом СЭП обеспечивает обмен электронными сообщениями не только между сотрудниками (внутри сети), но и между сотрудниками и внешними адресатами;

2) сервис электронного документооборота (далее – СЭД). Его задача – повышение эффективности организационно-управленческой (административной) деятельности ОВД, связанной с документационным обеспечением и представлением юридически значимого документооборота (см. об этом сервисе подробнее ниже);

3) сервис видео-конференц-связи МВД России (далее – СВКС-М). Предназначен для оптимизации и ускорения процесса получения и обработки информации для принятия управленческих решений, а также оперативной связи между сотрудниками МВД России;

4) сервис управления доступом к информационным системам и ресурсам (далее – СУДИС). Необходим для централизованного управления доступом пользователей и сервисов к сервисам ИСОД МВД России. Он обеспечивает выполнение следующих функций:

– идентификация и аутентификация пользователей;

– управление реестрами пользователей и сервисов ИСОД;

– назначение и отзыв полномочий пользователей и сервисов ИСОД;

– протоколирование событий безопасности сервисов ИСОД;

– подписание электронных документов с использованием средств электронной подписи;

5) ведомственный информационно-справочный портал (далее – ВИСП). Инструмент информационной поддержки управления и использования общих информационных ресурсов для сотрудников МВД России и других правоохранительных органов, который доступен для всех пользователей ИСОД МВД России. Он способствует формированию единого информационного пространства, структуризации и хранения ведомственной и межведомственной информации, усовершенствованию внутренних коммуникаций и сокращению временных затрат на сбор, обработку и поиск служебной информации. Он предоставляет сотрудникам доступ к следующим видам информации:

– внутренней ведомственной информации, связанной с ИСОД МВД России;

– сведениям об организационно-штатной структуре МВД России;

– адресно-телефонному справочнику МВД России;

– информированию сотрудников о мероприятиях, связанных с ИСОД МВД России.

Областью применения ВИСП является деятельность сотрудников и должностных лиц подразделений МВД России центрального аппарата и территориальных органов.

Для работы в ВИСП пользователь должен иметь учетную запись в СУДИС;

6) Интернет-сайт МВД России. Предназначен для предоставления пользователям сети Интернет информации о деятельности МВД России, позволяет получить информацию о руководстве, структуре и деятельности МВД России, результатах работы пресс-службы, о документах, регламентирующих деятельность МВД России, об отделениях полиции, участковых и т. д.

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.

Следует отметить, что указанный перечень прикладных сервисов не является исчерпывающим: ИСОД МВД России находится в постоянном развитии, дополняется новыми сервисами, изменяются названия и функционал старых, поэтому для получения наиболее актуальной информации о сервисах рекомендуем обратиться непосредственно к ресурсу ИСОД МВД России. При этом следует указать на то, что базовый состав ИСОД МВД России, а также инструкция об организации работ по эксплуатации сети представлены в соответствующем нормативном акте МВД России закрытого характера.

Все прикладные сервисы работают по единым технологическим и программным правилам, учитывают определенную функциональность и прикладной характер применения, что влияет на их интеграцию в ИСОД МВД России.

Для обеспечения доступа сотрудников к компонентам ИСОД МВД России и работы с ними создано полноценное ведомственное облако на основе виртуальной среды функционирования программных ресурсов и территориально распределенной системы связанных между собой ЦОД. Все базовые приложения и формируемые в них базы данных размещаются в этом облаке. Для реализации этого проекта была перестроена схема организации

ИМТС МВД России. Все объекты МВД России напрямую подключаются к облаку с обеспечением необходимой скорости доступа к его сервисам.

2.2. Подсистема информационной безопасности

В связи со значимостью информационных ресурсов ИСОД МВД России уделяется большое внимание обеспечению безопасности, обрабатываемой в системе информации. В ее состав входит подсистема информационной безопасности (далее – ПОИБ), включающая широкий набор современных средств защиты, централизованно управляемая и функционирующая с учетом строгого протоколирования событий информационной безопасности, оперативного реагирования на инциденты и систематического аудита безопасности на предмет уязвимостей на всех уровнях ведомственной информационно-технологической инфраструктуры.

Основной задачей ПОИБ является обеспечение для информации:

– конфиденциальности, целостности и доступности;

– защиты;

– достоверности;

– непрерывности обработки.

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. 2.1).

СУДИС отвечает за управление доступом пользователей в систему и к сервисам ИСОД МВД России, обеспечивает единую точку входа в сервисы ИСОД МВД России и регистрирует события безопасности.

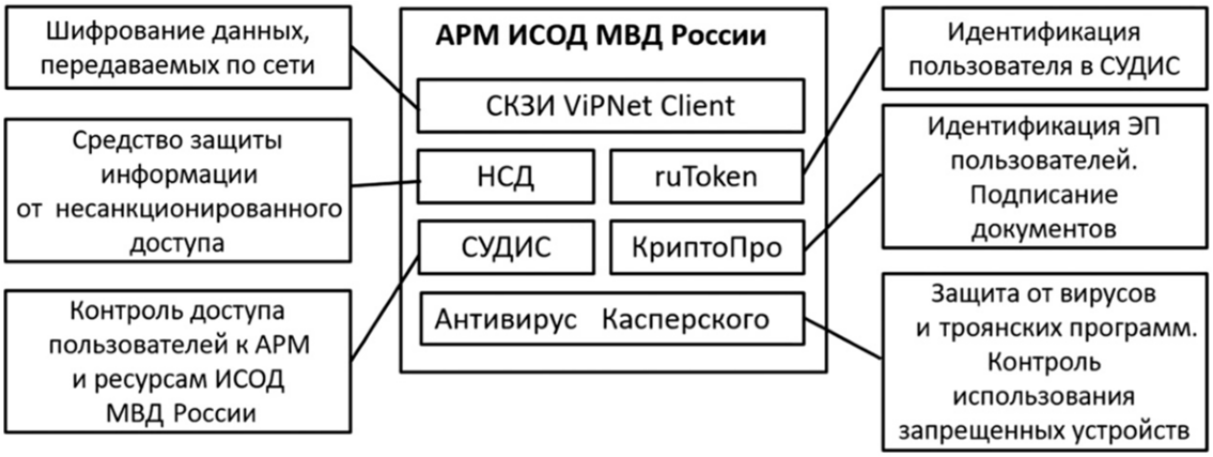

Рис. 2.1. Состав системы защиты АРМ ИСОД МВД России

С его помощью реализуется управление полномочиями как пользователей, имеющих доступ к сервисам, так и самих сервисов ИСОД МВД России и предоставляется доступ к ресурсам с помощью электронной подписи. Данный сервис – один из ключевых элементов подсистемы информационной 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.

