МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ
ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

К. М. Бондарь, В. С. Дунин,
А. В. Рыбак, П. Б. Скрипко

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В УПРАВЛЕНИИ ДЕЯТЕЛЬНОСТЬЮ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Учебно-практическое пособие

Допущено Министерством внутренних дел Российской Федерации
в качестве учебно-практического пособия для курсантов
и слушателей образовательных организаций системы МВД России,
сотрудников органов внутренних дел Российской Федерации

Москва
2018

Рецензенты:
Е. М. Шпагина (Московский университет МВД России имени В. Я. Кикотя);
Д. В. Столбов (Департамент информационных технологий, связи и защиты информации МВД России);
А. Б. Сизоненко, кандидат технических наук, доцент (Краснодарский университет МВД России);
О. И. Бокова, доктор технических наук, профессор (Воронежский институт МВД России);
Ю. Э. Голодков, кандидат технических наук, доцент (Восточно-Сибирский институт МВД России)

Авторский коллектив:
К. М. Бондарь, кандидат технических наук, доцент (гл. 1);
В. С. Дунин, кандидат технических наук (гл. 2, 3);
А. В. Рыбак, кандидат технических наук, доцент (гл. 4);
П. Б. Скрипко, кандидат технических наук, доцент (гл. 1, 3)

Применение современных инфокоммуникационных технологий в управлении деятельностью подразделений органов внутренних дел: учеб.-практ. пособие / К. М. Бондарь [и др.]. – М.: ДГСК МВД России, 2018. – 192 с.

В учебно-практическом пособии рассматриваются современные инфокоммуникационные технологии, теоретические вопросы и практика инфокоммуникационного обеспечения деятельности подразделений органов внутренних дел, в частности базовые принципы функционирования информационно-телекоммуникационных сетей, разные подходы и примеры решения задач управления подразделениями с помощью интегрированной системы информационно-аналитического обеспечения, основы применения методов системной динамики для оценки эффективности деятельности следственных подразделений.

Пособие адресовано курсантам и слушателям, обучающимся по специальностям 40.05.01 «Правовое обеспечение национальной безопасности», 40.05.02 «Правоохранительная деятельность» и направлению подготовки 40.03.01 «Юриспруденция», преподавателям и адъюнктам образовательных организаций системы МВД России; сотрудникам органов внутренних дел, занимающимся управленческой деятельностью.

Оглавление

Введение

Актуальность инфокоммуникационных технологий (в самом общем виде — совмещающих информационные и телекоммуникационные технологии) в управленческой деятельности всего современного общества трудно переоценить. Они, по сути дела, обеспечивают поддержку управленческих методов и подходов, определяют возможности их реализации, обоснование и выработку эффективных решений.

В силу сказанного инфокоммуникационные технологии уже нашли широкое применение практически во всех сферах человеческой деятельности, социума, быта и не перестают быть актуальными. Они стали традиционной формой реализации управленческой деятельности и в органах внутренних дел[1], причем ведется значительная работа по внедрению в качестве типовых решений новых, перспективных технологий во все сферы оперативно-служебной деятельности.

В системе образовательных организаций высшего образования МВД России в основных образовательных программах по специальностям 40.05.01 «Правовое обеспечение национальной безопасности», 40.05.02 «Правоохранительная деятельность» и направлению подготовки 40.03.01 «Юриспруденция» нет дисциплины, полностью соответствующей применению инфокоммуникационных технологий в управленческой деятельности подразделений ОВД. Но данная проблематика рассматривается в рамках отдельных тем ряда учебных дисциплин, где изучается теория и отрабатываются навыки использования инфокоммуникационных технологий в управленческой деятельности ОВД, в частности:

1) «Информатика и информационные технологии в профессиональной деятельности» (темы: «Основы телекоммуникационных технологий и локальные сети в профессиональной деятельности», «Интернет-технологии», «Единая информационная телекоммуникационная система МВД России», «Использование компьютерной графики в профессиональной деятельности», «Аудио- и видеотехнологии в правоохранительной деятельности», «Информационные системы как центры сбора, хранения и обработки служебной информации в профессиональной деятельности», «Документальные и фактографические автоматизированные информационные системы в оперативно-разыскной и следственной деятельности», «Интеллектуальные информационные системы как системы поддержки принятия решения в профессиональной деятельности»). Рассматриваемым вопросам отводится 14 ч;

2) «Информационные технологии в юридической деятельности» (темы: «Интегрированная мультисервисная телекоммуникационная

[1] Далее используется сокращение ОВД.

сеть МВД России», «Технология работы со справочными правовыми системами», «Автоматизированное рабочее место специалиста»). Здесь инфокоммуникационные технологии изучаются в течение 4 ч;

3) «Основы управления в органах внутренних дел» (темы: «Выработка и реализация управленческих решений в органах внутренних дел», «Организация информационно-аналитической работы в органах внутренних дел», «Организационные проблемы кадрового обеспечения и научной организации труда в органах внутренних дел»). Современным компьютерным технологиям посвящено 8 ч;

4) «Специальная техника органов внутренних дел» (темы из раздела специальной техники общего назначения: «Технические средства и системы связи органов внутренних дел», «Комплексы технических средств органов внутренних дел»). В рамках изучаемых положений дисциплины 4 ч выделено на особенности применения информационных технологий;

5) «Основы информационной безопасности в органах внутренних дел» (тема «Защита информации в инфокоммуникационных системах»). Вопросам применения информационных технологий уделяется 2 ч;

6) «Правовая статистика» (темы: «Инструментарий статистического исследования», «Анализ, обобщение, интерпретация и представление статистических данных»). Рассматриваемым технологиям отводится 4 ч.

Выстраивая структуру учебно-практического пособия, авторы постарались комплексно и по возможности максимально охватить общую проблематику применительно к содержанию указанных дисциплин с учетом опыта их преподавания в Дальневосточном юридическом институте МВД России.

В частности, в основе пособия — прежде всего работы сотрудников кафедры информационного и технического обеспечения органов внутренних дел. За последние годы ими было подготовлено и издано 18 научных и учебно-методических работ для обеспечения рабочих программ дисциплин «Информатика и информационные технологии в профессиональной деятельности», «Информационные технологии в юридической деятельности», «Основы управления в органах внутренних дел», «Специальная техника органов внутренних дел», «Основы информационной безопасности в органах внутренних дел».

Еще одной особенностью, определившей целевую направленность и структуру учебно-практического пособия, стало то, что все практические занятия по указанной выше тематике проводятся в ДВЮИ МВД России в компьютерных классах и предполагают использование различных инфокоммуникационных технологий.

Охарактеризуем структурные составляющие пособия.