Ежегодно в отношении информационной инфраструктуры МВД России регистрируется значительное количество компьютерных атак. Это свидетельствует о высокой критичности объектов ИТ МВД России. В этой связи во взаимодействии с ФСБ России разработан сегмент государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА МВД).

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

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.

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.

2.3. Сервис электронного документооборота

В качестве иллюстрации основных принципов построения и базовых технологий использования прикладных сервисов остановимся на наиболее популярных. Это один из сервисов обеспечения повседневной деятельности – сервис электронного документооборота (далее − СЭД). Спроектирован с учетом обеспечения масштабируемости функциональных компонент для автоматизации процессов документооборота во всех структурах ОВД.

При разработке СЭД за основу был взят принцип сервис-ориентированной архитектуры (англ. SOA, service-oriented architecture). Сервис-ориентированная архитектура представляет собой подход, при котором разрабатываемая информационная система делится на распределенные, слабо связанные заменяемые сервисы со стандартизированным интерфейсом. Сервис может быть реализован как независимое приложение или как компонент другого приложения с возможностью последующего выделения.

Задачи, решаемые СЭД:

1) повышение полноты и уровня оперативности информационной поддержки принятия управленческих решений в системе МВД России;

2) повышение уровня информационной поддержки и эффективности организационно-управленческой (административной) деятельности подразделений делопроизводства и режима территориальных органов и организаций;

3) повышение уровня информационного взаимодействия в части обмена юридически значимыми электронными документами;

4) создание единого информационного пространства документационного обеспечения в ОВД;

5) оптимизация потоков документов между различными уровнями ОВД;

6) обеспечение единообразия работы с электронными документами в ОВД с сохранением защищенности, управляемости и доступности документов;

7) обеспечение сквозного контроля прохождения документов и повышение уровня исполнительской дисциплины сотрудников;

8) обеспечение безопасного обмена документами в рамках СЭД;

9) обеспечение безопасного хранения и разграничения доступа к информации, включая протоколирование и аудит действий пользователей и электронную подпись.

СЭД обеспечивает обработку различных типов документов: регистрацию, контроль исполнения, архивное хранение входящих документов, обращений граждан, нормативных правовых актов, приказов и т. д.; позволяет импортировать информацию о документах из смежных систем (из системы межведомственного электронного документооборота, с официального сайта МВД России и др.). Также к функциям сервиса относятся поиск по зарегистрированным документам, использование различных справочников и классификаторов, построение отчетов, формирование дел в соответствии с номенклатурой.

В составе СЭД выделяют следующие группы сервисов:

1) интеграционные сервисы, обеспечивающие интеграцию между подразделениями документационного обеспечения и единое пространство документооборота в рамках МВД России;

2) документационные сервисы, позволяющие автоматизировать работу подразделений документационного обеспечения МВД России и исполнителей в части электронного документооборота. Это основная функциональная группа СЭД, в которую входят сервисы, предназначенные для непосредственной обработки документов;

3) мобильные сервисы – совокупность приложений для планшетных компьютеров, позволяющих автоматизировать деятельность руководителей подразделений МВД России по вынесению резолюций (выдаче поручений).

После входа в систему пользователю предлагается выбрать один из сервисов для работы с документами, в зависимости от его роли в организации (руководитель, делопроизводитель, исполнитель). При выборе сервиса «Документы», который предназначен для обработки регистрационных карточек, на экране отображается пользовательский интерфейс этого сервиса. Через него можно выбрать конкретный документ из списка и просмотреть полную информацию о нем, которая хранится в журнале документов. Та-

ким образом, пользователь сможет быстро и удобно обрабатывать документы и получать всю необходимую информацию о них.

Порядок работы с сервисом соответствует особенностям организации делопроизводства, изложенным в Инструкции по делопроизводству в ОВД Российской Федерации[1]. СЭД может быть использован только для управленческой (административной) деятельности подразделений ОВД, связанных с документационным обеспечением ОВД и представлением юридического значимого документооборота.

2.4. Федеральная информационная система Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации

Сервис специального программного обеспечения Федеральной информационной системы Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации (далее – ФИС ГИБДД-М). Это специальное программное обеспечение, которое 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.

Основными задачами ФИС ГИБДД-М являются:

1) автоматизация административных регламентов государственных услуг по регистрации транспортных средств, выдаче водительских удостоверений и получению информации об административных правонарушениях;

2) унификация и приведение АИС Госавтоинспекции в соответствие с современными требованиями доступности данных и надежности функционирования;

3) обеспечение информационного взаимодействия с ведомственными информационными ресурсами для создания единого информационного пространства МВД России;

4) формирование единой модели данных автоматизированной системы Госавтоинспекции;

5) обеспечение функционирования системы в режиме реального времени;

6) уменьшение расходов на создание, поддержку и эксплуатацию автоматизированных информационных систем, используемых в Госавтоинспекции.

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

---

[1] Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации : приказ МВД России от 20 июня 2012 № 615. Доступ из справ.-правовой системы «КонсультантПлюс».

1. Подсистема «Транспортные средства» предназначена для автоматизации регистрационных действий для транспортных средств и предоставления государственной услуги по регистрации автомототранспортных средств и прицепов к ним, а также обеспечения межведомственного взаимодействия в ходе предоставления государственной услуги.

2. Подсистема «Водительские удостоверения» обеспечивает автоматизацию функций Госавтоинспекции по учету сведений о правах лиц на управление транспортными средствами, выдаче водительских удостоверений и предоставлению государственной услуги по приему экзаменов на право управления транспортным средством.

3. Подсистема «Специальная продукция» предполагает учет изготовленной и распределенной в подразделениях Госавтоинспекции и Федеральной таможенной службы специальной продукции. Также реализована возможность автоматизированного формирования реестра утраченных, похищенных, уничтоженных, выбракованных экземпляров спецпродукции.

4. Подсистема «Административные правонарушения» позволяет автоматизировать производство по делам об административных правонарушениях участников дорожного движения, обеспечить выполнение делопроизводственных функций и взаимодействие с Федеральной службой судебных приставов и Федеральным казначейством.

5. Подсистема «Получение и предоставление сведений» предназначена для организации взаимодействия с помощью других информационных систем как МВД России, в том числе ГИАЦ МВД России, так и иных ведомств и организаций, например Интерпола.

Работа с каждой из названных подсистем ФИС ГИБДД-М строится по схожему принципу, который состоит в выборе действия или режима (постановка транспортного средства на учет, лишение водительского удостоверения и др.) и заполнении соответствующей формы необходимыми данными.

Одним из значимых и несомненных достоинств развертывания прикладных сервисов ИСОД МВД России является наличие понятных и подробных инструкций для различных категорий пользователей, которые постоянно дорабатываются с учетом изменений в функционале программных средств.

Эксплуатация ФИС ГИБДД-М обеспечивает в полном объеме обработку и обмен данными между подразделениями Госавтоинспекции. В любой момент сотрудникам доступна информация о регистрации автомобиля, лишении права на управление транспортным средством и др. Для граждан обеспечено получение информации о штрафах за совершение административных правонарушений и сведений об их оплате.

Детальное описание технологии работы с прикладными сервисами ИСОД МВД России доступно на соответствующем портале, где для каждо-

го 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.

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

Эксплуатация и развитие инфокоммуникационной платформы МВД России невозможны без тщательно продуманной и планомерно ведущейся работы по защите информации, о чем мы уже говорили выше, когда рассматривали ПОИБ.

В целях принятия организационных и технических мер по защите информации в ведомственных информационных системах разработаны и утверждены модели угроз и нарушителей ИСОД МВД России. При этом доступ к сервисам и информационным ресурсам осуществляется с использованием персональных электронных идентификаторов и сертификата открытого ключа электронной подписи в рамках делегированных прав доступа.

Одной из главных задач внедрения новых ИТ в деятельность ОВД является организация эффективного внутриведомственного информационного взаимодействия на основе формирования единой системы информационно-аналитического обеспечения ОВД.

Именно на это направлено сегодня развитие современной целостной информационно-телекоммуникационной системы ОВД. В этой связи особое внимание уделяется выработке сетевых интеграционных решений, обеспечивающих надежность и эффективность функционирования ИМТС МВД России в составе ИСОД МВД России, обладающей требующимся для ОВД комплексом современных технических и технологических возможностей.

Отметим, что к настоящему времени достигнуты значительные успехи в развитии информационной и телекоммуникационной инфраструктуры ОВД. При этом одним из главных достижений является создание и ввод в эксплуатацию ИСОД МВД России. Прикладные сервисы, входящие в состав этой системы, соответствуют основным направлениям деятельности подразделений системы МВД России. Архитектура ИСОД МВД России выполнена с учетом перспектив развития инфокоммуникаций в ОВД, к которым относят дальнейшую интеграцию информационных систем, повышение эффективности функционирования сервисов ИСОД, повышение пропускной способности ИМТС МВД России и повышение доступности информационных услуг для сотрудников.

Вопросы для самоподготовки

1. Какая система обеспечивает деятельность МВД России?
2. Какие задачи решает подсистема информационной безопасности?
3. Какой сервис облегчает работу с документами в МВД России?
4. Что такое ФИС ГИБДД-М и какие возможности он предоставляет?
5. Какие еще сервисы используются в работе МВД России и зачем они нужны?

ГЛАВА 3. ОСНОВЫНЕ ХАРАКТЕРИСТИКИ И МЕТОДЫ РАБОТЫ С ОПЕРАЦИОННОЙ СИСТЕМОЙ ОБЩЕГО НАЗНАЧЕНИЯ ASTRA LINUX CE (ОРЁЛ)

3.1. Начало и завершение работы

Графический вход пользователя в систему осуществляется при помощи утилит fly-dm (запуск серверной части системы) и fly-qdm (поддержка графического интерфейса), переход к которым происходит после окончания работы загрузчика. Утилиты обеспечивают загрузку графической среды для работы пользователя в системе, соединение с удаленным XDMCP-сервером, а также завершение работы системы. После установки операционной системы (далее – ОС) значения параметров графического входа устанавливаются по умолчанию. Изменение установленных значений осуществляется с помощью утилиты рабочего стола fly-admin-dm («Настройка графического входа») в режиме администратора (рис. 3.1).