В главе 1 *«Информационные и телекоммуникационные технологии в информационно-аналитическом обеспечении управления деятельностью подразделений в органах внутренних дел»* в рамках основных положений информационного обеспечения управления рассматриваются представления об управленческой информации, ее свойствах и особенностях, приводятся этапы информационного обеспечения в соответствии со сложившейся практикой управленческой деятельности, раскрывается состав и классификация информации для обеспечения служебной деятельности ОВД. Говоря о современном состоянии и тенденциях развития информационных и телекоммуникационных технологий, значительное внимание уделяется единой системе информационно-аналитического обеспечения деятельности МВД России[1], ее архитектурным особенностям, эксплуатационным возможностям и внедрению. При этом особый акцент делается на решениях в части применения современных аналитических инструментов. Учитывая, что основу функционирования ИСОД МВД России составляют облачные информационные системы, дается их понятие, приводится классификация и требования, предъявляемые к ним. В качестве приоритетных решений, отражающих текущий уровень информационного обеспечения деятельности ОВД, рассматриваются системы видеонаблюдения и геоинформационные системы. Помимо описания принципов работы систем подобного класса приводятся конкретные примеры их применения в деятельности ОВД. Материал главы основывается на положениях, изложенных авторами в ряде работ [42; 49; 52; 54; 60; 61; 63; 72; 74].

В главе 2 *«Основы функционирования информационно-телекоммуникационных сетей в органах внутренних дел»* приводится понятийный аппарат сетевых технологий, в том числе базовая модель сетевого взаимодействия (OSI), сервисные возможности корпоративных сетей. Применительно к корпоративным сетям ОВД дается характеристика интегрированной мультисервисной телекоммуникационной сети МВД России[2], рассматривается состав и структура, функциональные возможности и направления дальнейшего развития ИМТС МВД России с учетом инфраструктурной поддержки ИСОД МВД России и облачной архитектуры информационных систем МВД России. В качестве одного из решений, основанных на согласованном применении современных инфокоммуникационных сетей в деятельности ОВД, представляется архитектура аппаратно-программного комплекса[3] «Безопас-

---

[1] Далее используется сокращение ИСОД МВД России.

[2] Далее используется сокращение ИМТС МВД России.

[3] Далее используется сокращение АПК.

ный город», приводятся принципы его построения, функциональные особенности, преимущества и перспективы развития. Положения этой главы являются результатами длительных исследований авторов в этой области и были отмечены в ряде публикаций [49; 51; 56—58; 60; 61; 63].

Глава 3 *«Решение задач управления деятельностью подразделений органов внутренних дел на базе интегрированной системы информационно-аналитического обеспечения»* ориентирована в основном на практические аспекты использования информационных и телекоммуникационных технологий в решении задач управления. С учетом современных особенностей аналитической работы в ОВД обосновывается актуальность применения систем поддержки принятия решений, основанных на методах интеллектуального анализа, описывается архитектура таких систем, приводится классификация, требования к ним и принципы их реализации. Рассматриваются аналитические системы построения деревьев решений (или правил if… then). В качестве иллюстрации технологии поддержки решения задач управления приведен пример обеспечения охраны общественного порядка при проведении массовых мероприятий.

Интеграция систем данного класса с аппаратно-программными средствами многофункционального информационно-аналитического центра ДВЮИ МВД России, состав, структура и функции которого рассматриваются в данной работе, обеспечивает совершенно новый уровень решения учебных задач. К таковым относится изучение возможностей применения инфокоммуникационных технологий в цикле управления деятельностью подразделений, который включает сбор, обработку и анализ информации об оперативной обстановке на территории обслуживания, выработку и анализ вариантов решений, планирование и расстановку сил и средств, контроль и оперативное управление проведением различных мероприятий. Об этом авторы писали в ряде работ [51; 52; 54; 72; 74].

В главе 4 *«Применение методов математического моделирования для оценки эффективности деятельности следственных подразделений»* рассматривается новый подход в оценке эффективности деятельности территориальных подразделений на примере следственных отделов.

Этот подход основывается на динамическом равновесии элементов системы «преступность — ресурсы» — весьма важном понятии с точки зрения разработки математических моделей для оценки эффективности работы ОВД. В основе моделирования используется нелинейная зависимость показателя раскрытых и расследованных преступлений от таких параметров, как интенсивность зарегистрированной преступ-

ности (число преступлений, соотнесенное с численностью населения) и кадровая обеспеченность (количество сотрудников территориальных органов МВД России, соотнесенное с численностью населения). Это позволяет рассчитать нормативные показатели эффективности деятельности подразделений (в частности следственных), зависящие от сложившейся в отчетный период оперативной обстановки, нагрузки и трудоемкости раскрытия преступлений. Эффективность деятельности подразделений оценивается на основе сравнения итоговых и нормативных показателей.

Безусловно, предложенная технология является лишь первым шагом по изменению подхода к оценке деятельности территориальных подразделений ОВД. Применение математической модели системной динамики, отражающей некую объективную взаимосвязь между параметрами оперативной обстановки, позволит оценить потенциальные ресурсы подразделений, их предельные возможности в раскрытии и расследовании преступлений и в итоге избавиться от пресловутой «палочной системы». Работа над указанной проблематикой также ранее проводилась авторами [42; 54; 72].

ГЛАВА 1. ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОМ ОБЕСПЕЧЕНИИ УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПОДРАЗДЕЛЕНИЙ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

1.1. Основные положения информационного обеспечения управления деятельностью подразделений в органах внутренних дел

Особенности современного управления в разных сферах свидетельствуют о том, что этот процесс невозможен без информационных технологий[1]. По сути дела, сейчас мы наблюдаем повсеместное применение компьютерной техники, прежде всего это касается основных направлений управленческой деятельности: аналитической работы, планирования действий, контроля и оценки результатов и т.д. Вместе с тем в области принятия решений требуется переход на качественно новый уровень. Это обусловлено динамичными процессами, протекающими в обществе.

К такому уровню относят: учет внешних и внутренних параметров в как можно большем количестве, прогноз развития ситуации, мгновенное принятие решений и т.д. Классические в управлении факторы, такие как интуиция, личный опыт руководителя, объемы имеющихся ресурсов, не всегда достаточны для решения такого рода задач.

Указанное обстоятельство в полной мере относится и к управленческой деятельности ОВД. Здесь в условиях неопределенности и риска обоснование и принятие эффективного управленческого решения требует учитывать и держать под контролем различные аспекты правоохранительной деятельности: функционирование уголовного розыска, следственные действия, работу дежурной части, патрулирование территории и т.д.

Одним из наиболее продуктивных подходов, позволяющим в значительной мере преодолеть указанные затруднения, является более

[1] Далее используется сокращение ИТ.

широкое применение ИТ. Оно требует определенной аппаратно-программной оснащенности и эффективной организации информационного обеспечения управленческой деятельности.

Понятие и характеристики управленческой информации. Слово «информация» произошло от латинского *information* — изложение, разъяснение какого-либо факта, события, явления. В широком смысле *информация* — это сведения о той или иной стороне материального мира и происходящих в нем процессах. При изучении информации учитываются закономерности ее создания, преобразования и использования в различных сферах человеческой деятельности.

Основу разделения информации составляет ее предметное содержание. Она очень разнообразна, и в зависимости от направления использования в человеческой деятельности можно назвать следующие виды: научная, техническая, производственная, управленческая, экономическая, социальная, правовая и т. п. При этом для каждого вида выделяют специфические технологии обработки, смысловую ценность, формы представления и отображения, характеристики точности, достоверности, оперативности отражения фактов, явлений, процессов.