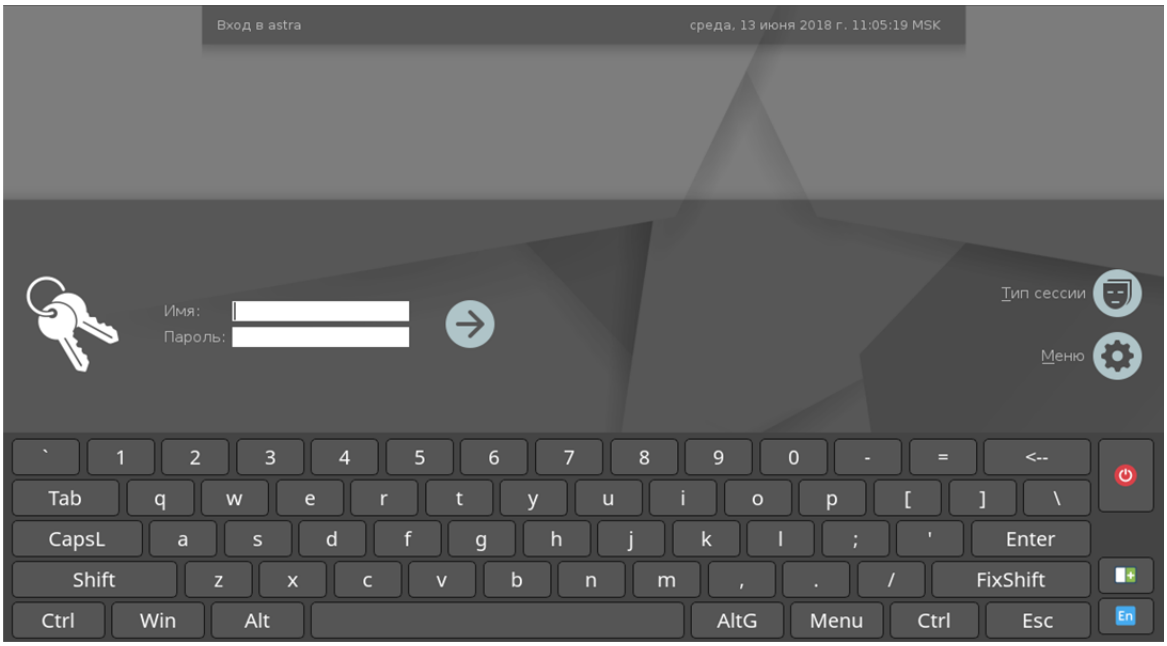

Рис. 3.1. Окно входа в систему

Для входа в систему необходимо в соответствующих полях ввести имя пользователя и пароль. Если для пользователя заданы мандатный уровень и категории, то после ввода пароля отобразится окно выбора соответствующих значений.

Описание утилит fly-dm, fly-qdm и fly-admin-dm можно найти в электронной справке. Вызов электронной справки осуществляется с помощью ярлыка «Помощь», размещенном на первом рабочем столе, или путем нажатия клавиши <F1> в активном окне графической программы.

Если рабочий стол Fly запущен, то для завершения работы пользователю следует нажать кнопку меню «Пуск» на панели задач и затем на открывшейся панели меню нажать на кнопку [Завершение работы] (в случае классического меню «Пуск» – выбрать пункт «Завершение работы») либо выполнить в терминале команду: fly-shutdown-dialog.

Откроется окно «Выход или выключение» для установки режима завершения работы и выключения (рис. 3.2).

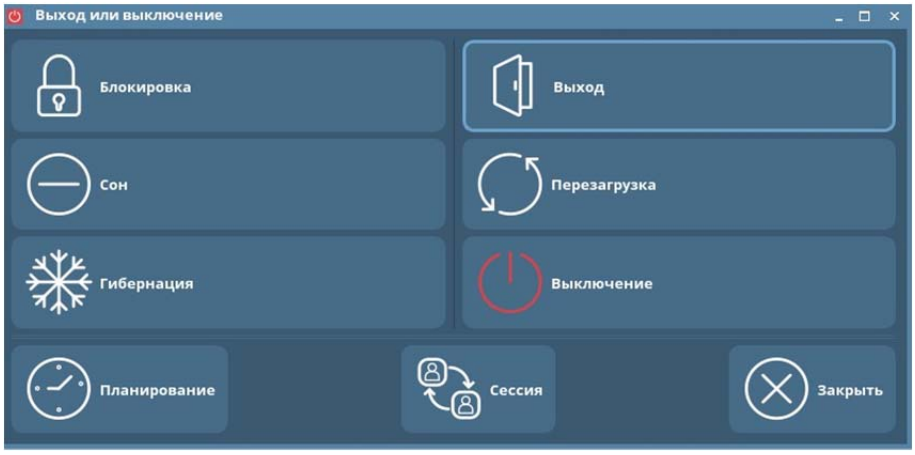

Рис. 3.2. Окно для выбора режима завершения работы

Для завершения работы в графическом режиме выбрать один из вариантов:

– [Выход] – завершается пользовательская сессия и выполняется переход в окно графического входа в систему;

– [Перезагрузка] – выполняется перезапуск ОС;

– [Выключение] – выполняется программа выключения компьютера.

Описание установки всех режимов завершения работы и выключения приведено в электронной справке к программе «Менеджер окон» (утилита fly-wm).

Переход в консольный (текстовый) режим работы может быть осуществлен из окна графического входа в систему или из графического режима работы.

Для перехода в консольный режим из графического окна входа в систему следует нажать кнопку [Меню] графического окна и в открывшемся меню выбрать пункт «Консольный вход». Появится модальное окно с сообщением о том, что переключение в консольный режим приведет к показу только консольного входа, а графический вход будет показан снова через 10 с после окончания последнего успешного консольного входа или через 40 с, если ни один консольный вход не будет выполнен. Управляющие кнопки окна:

– [Да] – закрыть окно и выполнить переход к виртуальной консоли;

– [Отмена] – закрыть окно и вернуться в окно графического входа в систему.

После перехода к виртуальной консоли на экране монитора появится приглашение командной строки. Для входа в систему следует ввести имя учетной записи пользователя и пароль, а также подтвердить мандатный уровень и категорию пользователя, если они заданы.

Для завершения работы в консольном режиме следует выполнить команду: exit

На экране монитора снова отобразится приглашение командной строки. Если после этого не выполнять других операций, то через 10 секунд будет выполнен переход к графическому окну входа в систему.

Для перехода в консольный режим из графического режима следует нажать на клавиатуре сочетание клавиш <Ctrl+левый Alt+F1>, либо <Ctrl+левый Alt+F2> и т. д. до <Ctrl+левый Alt+F6>. Будет выполнен переход к одной из шести виртуальных консолей. Для возврата из консольного режима к графическому нажать <Ctrl+левый Alt+F7>.

3.2. Рабочий стол Astra Linux

Защищенная графическая подсистема в составе ОС функционирует с использованием графического сервера Xorg.

В нее также входит рабочий стол Fly, который состоит из программы «Менеджер окон» (утилита fly-wm) и набора пользовательских и административных графических утилит и программ.

Для загрузки рабочего стола ОС необходимо при графическом входе в ОС установить тип сессии «Десктоп».

Рабочий стол также запускается в режимах, оптимизированных для работы на устройствах с сенсорными экранами: в планшетном режиме (тип сессии «Планшетный») и в режиме для мобильных устройств (тип сессии «Мобильный»).

По умолчанию для входа в систему установлен тип сессии, с которым осуществлялся вход последний раз.

В графическую подсистему встроена мандатная защита. В области уведомлений (системном трее) панели задач располагается индикатор мандатного уровня и мандатной категории, на котором в числовой форме и в виде цвета фона сообщается о величине уровня:

1) «Уровень 0» – голубой;
2) «Уровень 1» – желтый;
3) «Уровень 2» – оранжевый;
4) «Уровень 3» – темно-розовый;
5) «Уровень 4» – красный;
6) «Уровень 5» – коричневый;
7) «Уровень 6» – пурпурный;
8) «Уровень 7» – темно-фиолетовый.

Любое окно вновь запущенного приложения будет снабжено цветной рамкой, цвет которой будет совпадать с цветом индикатора.

При работе на разных мандатных уровнях и категориях пользователю следует учитывать, что ОС формально рассматривает одного и того же пользователя, но с различными мандатными уровнями, как разных пользователей и создает для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается.

Рабочий стол Fly предоставляет пользователю:

– графический вход, позволяющий входить в локальную или удаленную систему и запускать графические приложения на заданных мандатных уровнях;

– рабочий стол для размещения элементов графического интерфейса;

– значки на рабочем столе, представляющие как файлы и/или каталоги, так и ярлыки для программ, устройств, ссылок на файлы, каталоги и/или адреса в сети;

– панель задач, содержащую: кнопку меню «Пуск», панель быстрого запуска с кнопками управления окнами приложений, переключатель рабочих столов, панель переключения задач и область уведомлений со значками программ, использующих системные разделы;

– меню приложений (в виде меню-панели или классического меню), доступное через кнопку меню «Пуск» на панели задач;

– интегрированный менеджер рабочих столов, позволяющий размещать окна приложений в пространстве, превышающем размер видимой области экрана, оперативно управлять окнами приложений и навигацией рабочих столов, а также настраивать конфигурацию рабочих столов;

– механизм прямого переноса данных из меню «Пуск» на рабочий стол и на панель быстрого запуска, а также с рабочего стола на панель быстрого запуска;

– индикатор мандатного уровня (секретности) и мандатной категории;

– стандартное оформление окон приложений, дополненное цветовой индикацией мандатных уровней, и стандартные способы манипулирования окнами;

– высокую гибкость в настройке как внешнего вида, так и процесса функционирования рабочего стола, значков и окон приложений, панелей и их реквизитов;

– «горячие» клавиши, назначаемые и редактируемые с помощью специальной графической утилиты;

– средства для редактирования меню, доступного через кнопку меню «Пуск», и панели быстрого запуска, а также для создания ярлыков и коллекций ярлыков;

– набор утилит для администрирования как системы в целом, так и самого рабочего стола, в т. ч. для поддержки механизма мандатного управления доступом;

– набор приложений для повседневного использования (менеджер файлов, текстовый редактор и т. п.);

– переключение в планшетный режим.

Описание всех графических утилит и программ рабочего стола Fly, а также полное описание его режимов работы и предоставляемых возможностей также приведено в электронной справке.

Программа «Панель управления» позволяет централизовано использовать некоторые административные и пользовательские утилиты рабочего стола Fly, которые для удобства разделены на несколько категорий (рис. 3.3.)