Среди *важнейших свойств управленческой информации* отмечаются следующие:

- достоверность и полнота;
- ценность и актуальность;
- ясность и понятность.

Достоверной считается информация, не искажающая истинное положение дел. Недостоверная информация создает основу неправильного понимания ситуации или принятия неправильных решений.

Свойство *полноты* информации определяется достаточностью ее для понимания и принятия решений. Сдерживание в принятии решений или их принятие с возможными ошибками прежде всего связано с неполнотой информации.

В зависимости от классов решаемых задач формируется понятие *ценности* информации.

При работе в постоянно изменяющихся условиях важное значение имеет свойство ее *актуальности*.

Ясная и понятная информация выражается языком, на котором говорят те, кому она предназначена. Иначе она может потерять ценность и актуальность и стать практически бесполезной.

В современном обществе информация выступает одним из главных ресурсов жизнедеятельности, который содержится в больших и сложных человеко-машинных информационных системах. Важной особенностью при этом является то, что информация не убывает со временем, в отличие от других природных ресурсов, а, наоборот, ее объем посто-

янно увеличивается. Это создает условия для накопления опыта, способствуя выработке обоснованных управленческих решений.

Управленческая информация — та, которая обслуживает и обеспечивает решение задач организационного управления. К ней относятся разнообразные сведения экономического, технологического, социального, юридического, демографического и другого содержания. Еще раз подчеркнем ее важность как одного из ведущих ресурсов наряду с материальными, трудовыми, финансовыми [63].

В деятельности ОВД в технологии обработки управленческой информации первичные сведения о состоянии правопорядка, зарегистрированных преступлениях, социально-демографических условиях являются, по сути, предметами труда. Результатная информация в виде отчетов, справок, вариантов решений играет роль при анализе и принятии управленческих решений.

Информация, используемая в деятельности ОВД, — это совокупность различных сведений нормативного, учетного, документального характера. Они задействованы в таких информационных процессах, как фиксация, передача, обработка, хранение и применение в процессе планирования, учета, контроля, анализа на всех уровнях управления подразделениями. В составе обозначенного вида информации содержатся данные о состоянии правопорядка на территории обслуживания, кадровых, материально-технических и финансовых ресурсах, а также данные о состоянии объектов управления на определенный момент [72].

Функциональный аспект ИТ управления. Территориальные подразделения ОВД являются сложными системами. В их составе большое число элементов для выполнения специальных и управленческих функций. Указанные объекты представлены многоуровневой структурой, а также имеют обширные внешние и внутренние информационные связи. Обеспечение нормального функционирования сложных систем при взаимодействии разнообразных ресурсов и групп людей требует управления как отдельными элементами, так и системами в целом.

Управление ориентировано на достижение стоящих перед каждой системой целей, на создание условий их выполнения. К таким *условиям* можно отнести обеспечение устойчивости определенной структуры, ее эффективного функционирования; поддержание установленного режима деятельности; сохранение или формирование у системы тех или иных качественных особенностей; выполнение заданных программ работы.

Управление, таким образом, является целенаправленной деятельностью и в конкретных ситуациях осуществляется на основе принципов принятия решений. В реальных социально-экономических системах,

как правило, выделяется не одна, а несколько целей, которые упорядочиваются по их важности и с учетом заданных приоритетов.

Накопленная и функционирующая в системе управления информация, в том числе поступающая из внешней среды по каналам прямой и обратной связи, формирует соответствующие управляющие воздействия.

Исходя из сказанного, подчеркнем информационный характер любого управления. Действительно, *важнейшей функцией любой системы управления является получение информации*. На ее основе выполняются процедуры по обработке с помощью заданных алгоритмов и программ, формируются управленческие решения, определяющие дальнейшее поведение системы.

В физическом плане информация фиксируется и передается на материальных носителях. Поэтому требуются определенные действия человека по восприятию, сбору информации, ее записи, передаче, преобразованию, обработке, хранению, поиску и выдаче с помощью компьютеров и других технических средств. Указанные действия входят в технологию управления как составные элементы и в итоге обеспечивают нормальное протекание информационного процесса.

Углубленное изучение теории и практики протекания информационных процессов обусловлено применением технических средств для получения информации в ходе наблюдения за деятельностью объекта, сбора данных, их регистрации, передачи по телекоммуникационным каналам. В этом смысле информатика устанавливает законы преобразования информации в условиях функционирования автоматизированных систем, разрабатывает методы ее алгоритмизации, формирования языковых средств общения человека и компьютера.

В сложных социально-экономических системах выработка эффективных управленческих решений требует, наряду с созданием соответствующих алгоритмов управления, переработки значительных объемов разнообразной информации. Поэтому в определенный период была обоснована необходимость разработки автоматизированных информационных систем[1] управления.

В самом общем виде *автоматизация* — это комплекс действий и мероприятий технического, организационного и экономического характера, позволяющих снизить или полностью исключить непосредственное участие человека в выполнении той или иной функции производственного процесса, процесса управления. Тогда можно привести следующее определение АИС.

---

[1] Далее используется сокращение АИС.

АИС — человеко-машинная система с автоматизированной технологией получения результатной информации, необходимой для информационного обслуживания специалистов и оптимизации процесса управления в различных сферах человеческой деятельности.

Данные системы позволяют обеспечивать многовариантность расчетов, принимать рациональные управленческие решения, в том числе в режиме реального времени, организовывать комплексный учет и анализ, поддерживать достоверность и оперативность информации, получаемой и используемой в управлении, и т. д.

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).

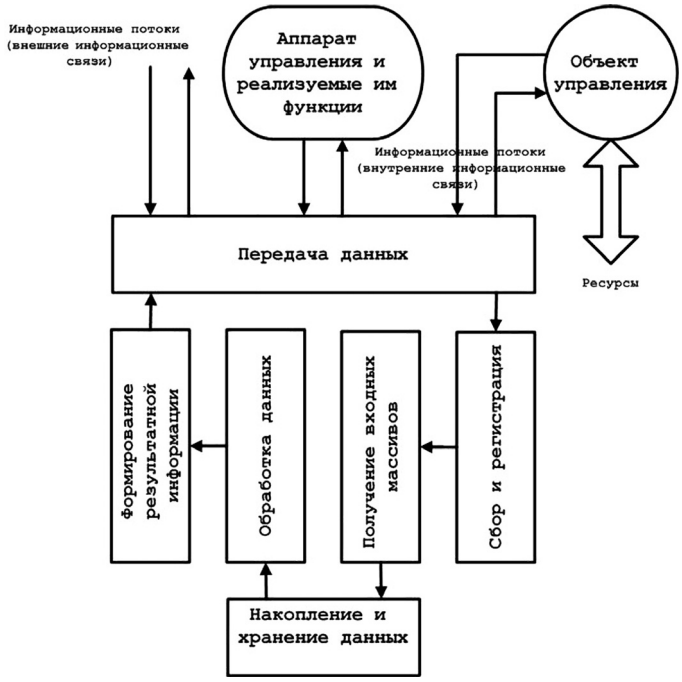


Рис. 1.1. Функциональная структура АИС

Обозначим эти элементы АИС в составе системы управления: аппарат управления, информация, методы и средства ее обработки. Из этой структуры выделим аппарат управления. Тогда оставшиеся элементы, технологически тесно взаимосвязанные, при условии единого системного использования программно-математических методов и технических средств управления образуют *автоматизированную информационную технологию* обработки данных.