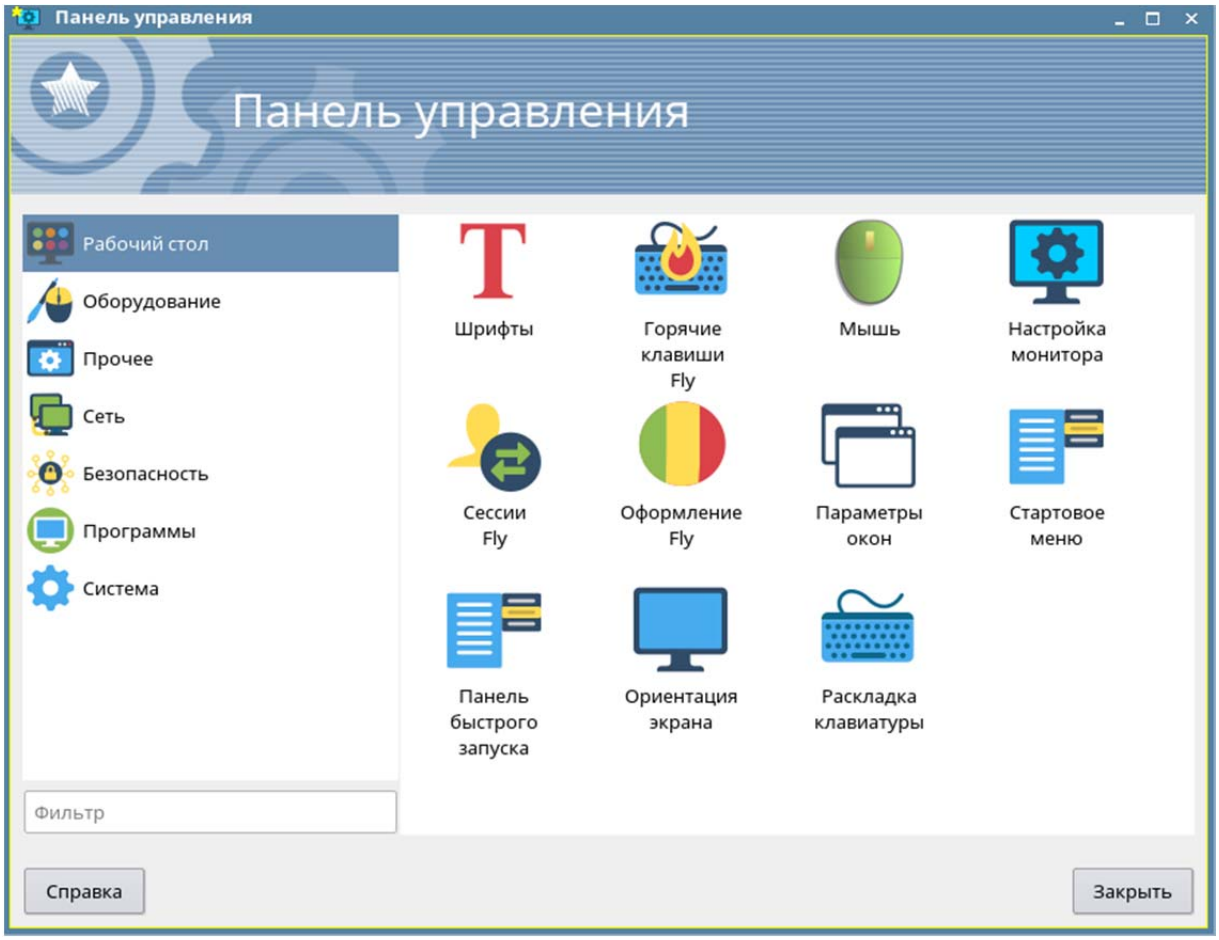

Рис. 3.3. Панель управления

Каждый пользователь в системе имеет возможность выполнить индивидуальные настройки своего рабочего стола (внешний вид, расположение элементов, особенности работы с клавиатурой и мышью). Однако часть настроек жестко задана администратором и недоступна обычному пользователю. Некоторые из возможностей настройки могут быть реализо-

ваны при использовании утилит настройки из меню «Пуск – Настройки – Панель управления» или непосредственно из меню «Пуск – Настройки».

Категория «Рабочий стол» программы «Панель управления» объединяет графические утилиты, которые могут быть применены для индивидуальной настройки рабочего стола. Перечень утилит, доступных пользователю, приведен в таблице 3.1, описание утилит приведено в электронной справке.

Таблица 3.1

Утилиты для настройки рабочего стола

Утилита	Описание
fly-admin-fonts «Шрифты»	Просмотр и импорт системных шрифтов
fly-admin-hotkeys «Горячие клавиши Fly»	Запуск редактора горячих клавиш для настройки соответствия между сочетаниями клавиш и действиями
fly-admin-mouse «Мышь»	Настройка кнопок мыши и скорости перемещения курсора
fly-admin-screen «Настройка монитора»	Настройка размера изображения, разрешения, частоты обновления и других параметров монитора
fly-admin-session «Сессии Fly»	Настройки для сессий рабочего стола
fly-admin-theme «Оформление Fly»	Настройка обоев, тем, шрифтов, экрана блокировки и других элементов рабочего стола
fly-admin-winprops «Параметры окон»	Настройка поведения и внешнего вида окон рабочего стола
fly-menuedit «Стартовое меню»	Настройка структуры меню «Пуск»
fly-menuedit «Панель быстрого запуска»	Добавление и удаление программ из панели запуска

Доступ к графическим программам и утилитам осуществляется из меню «Пуск». Программы сгруппированы по категориям в соответствии с их назначением.

3.3 Программа «Менеджер файлов»

Программа «Менеджер файлов» (утилита fly-fm) предназначена для просмотра папок рабочего стола и элементов файловой системы (ФС) и выполнения основных функций управления файлами. Позволяет подключать и отключать ФС носителей доступных устройств хранения данных, таких как локальные жесткие диски и их разделы, компакт- и DVD-диски, USB-накопители. Также позволяет обращаться к сетевым Samba-ресурсам, работать с архивами и выполнять кодирующее/раскодирующее преобразование (рис. 3.4).

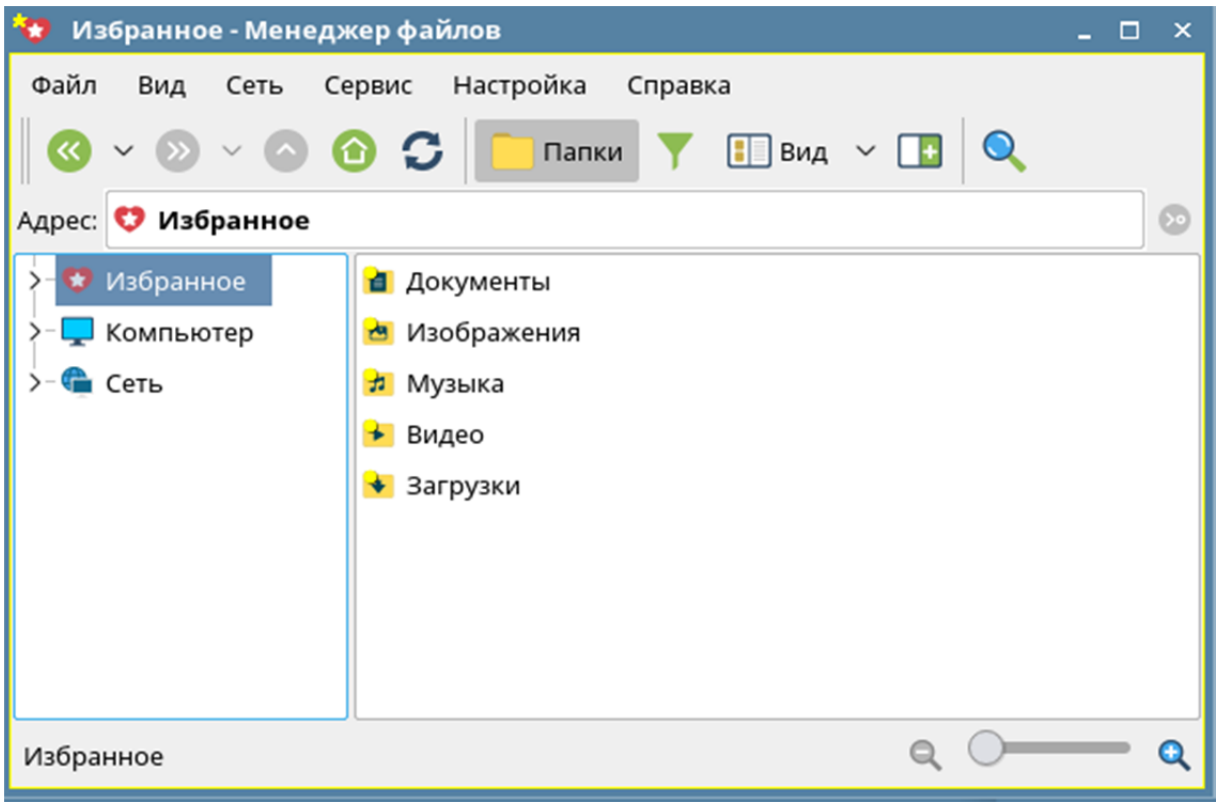

Рис. 3.4. Панель управления

В планшетном режиме программа по умолчанию запускается с установленными настройками, оптимизированными для работы на устройствах с сенсорными экранами. В частности, на панели просмотра слева от имени элемента отображаются значки для переключения флага выполнения групповых операций, при котором отображение графических элементов видоизменяется.