Данная технология также представляет собой человеко-машинную систему, в рамках которой реализуется информационная модель, формализующая процессы обработки данных в конкретной предметной области. Кроме этого, посредством автоматизированной информационной технологии устанавливается прямая и обратная информационная связь между объектом управления и аппаратом управления, она также вводит в систему и выводит из нее потоки внешних информационных связей.

Исходя из функциональных направлений деятельности автоматизированной информационной технологии также определяются составляющие ее структуры. В качестве основ для выполнения необходимых функций она включает следующие процедуры: сбор и регистрацию данных; подготовку информационных массивов; обработку, накопление и хранение данных; формирование результатной информации; передачу данных от источников возникновения к месту обработки, а результатов (расчетов) — к потребителям информации для принятия управленческих решений [63].

Как и в других случаях, для правовой, криминологической и статистической информации обычно осуществляются все процедуры преобразования. Хотя в ряде ситуаций некоторые процедуры могут отсутствовать. Бывает различной также и последовательность их выполнения, в том числе возможны повторы отдельных процедур.

Именно объект управления, ведущий автоматизированную обработку информации, во многом определяет состав процедур преобразования и особенности их выполнения.

Рассмотрим **особенности выполнения основных процедур преобразования информации в управленческой деятельности ОВД.**

1. *Сбор и регистрация информации* для различных организационных объектов происходят по-разному. Нам представляется, что наиболее сложна эта процедура в автоматизированных управленческих процессах штабов ОВД, где производятся сбор и регистрация первичной учетной информации, отражающей состояние деятельности конкретного подразделения и криминологической обстановки на его территории. Но следует отметить, что не менее сложна эта процедура и в дежурных частях ОВД, подразделениях тылового, финансового

и документационного обеспечения, где оформляются, передаются различные документы.

При этом *имеет значение достоверность, полнота и своевременность первичной информации*. В ОВД сбор и регистрация информации происходят при регистрации заявлений и сообщений о правонарушениях, приеме информации от других подразделений и т. п. В отдельных случаях учетные данные формируются на рабочих местах сотрудников при подсчете количества подозреваемых, оценке нанесенного материального ущерба. Измерение, подсчет, выяснение временны́х и количественных характеристик работы отдельных исполнителей производятся в процессе сбора фактической информации.

Сбор информации, как правило, сопровождается *фиксацией на материальном носителе* (в документе, журнале), вводом в компьютер (в виде файлов баз данных, документов других информационных форматов). Запись в первичные документы пока в основном осуществляется вручную. Это определяет наибольшую трудоемкость процедуры сбора и регистрации, а процесс автоматизации документооборота по-прежнему делает весьма актуальным. Основу реализации функций автоматизации управления составляет использование технических средств сбора и регистрации информации, совмещающих операции количественного измерения, регистрации, накопления и передачи информации по каналам связи, ввода непосредственно в компьютер для формирования нужных документов или накопления в системе полученных данных.

2. Для *передачи информации* применяют различные способы: доставка с помощью курьерской службы, пересылка по почте, дистанционная передача по телекоммуникационным каналам и др. Конечно, *дистанционная передача по телекоммуникационным каналам* принципиально сокращает время передачи данных. Но для ее реализации необходимы специальные технологии, что повышает сложность и стоимость процесса передачи. На практике в ОВД *предпочтительным вариантом является использование технических средств сбора и регистрации информации*, которые автоматически получают ее с установленных в точках сбора данных датчиков, передают в компьютер для последующей обработки, что повышает достоверность информации и снижает трудоемкость процесса. В качестве примера можно привести подсистему видеонаблюдения в составе АПК «Безопасный город» (см. о нем в подразд. 2.3).

Надо отметить, что дистанционно может передаваться и первичная информация с мест ее возникновения, и результатная. Результатная информация фиксируется различными устройствами: мониторами, информационными панелями, печатающими устройствами. Поступает

информация по телекоммуникационным каналам в центр обработки, как правило, при непосредственном вводе в компьютер при помощи специальных программных и аппаратных средств.

Рассматриваемый вариант передачи информации с помощью современных телекоммуникационных средств постоянно развивается и совершенствуется. Этот способ особенно важен в многоуровневых внутриведомственных системах, таких, например, как МВД России. Здесь дистанционная передача значительно ускоряет попадание информации с одного уровня управления на другой и сокращает общее время обработки данных.

3. *Получение входных массивов* предусматривает, как правило, обязательное преобразование исходных данных в форму и вид, пригодный для ввода в компьютер, а также для последующей записи на машинные носители или передачи по телекоммуникационным каналам. Такое преобразование называют машинным кодированием.

Машинное кодирование — процесс перевода обычных для человека видов информации в форму машинного представления (записи) для последующей фиксации на машинных носителях в компьютерных кодах. Данный процесс происходит путем переноса данных первичных документов на так называемые машинные носители, информация с которых затем вводится в компьютер для обработки. Запись информации на машинные носители может быть как самостоятельной процедурой, так и результатом обработки.

4. *Хранение и накопление информации* обусловлено необходимостью ее многократного использования, для чего требуется наличие условно постоянной, справочной и других видов информации и комплектация первичных данных до их обработки. Данная процедура преобразования информации выполняется в информационных базах, на машинных носителях в виде информационных массивов, где данные располагаются по порядку, установленному в процессе проектирования предметной базы данных.

С процедурой хранения и накопления непосредственно связан поиск данных. Он представляет собой выборку из хранимой информации нужных данных, включая информацию, подлежащую корректировке или замене. Поиск информации выполняется автоматически на основе составленного пользователем или компьютером запроса информации и формы ее представления.

5. *Обработка информации* в деятельности ОВД производится на компьютере, как правило, децентрализованно, в местах возникновения первичной информации. Там организуются автоматизированные рабочие места специалистов той или иной службы (отраслевого подразделения, дежурной части, отдела материально-технического снаб-

жения, штаба, отдела делопроизводства и режима и т.п.). Но имеется возможность проведения обработки не только автономно, но и в вычислительных сетях с помощью набора программных средств и информационных массивов для решения функциональных задач.

В соответствии с алгоритмами, реализованными в программах, на компьютере формируются результатные сводки, которые печатаются на бумаге или отображаются на экране. Кроме печати может быть запущена процедура тиражирования или электронной рассылки в случаях, если документ с результатной информацией необходим нескольким пользователям.

6. *Принятие решения* в автоматизированной системе организационного управления, как правило, осуществляется специалистом с применением или без применения технических средств. Во втором случае требуется тщательный анализ результатной информации. Осложняющим условием выполнения задачи принятия решения является то, что специалисту приходится выбирать из множества допустимых наиболее приемлемое, сводящее к минимуму потери ресурсов (временны́х, трудовых, материальных и т.д.). Применение компьютеров при этом повышает качество анализа обрабатываемых сведений, а также обеспечивает постепенный переход к автоматизации выработки оптимального решения в процессе диалога пользователя с вычислительной системой. В частности, в большей мере этому способствует использование современных технологий экспертных систем и систем поддержки принятия решений (см. о них в подразд. 3.1).

Компоненты информационной системы ОВД. В деятельности ОВД удельный вес информационных функций значителен на всех уровнях работы — от принятия общих управленческих решений до конкретных действий по раскрытию, расследованию преступлений и профилактике правонарушений. Еще одной важной особенностью является жесткая необходимость документирования характеристик объектов и субъектов правонарушения, а также большинства оперативно-разыскных, следственных и иных действий сотрудников ОВД. Иными словами, деятельность ОВД, в том числе управленческая, имеет в значительной степени информационный характер и составляет работу с информацией [72].

Управленческая информация ОВД — это любые сведения (сообщения, данные), которые использовались, используются либо могут использоваться при осуществлении основных функций управления в ОВД (учет, анализ, прогнозирование, планирование, принятие управленческого решения, организация, регулирование и контроль).

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:

1) внешние условия, факторы среды функционирования;

2) 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 винно-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.

Следует подчеркнуть, что, несмотря на значительную распространенность, *классификация информационных систем условна*. Чаще всего эти системы делят по служебной направленности обрабатываемой информации: оперативно-разыскные, разыскные, оперативно-справочные, профилактические, криминалистические, кадровые, бухгалтерские, медицинские и т.д. Встречаются и иные формы информационных систем. Так, в практике ОВД получила распространение такая разновидность, как учеты.

Учеты — это особая форма организации информационных систем, ориентированная на сбор и упорядоченное накопление информации в целях ее многократного использования.

Ведение учета — это обеспечение функционирования всех информационных процессов в подобной системе.

Объекты учета — это реальные объекты окружающей среды или так называемой предметной области, информация о которых подлежит накоплению в рамках того или иного учета (лица, события, явления, предметы, отдельные информационные сообщения, документы и т. д.).

В настоящее время вместе с понятием «информационная система» в деятельности ОВД нашел распространение термин «система информации». Кратко охарактеризуем его.

Система информации — совокупность видов управленческой информации, для которой определены состав и характеристики отдельных элементов информации, форма представления, а также регламент хранения и обмена данными.

Соотношение представленных понятий состоит в том, что *информационная система является частью системы информации*. Многие информационные системы, а не одна, применяются потому, что информация, используемая в ОВД, различается по содержанию, предназначению, методам, средствам сбора, передачи и обработки.

Для эффективного обеспечения управленческой деятельности в ОВД выделены *специальные информационные подразделения* с собственной структурой. К ним относятся учетные группы, главный информационный центр[1], информационные центры управлений и т. д.

Эти подразделения создают и обеспечивают совершенствование информационных систем для выполнения задач управления ОВД. В совокупности они реализуют функцию органа управления и составляют информационное обеспечение управления.

Информационное обеспечение управления предназначено для того, чтобы из всей совокупности информации с учетом общих ее источников, периодичности поступления отобрать только те сведения, которые необходимы и достаточны для выполнения управленческих функций.

Для более наглядного представления особенностей информационного обеспечения управленческой деятельности его можно представить в виде переходящих из одного в другой этапов деятельности соответствующих служб, отдельных сотрудников в целях оптимизации процесса. Эти этапы схематично могут выглядеть следующим образом (табл. 1.1).

[1] Далее используется сокращение ГИАЦ МВД России.

Таблица 1.1

Этапы информационного обеспечения управления деятельностью подразделений в органах внутренних дел

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

Таким образом, выполнение современных требований к управлению деятельностью в ОВД основано на более широком применении информационных и телекоммуникационных технологий, внедрении АИС, реализующих полный цикл обработки управленческой информации. Адекватное современным условиям управление невозможно без эффективной организации системы информационного обеспечения, к задачам которого наряду с реализацией оперативного доступа к информации относят анализ, прогнозирование и подготовку оптимальных решений.

1.2. Современное состояние и тенденции развития информационных технологий в органах внутренних дел

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»* [2, ст. 11].

В этих целях создан единый центр, осуществляющий координацию работ по продвижению ИТ в системе МВД России. Департамент ин-

формационных технологий, связи и защиты информации 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 последнее время были успешно осуществлены *мероприятия по созданию на принципиально новом техническом уровне ИСОД МВД России. Созданы системы централизованной обработки данных*[1], обеспечивающие вычислительными ресурсами информационные системы и прикладные сервисы ИСОД.

Сегодня силами Департамента информационных технологий, связи и защиты информации МВД России проводится сложный комплекс мероприятий по переводу работы всех подразделений МВД России по ключевым направлениям оперативно-служебной деятельности на всей территории страны на типовое унифицированное программное обеспечение. В рамках создания и эксплуатации ИСОД МВД России *предусматривается, что по всем базовым направлениям должны иметься типовые решения*. Например, все следственные подразделения, работающие на территориальном, региональном, межрегиональном и федеральном уровнях, должны использовать одно прикладное приложение. Особенности такого приложения — учет специфики решения соответствующих задач на каждом из уровней управления, а также обеспечение формирования единой базы данных.

В силу сказанного обратимся к краткому изложению **особенностей ИСОД МВД России** (более подробно эта система будет рассмотрена в подразд. 2.2), а также поясним **актуальность и практическую значимость ее создания и использования** в современный период и в ближайшей перспективе (рис. 1.2).

В ОВД за последние годы проведена значительная работа по развитию информационной инфраструктуры. Была *создана единая информационно-телекоммуникационная система органов внутренних дел* на основе ведомственной инфраструктуры и обеспечен базовый уровень технического оснащения подразделений ОВД. В дальнейшем в результате проведенных работ *появилась ИМТС МВД России* (см. о ней в подразд. 2.1), к которой подключили узлы связи подразделений системы МВД России.

Основной *причиной создания ИСОД МВД России* стало отсутствие единых архитектурных решений и системного подхода к внедрению автоматизированных систем. Имевшиеся до этого программные решения существовали параллельно — отдельно для службы полиции,

[1] Далее используется сокращение ЦОД.

Рис. 1.2. Развитие ИСОД МВД России

отдельно для уголовного розыска, отдельно для подразделений экономической безопасности и т. д. Каждое из них выполняло свои задачи. В то же время особенностью информационного обеспечения ОВД является то, что информация, которая требуется, например, конкретному подразделению полиции, необходима и другим структурам. Но оперативно получить ее из разных систем на одно рабочее место довольно сложно — из-за несовместимости форматов. Для использования сотрудниками ОВД разных систем приходилось устанавливать несколько компьютеров на одном рабочем месте.

Поэтому одной из первостепенных задач при создании ИСОД МВД России явилось «связывание» между собой всех существовавших на тот момент информационных систем.

Еще одной причиной, и не менее важной, было то, что информационные системы разрабатывались без учета современных тенденций: их использование предполагало установку программ непосредственно на рабочих местах пользователей и серверах локальных сетей, а также создание отдельных центров обработки данных на региональных уровнях. Это повлекло за собой высокую стоимость обслуживания, низкую надежность и недостаточную производительность систем.