3.4. Раздел «Офис»

Большая часть работы, осуществляемая в ОВД, производится в офисных пакетах. Достойной заменой проприетарному пакету MS Office

является кроссплатформенный, свободно распространяемый офисный пакет с открытым исходным кодом офисный пакет Libreoffice.

LibreOffice содержит инструменты для решения офисных задач, например, таких как: написание текстов, работа с электронными таблицами, создание графических объектов и презентаций.

LibreOffice предназначен для обработки следующих видов документов:

1) тексты с профессиональной разметкой, включающей встроенные объекты, формы, развитую систему ссылок, сносок, правок и т. п.;

2) электронные таблицы, в том числе сопряженные с БД и автоматизацией на языках Basic, Java, Python, C/C++;

3) презентации с возможностью экспорта в форматы PDF, SWF, HTML;

4) деловая графика с возможностью импорта и экспорта графики во все популярные векторные (SVG, WMF, EMF и т. д.) и растровые (BMP, PNG, TIFF, GIF, JPEG и т. д.) форматы хранения изображений;

5) математические формулы с языком описания, диаграммы и БД. LibreOffice состоит из шести компонентов;

6) Текст LibreOffice – текстовый редактор и редактор web-страниц Writer;

7) Таблица LibreOffice – редактор электронных таблиц Calc;

8) Презентация LibreOffice – средство создания и демонстрации презентации Impress;

9) Рисунок LibreOffice – векторный редактор Draw;

10) База данных LibreOffice – система управления базами данных Base;

11) Математика LibreOffice – редактор Math для создания и редактирования математических формул.

Таким образом, все наиболее применяемые программы из состава пакета MS Office имеют аналогичные по функционалу программы в Libreoffice.

Первое и самое главное отличие MS Office и LibreOffice в архитектуре программ. Если MS – набор отдельных программ, то LibreOffice – единый организм с несколькими интерфейсами управления. При этом установленный LibreOffice занимает в 2-3 раза меньше места на жестком диске.

Существенное повышение эффективности работы в LibreOffice позволяет использование горячих клавиш:

– Ctrl+Q – выход	– Ctrl+K – вставка гиперссылки
– Ctrl+W – закрыть текущий документ	– Ctrl+L – выравнивание по левому краю
– Ctrl+E – выровнять текст по центру	– Ctrl+Z – отменить действие

– Ctrl+Shift+E – запись изменений в документе – Ctrl+R – выровнять текст по правому краю – Ctrl+Shift+R – показать/скрыть линейку – Ctrl+Y – вернуть отмененное действие – Ctrl+Shift-Y – повторить последнее действие (или продублировать введенное слово). – Ctrl+U – подчеркивание – Ctrl+I – курсив – Ctrl+O – открыть файл – Ctrl+Shift+O – просмотр печати – Ctrl+P – печать документа – Ctrl+Shift+P – верхний индекс – Ctrl+A – выделить весь текст – Ctrl+S – сохранить – Ctrl+D – двойное подчеркивание – Ctrl+Shift+S – сохранить как – Ctrl+F – поиск – Ctrl+H – замена – Ctrl+J – выравнивание по ширине – Ctrl+Shift+J – полноэкранный режим	– Ctrl+X – вырезать – Ctrl+C – копировать – Ctrl+Shift+C – вставить как – Ctrl+Alt+C – вставить примечание/комментарий – Ctrl+V – вставить – Ctrl+Shift+V – вставить как – Ctrl+Shift+Alt+V – вставить неформатированный текст – Ctrl+B – полужирный шрифт – Ctrl+Shift+B – нижний индекс – Ctrl+N – новый документ – Ctrl+M – отмена форматирования – Ctrl+[0-5] – стили текста – Alt+Shift+F8 – режим блочного/обычного выделения – Ctrl+F3 – редактор автотекста – Shift+F3 – переключение регистра текста (заглавные/прописные) – F4 – источники данных – F5 – навигатор документа – F7 – правописание – F11 – выбор стилей – F12 – нумерованный список – Ctrl+F12 – вставить таблицу

Для вычисления непосредственно в документе и в таблицах достаточно нажать клавишу F2 и ввести выражение для вычисления и после нажатия «Enter» результат будет отображен. Двойной клик на результате применяется для изменения формулы.

В таблице – в ячейке набрав «=» после чего таблица будет работать в режиме считающей ячейки – появляется возможность набора формул. Редактирование осуществляется также по нажатию клавиши F2.

Сохранение в форматах Jpeg/PNG/PDF/MediaWiki через меню «Экспорт» (бывает полезно при склейке сканов).

Открытие файла независимо от формата. Через меню «Открыть» можно открывать любой поддерживаемый файл. То есть из Writer(Word) можно открыть файл Calc(Excel) и он нормально откроется в Calc.

Возможно открытие и редактирование файлов формата PDF (схема работы такая же, как и с обычным текстовым файлом).

В LibreOffice содержится Меню оперативного редактирования таблиц. Окно с оперативными функциями по работе с таблицами (вставка/удаление/выделение ячеек/строк/столбцов) отображается, пока курсор находится в таблице.

Возможна массовая вставка строк и столбцов в таблицу через меню правой кнопки мыши (строка/столбец – вставить).

Допускается смена регистра через меню правой кнопки мыши и по комбинации клавиш Shift+F3.

Кнопка Insert переключает режимы редактирования текста «добавление»/«Замена». Эта функция также содержится в MS Office.