В соответствии с отмеченными противоречиями ИСОД МВД России была представлена как совокупность всех используемых АИС об-

работки информации, АПК и комплексов программно-технических средств, а также систем связи и передачи данных, необходимых для эффективного обеспечения служебной деятельности. При ее создании ставилась цель решения задач автоматизации основных видов деятельности подразделений МВД России, организации централизованного хранения и обработки данных.

В итоге *для сотрудников всех подразделений ОВД ИСОД МВД России является единым источником информации*, обеспечивает организацию электронного взаимодействия между ними, разграниченного доступа к информационным ресурсам. Важной особенностью является и *предназначенность для повышения эффективности принимаемых решений* за счет улучшения качества подготавливаемых отчетов, основанных на актуальных и достоверных данных, обеспечения оперативного и своевременного анализа ключевых показателей деятельности МВД России. Еще один значимый результат состоит в более эффективном выполнении государственных функций и предоставлении государственных услуг за счет снижения времени и трудоемкости операций по обработке информации.

Обеспечение доступа сотрудников к компонентам ИСОД МВД России и работы с ними базируется на *полноценном ведомственном облаке*, представляющем территориально распределенную систему связанных между собой центров обработки данных. В этом облаке размещаются все базовые приложения и формируемые в них базы данных.

Функционирование такого ведомственного облака потребовало перестройки схемы организации ИМТС МВД России. В частности, все объекты МВД России напрямую подключаются к облаку с обеспечением необходимой скорости доступа к его сервисам. Скорость рассчитывается исходя из количества прикладных решений, имеющихся на конкретном объекте пользователей. В дальнейшем по понятным причинам ведется закрытие соответствующих каналов средствами шифрования, обеспечивающими необходимый уровень защиты передаваемых данных. Используются типовые программные решения и формируется единое хранилище данных на основе загрузки сведений из уже действующих информационных систем.

Важнейшим элементом инфраструктуры ИСОД МВД России является *система ЦОД*. Эта система создается на нескольких территориально удаленных площадках в целях обеспечения требуемого уровня показателей надежности и доступности информационно-телекоммуникационных услуг.

В технической архитектуре ЦОД применены как существующие, уже апробированные, технологии, так и перспективные. Развитие обеспечивается путем замены устаревающих компонентов на более со-

временные без кардинальной перестройки всей системы ЦОД. Кроме того, данная система предполагает инвариантность инфраструктуры для выполнения различных прикладных задач, а также возможность внедрения единой централизованной системы управления сетью и сетевой безопасностью.

Ключевым предложением является унификация решений и программно-технической платформы, обеспечение единой точки доступа к информационным системам и информационным ресурсам МВД России, а также разработка типового программно-технического решения по обеспечению основных направлений деятельности территориальных подразделений МВД России. Такой подход направлен на накопление данных, формируемых в ходе повседневного выполнения сотрудниками функциональных обязанностей, автоматизацию подготовки документов и принятия решений.

Значительное внимание уделено и *разработке специального программного обеспечения*. Главной его целью является комплексная автоматизация основных направлений деятельности подразделений МВД России: уголовного розыска, предварительного следствия, дознания, исполнения административного законодательства, служб участковых уполномоченных полиции, дежурных частей, патрульно-постовой службы полиции, ГИБДД и др.

Для ЦОД применяются технологии виртуализации и динамического увеличения производительности в зависимости от количества одновременно работающих пользователей и обрабатываемых запросов. Это обеспечивает необходимый уровень гибкости и масштабируемости приложений, да к тому же с гарантией использования информационных ресурсов исключительно сотрудниками МВД России [66].

Использование рассматриваемой системы позволяет повысить эффективность принятия управленческих решений. Это возможно за счет анализа сводной информации, основанной на актуальных данных об объекте управления, а также поиска и выявления закономерностей, характеризующих его, прогнозирования развития ситуации. В целом указанный набор возможностей приводит к оптимизации процесса планирования управляющих воздействий.

Не осталось в стороне и *межведомственное электронное взаимодействие при предоставлении государственных услуг*. Здесь разработаны и зарегистрированы электронные сервисы, внедрено программное обеспечение, организованы защищенные каналы связи, где МВД России выступает в качестве поставщика данных. К специальному программному обеспечению межведомственного электронного взаимодействия получили доступ сотрудники, принимающие непосредственное участие в предоставлении государственных услуг.

В последнее время на фоне гиперактивного развития ИТ особенно остро стоит вопрос обеспечения защиты информационных систем и ресурсов МВД России от различного рода угроз, включая кибератаки. В МВД России во исполнение требований федеральных и ведомственных нормативных правовых актов [4; 27] осуществляется *работа по развитию и совершенствованию существующей системы защиты информации*.

К настоящему времени закончен большой объем работ по лицензированию и аккредитации ОВД в качестве органов по аттестации объектов информатизации по требованиям безопасности информации, по обеспечению их необходимым комплектом контрольно-измерительной и поисковой техники. Продолжается оснащение подразделений МВД России средствами защиты информации. Осуществляется подготовка специалистов в области технической защиты информации на базе образовательных организаций МВД России, в рамках программ высшего образования, профессионального обучения и повышения квалификации изучаются вопросы обеспечения информационной безопасности в подразделениях МВД России.

В этой сфере решаются не только такие классические задачи, как защита информации, информационных ресурсов и информационных систем ОВД от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования, но и задачи, ставшие актуальными в последнее время: создание и развитие системы информационной безопасности ОВД с учетом реализации облачной архитектуры, формирование и совершенствование системы мониторинга состояния информационной безопасности ОВД. Важным моментом при этом является акцент на приоритетном использовании отечественных средств и систем защиты информации.

В ведомственных документах [см., например: 27] четко сформулированы ключевые направления реализации информационной безопасности ОВД, среди которых хотелось бы обратить внимание на наиболее актуальные с учетом современного состояния и развития инфокоммуникационных 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.

При этом ключевым условием реализации указанных векторов развития и совершенствования систем информационной безопасности в ОВД, несомненно, является повышение уровня квалификации сотрудников по направлениям деятельности в области осуществления мероприятий по защите информации.

Как известно, обеспечение общественной безопасности является одной из приоритетных задач МВД России. Поэтому *серьезное внимание уделяется оснащению полицейских подразделений инновационными разработками и их техническому совершенствованию* с целью качественного контроля ситуации и своевременного реагирования на происшествия.

Примером в этой области служит внедрение в деятельность наружных подразделений полиции подсистемы мобильного доступа к информационным ресурсам на базе АПК «Барс». Этот комплекс позволяет сотрудникам получать из информационных систем МВД России оперативную и достоверную информацию о гражданах, транспортных средствах и лицах, находящихся в розыске. Его применение дает высокую эффективность не только в раскрытии преступлений «по горячим следам», но и в обеспечении безопасности информации от несанкционированного доступа.

Освещенная тенденция интеграции информационных ресурсов и систем в составе сервисов ИСОД МВД России не единственная. Еще одним направлением, интересным в плане развития ИТ, является **разработка и внедрение в практику ОВД средств ИТ для решения ряда специфических задач**.