Замена абзацев местами можно произвести комбинацией клавиш Ctrl+Alt+Вверх.

Таким образом, можно сделать вывод, что пакет свободно распространяемого и открытым исходным кодом LibreOffice представляет собой практически полноценную замену проприетарному MS Office. Трудности перехода на данное программное обеспечение могут вызвать небольшие различия в интерфейсе программ и различной реализацией одних и тех же функций.

Вопросы для самоподготовки

1. Как начать и завершить работу в операционной системе Astra Linux CE?
2. Какие компоненты входят в рабочий стол Astra Linux и как ими пользоваться?
3. Как использовать программу «Менеджер файлов» и какие функции она предоставляет?
4. Какие программы входят в раздел «Офис» и для чего их можно использовать?

ЗАКЛЮЧЕНИЕ

Использование телекоммуникационных технологий в профессиональной деятельности ОВД реализовано на основе Единой системы информационно-аналитического обеспечения деятельности МВД России. Данная система позволяет создать единое информационное пространство для всей структуры МВД России, максимально оптимизировать служебную деятельность практически каждого сотрудника ОВД, незамедлительно получать необходимую информацию на всех уровнях управления, качественно улучшить информационное взаимодействие ОВД в рамках существования общегосударственной информационно-телекоммуникационной системы.

Министерство внутренних дел Российской Федерации в начале 2020 года начало масштабную программу замены зарубежного проприетарного системного программного обеспечения корпорации MS Windows на отечественную операционную систему «Astra Linux». Одновременно началась реализация программы обучения пользователей и системных администраторов работе с данной операционной системой.

Операционная система «Astra Linux» является производной распространяемых под свободной лицензией дистрибутива Debian. Анализ реестра российского программного обеспечения показывает, что практически все операционные системы, большая часть офисных программ и системы управления базами данных берут за основу свободное программное обемпечение с открытым исходным кодом. Данный подход представляется разумным, однако даже эта категория программного обеспечения не всегда является независимой от западных компаний, которые осуществляют финансовую и техническую поддержку. Ввиду этого для ответственных информационных систем необходима тщательная проверка и верификация кода, которая была осуществлена при разработке с привлечением Академии наук Российской Федерации, ФСБ России и ФСТЭК России.

Для успешной работы в современной информационной среде от пользователей требуется не только знание интерфейсов программного обеспечения, но и понимание механизмов информационного обмена и взаимодействия их между собой, умение выявлять и исправлять ошибки в информационных базах. Систематизация понятий в этих сферах позволяет не только свободно ориентироваться в информационных системах, но и быть готовым к их изменениям.

Таким образом, данное учебное пособие позволит курсантам и слушателям, а также практическим работникам подразделений МВД России получить необходимые знания для эффективного выполнения профессиональных задач с использованием современных информационных технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Нормативные правовые акты

1. **Российская Федерация. Законы.** Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г.: (ред. 01.07.2020). – Текст : электронный// Официальный интернет-портал правовой информации: [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 22.03.2023).

2. **Российская Федерация. Законы.** О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 29.12.2022) // Собрание законодательства Российской Федерации. – 2011. – № 7. – Ст. 900. – Текст : непосредственный.

3. **Российская Федерация. Законы.** Об образовании в Российской Федерации : Федеральный закон от 21 декабря 2012 г. № 273-ФЗ. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 22.03.2023).

4. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 22.03.2023).

5. О безопасности : Федеральный закон от 28 декабря 2010 г. № 390-ФЗ. – Текст : электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 22.03.2023).

6. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от декабря 2016 г. № 646. – Текст : электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 22.03.2023).

7. Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации : приказ МВД России от 20 июня 2012 г. № 615. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 20.02.2023).

8. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года : приказ МВД России от 14 марта 2012г. № 169 – URL: http://www.consultant.ru (дата обращения: 20.02.2023). – Текст : электронный.

9. Об утверждении Правил организации доступа к информационно-телекоммуникационной сети «Интернет» в органах внутренних дел Российской Федерации : приказ МВД России от 24 декабря 2015 г.

№ 1228. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 20.02.2023).

10. Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации : приказ МВД России от 23 сентября 2015 г. № 926. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 20.02.2023).

2. Основная литература

1. **Внуков, А. А.** Защита информации : учебное пособие для вузов / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2020. – 161 с. – (Высшее образование). – ISBN 978-5-534-07248-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/422772 (дата обращения: 22.03.2023).

2. **Гостев, И. М.** Операционные системы : учебник и практикум для вузов / И. М. Гостев. – 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2023. – 164 с. – (Высшее образование). – ISBN 978-5-534-04520-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/512144 (дата обращения: 22.03.2023).

3. **Дрёмова, Ю. Г.** Национальные инновационные системы : учебное пособие для вузов / Ю. Г. Дрёмова. – Москва : Издательство Юрайт, 2023. – 180 с. – (Высшее образование). – ISBN 978-5-534-15224-1. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/520392 (дата обращения: 22.03.2023)

4. **Запечников, С. В.** Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Высшее образование). – ISBN 978-5-534-02574-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/433133 (дата обращения: 22.03.2023).

5. **Казарин, О. В.** Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2019. – 342 с. – (Бакалавр и магистр. Модуль). – ISBN 978-5-534-05142-1. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/441287 (дата обращения: 22.03.2023).

6. **Нестеров, С. А.** Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. – Москва : Издательство Юрайт, 2019. – 321 с. – (Профессиональное образование). – ISBN 978-5-534-07979-1. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/442312 (дата обращения: 22.03.2023).

7. **Щеглов, А. Ю.** Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/433715 (дата обращения: 22.03.2023).

Учебное издание

Антонов Вячеслав Викторович
(доктор технических наук, доцент)
Гурьянова Венера Рафисовна
(кандидат физико-математических наук, доцент)
Тугузбаев Гаяз Ахтямович
(б/с, б/з)

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Редактор *Е. А. Ермолаева*

Подписано в печать: 23.06.2023	Выход в свет: 29.06.2023
Гарнитура Times	Формат 60x84 1/16
Уч.-изд. л. 2,8	Усл. печ. л. 3
Тираж 50 экз.	Заказ № 29

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2