Обратимся, например, к *использованию аналитической программной платформы класса Business Intelligence (BI)*, дающей основу для разработки прикладных решений различных аналитических задач [46]. В качестве таких решений выступает реализация ассоциативного поиска и обработки данных в оперативной памяти, извлечение и объединение информации из множества разнородных источников.

Ассоциативный поиск и обработка данных в оперативной памяти производятся по всему массиву данных. Действует принцип интернет-поисковика: достаточно начать вводить в поисковую строку слово, фразу, и система станет показывать результаты уже по мере их ввода.

В случае же извлечения и объединения информации из множества разнородных источников применяется огромное количество графиче-

ских элементов для представления данных (таблицы, сводные таблицы, гистограммы, диаграммы, графики, календари, слайдеры, интеграция с онлайн-картами и т.д.). Платформа предоставляет пользователю, обладающему соответствующими правами, возможность анализировать отчеты с любого рабочего места, на котором есть браузер.

Платформа класса BI находит применение в решении задач анализа деятельности службы 02 и дежурной части. Источниками данных выступают внутренние системы, осуществляющие поддержку деятельности ведомства.

Анализ и оценка деятельности операторов службы 02 ведутся по многим показателям, среди которых среднее время работы сотрудника (смены), общее количество зарегистрированных карточек, среднее время регистрации карточек.

По результатам рассмотрения показателей формируются различные рейтинги: рейтинг смен, 10 лучших и 10 худших сотрудников и т.д.

Анализируются и обращения о правонарушениях: среднее количество происшествий в то или иное время суток, количество происшествий по времени регистрации (больше/меньше двух минут), время регистрации по типам происшествий, происшествия по степени важности и т.д.

В целом группа рассмотренных показателей позволяет помочь проанализировать работу операторов и провести оценку эффективности их деятельности.

Для решения задач дежурной части формируются другие специальные аналитические показатели. Они отражают общую картину деятельности службы, качество и время реагирования на инциденты. В оценке работы учитываются следующие параметры: общее количество происшествий, среднее время отработки происшествия, рейтинг правонарушений, соотношение ложных и подтвердившихся вызовов. Особенность в том, что многие показатели привязаны к карте. Эта часть технологии позволяет проанализировать их как в целом по городу, так и по территориям ответственности, что упрощает оценку работы службы в разрезе административных округов (территорий обслуживания).

Следует отметить, что аналитика и статистика по всем направлениям является востребованной, актуальной и вызывает широкий интерес со стороны аппарата управления. В то же время имеется и класс задач, решение которых представляется довольно важным с точки зрения анализа деятельности подразделений. К указанному классу относится *автоматизация составления отчетности*: данных по показателям уголовной статистики и оперативных сводок (анализ регистрации уголовных дел — возбуждено/отказано, анализ уголовных дел по статьям и т.д.); данных по линии работы ГИБДД (учет краж транспорт-

ных средств по территориальному признаку, по маркам автомобилей, по времени суток и т.д.).

Кроме того, применение аналитических средств класса BI *способствует решению вопросов управления кадровым обеспечением* (например, можно регулировать штатную численность сотрудников в части ее увеличения на территориях, отличающихся высоким количеством совершения преступлений); *повышению эффективности профилактических мероприятий* на основе выделения целевых групп преступлений и концентрации усилий по их профилактике и предупреждению.

Таким образом, в результате полномасштабного реформирования системы МВД России значительные успехи были достигнуты в сфере совершенствования информационного обеспечения деятельности ОВД, в числе которых создание современной информационно-телекоммуникационной инфраструктуры на базе ИМТС МВД России, внедрение ИСОД МВД России и центров обработки данных, разработка ряда специализированных территориально распределенных систем, стандартизация и унификация требований к существующим и разрабатываемым АИС на основе облачной архитектуры, смещение акцента в эксплуатационных требованиях к АИС и технологиям в сторону аналитических и интеллектуальных функций.

1.3. Облачные технологии и сервисы, перспективы их применения в органах внутренних дел

Развитие ИТ в системе МВД России происходит стремительно. Ежегодно внедряются в деятельность различных департаментов и служб новые информационные системы, происходит модернизация существующих.

Применяемые системы становятся более:

- *интеллектуальными*. А наличие слова «аналитический» в их названии — это уже не дань моде, а насущная необходимость, все больше отражающая реальность;
- *мобильными*. Полноценное использование всех доступных ресурсов и возможностей информационных систем наиболее востребовано «на земле», а не в кабинете. Кроме того, преимуществами этих систем имеют возможность пользоваться практически все сотрудники, независимо от их удаленности от центра;
- *сложными*. Известно, что, с одной стороны, более сложная система часто имеет лучшую функциональность, она более мощная и качественная. Но, с другой стороны, ее сложнее обслуживать и поддерживать, для ее развертывания и работы требуется подготовленный персонал, качественное и современное оборудование.

Во многом это создает серьезные препятствия на пути дальнейшего развития информационных систем в структуре МВД России. Дело в том, что вполне вероятно состояние, при котором информационные системы достигнут пика сложности. Для их работы и обслуживания необходимо будет создавать целые отделы специалистов, а их разработка, ввод в эксплуатацию и использование будут стоить больших денег.

Оценка с точки зрения практики и практичности говорит о том, что для решения большинства проблем информатизации МВД России нет необходимости в создании систем повышенной сложности, а может, и суперсистем по сложности реализации. Для обеспечения функциональности вполне достаточно перспективного направления развития информационных систем и технологий. Речь идет об облачных технологиях (облачных вычислениях).

Термин «облачные вычисления» стал использоваться в области ИТ с 2008 г. Приведем его трактовку на данный момент.

Облачные вычисления — это инновационная технология, которая предоставляет динамично масштабируемые вычислительные ресурсы и приложения через Интернет в качестве сервиса под управлением поставщика услуг.

Для системы МВД России реализация облачных технологий осуществляется в инфраструктуре ИМТС МВД России. Идея облачных вычислений восходит к центрам коллективного пользования, к предоставлению услуг, связанных с прикладными сервисами. Специалисты прогнозируют перемещение большей части ИТ к облачным в течение 5—7 лет [66].

Главная задача таких технологий — обеспечить пользователя качественной услугой. Исходя из этого, выделим **несколько моделей предоставления услуг** (рис. 1.3).

1. *Инфраструктура как услуга (IaaS).* Эта модель предоставляет пользователям различные информационные ресурсы: виртуальный сервер, хранилища сетевой инфраструктуры. Имеются широкие возможности по настройке сервиса, но в то же время это затрудняет обслуживание. Чтобы избежать подобных проблем, часто предлагают ряд шаблонов по предоставлению виртуальной инфраструктуры.

2. *Платформа как услуга (PaaS).* В рамках данной модели предоставляется доступ к программной платформе: пользователи могут создавать и размещать собственные приложения в ее формате, имеют доступ к управлению ресурсами более низкого уровня (операционная система, хранилища данных и т.д.). Поэтому такая модель может оказаться очень полезной при разработке новых информационных систем для МВД России, поскольку подразумевает выбор платформы, а не ее создание.

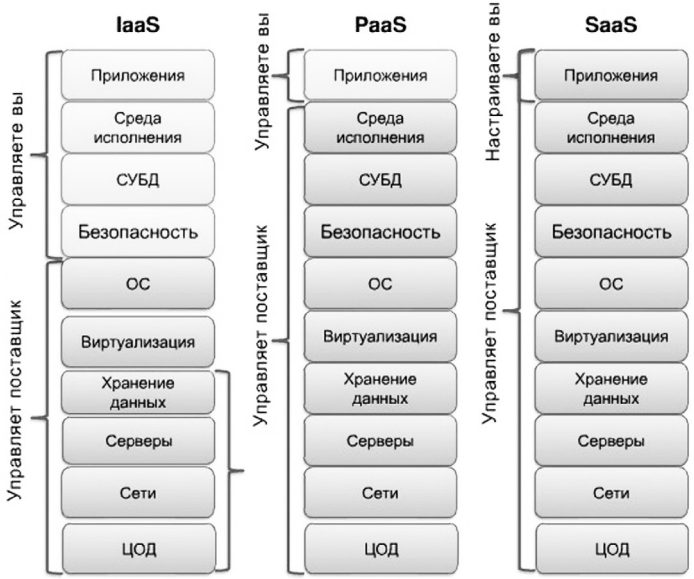


Рис. 1.3. Модели предоставления облачных услуг

3. *Программное обеспечение как услуга (SaaS).* Рассматриваемая модель предоставляет услуги программного обеспечения. В ней пользователи получают доступ только к нему через сеть. Использование данной модели, например, вполне обоснованно в системах электронного документооборота.

Эти модели не ограничивают возможности предоставления информационных сервисов. Разделение их на три варианта возникло естественным образом исходя из потребностей пользователей.

Помимо различных способов предоставления сервисов имеются **несколько вариантов развертывания облачных систем** (рис. 1.4).

1. *Частное облако.* Оно используется для предоставления сервисов внутри одного подразделения (службы, управления, департамента), которое является одновременно и заказчиком, и поставщиком услуг.

2. *Публичное облако*. Его применяют облачные провайдеры (например ФКУ «ГИАЦ МВД России» для предоставления сервисов внешним заказчикам.

3. *Смешанное (гибридное) облако*. Подразумевает совместное использование двух вышеперечисленных вариантов развертывания.

Естественно, что сейчас не существует эталонной облачной инфраструктуры. Может использоваться целый ряд различных программных и аппаратных решений.

Рис. 1.4. Модели развертывания облачных услуг

Постараемся определить **основные свойства облачных технологий** независимо от конкретной реализации. Некоторые из этих характеристик присущи не только облачным решениям, что может создать ложное впечатление об их сути. Возникает вопрос: не новое ли это название для уже давно известных технологий? Мы полагаем, что нет. Облачные системы ориентированы прежде всего на предоставление сервисов со стороны ИТ, что и отличает их от классических информационных систем. При этом для реализации требуется совместное использование множества технологий, в то время как каждая технология по отдельности не служит полноценным решением для создания сервис-ориентированной инфраструктуры. Итак, отметим основные свойства «облачных» технологий.

1. *Эластичность*. Понимается как способность к горизонтальному и вертикальному масштабированию. Подчеркнем, что помимо динамического увеличения числа используемых ресурсов требуется также и возможность сокращения выделяемых вычислительных мощностей. Таким образом, указанное свойство обеспечивает облачным системам ряд экономических преимуществ по сравнению с классическими информационными системами.

2. *Отказоустойчивость*. Чтобы система обладала этим свойством, требуется избыточное количество ресурсов. В облаке возможно избежать этого за счет использования виртуализации. Но в то же время обеспечение аппаратной отказоустойчивости требует некой избыточности.

3. *Обеспечение фиксированного качества сервиса*. Свойство предполагает прежде всего гарантию высокой доступности сервисов. Но есть и другие, не менее важные, характеристики: малое время реакции на действия пользователя, соответствие заявленной производительности и т. д. Без наличия гарантий качества предоставляемых услуг использование облачных технологий становится крайне рискованным и, возможно, убыточным.

4. *Динамичность*. Она определяется временем, в течение которого информационная система может отреагировать на изменяющиеся запросы пользователя. При быстрой перестройке система становится основой для обеспечения непрерывности процессов. Причем в случае с облачными инфраструктурами за это не приходится платить избыточным количеством используемых ресурсов.

5. *Виртуализация*. Позволяет реализовать ключевые требования к облачным системам за счет абстрагирования от физического оборудования. При этом упрощается обслуживание систем, повышается отказоустойчивость инфраструктуры. Использование виртуализации дает эластичную масштабируемость облачных систем.

6. *Управление хранением данных*. В принципе облачные системы часто бывают распределенными, тогда задача эффективного управления доступом к данным в них стоит остро. Помимо обеспечения целостности данных необходимо также учитывать скорость доступа к ним и возможное увеличение объема хранимой информации.

7. *Безопасность*. Использование облачных технологий требует выработки новой стратегии безопасности данных, связанной с их особенностями.

8. *Интерфейс прикладного программирования (API) для облачных приложений*. В работе облачных систем важной функцией является наличие стандартизированных программных интерфейсов для взаимодействия облака и его приложений. Концепция позволяет разработчикам создавать облачные программы изначально используя все преимущества облачных инфраструктур и технологий.

При наличии в облачных системах целого ряда существенных недостатков и недоработок идея простого и динамичного предоставления информационных сервисов уже завоевала популярность в информационной среде. Именно поэтому такая идея и была использована в информационном обеспечении деятельности МВД России.

Сегодня наблюдается постоянное совершенствование, улучшение модели облачных систем. В то же время эксперты видят основную проблему не в решении технических вопросов, а в урегулировании проблем, связанных с юридическими аспектами функционирования облачных систем, для чего необходимы экономические методики планирования и анализа эффективности.

Успешное решение этих вопросов может привести к новому этапу развития информационных систем, существенному сокращению сроков их проектирования, повышению качества функций и услуг. Уже сегодня при разработке информационных систем необходимо планировать будущее ИТ МВД России исходя из этого.

Реализация облачной архитектуры в создаваемых в МВД России информационных системах и разрабатываемых технологиях является залогом их эффективной эксплуатации и длительности жизненного цикла. Качественные характеристики облачных вычислений в состоянии обеспечить такую степень предоставления сотрудникам ОВД информационных услуг, которая позволит существенно повысить уровень решения профессиональных задач.

1.4. Видеотехнологии и геоинформационные системы

Видеотехнологии. Телевизионная связь как таковая в деятельности ОВД чаще всего применяется для целей дистанционного наблюдения за различными объектами: территориями, помещениями, транспортом, людьми и т.д. [62, ч. 3].

Система видеонаблюдения не только обеспечивает непрерывный оперативный контроль ситуации на объекте, но и автоматически обнаруживает вторжение в контролируемое пространство, осуществляет видеозапись тревожных событий или непрерывную запись всей видеоинформации.

Кабельное телевидение — это телевизионные системы наблюдения, или системы замкнутого телевидения (англ. *closed circuit television* — CCTV), в которых изображение объекта с видеокамеры передается по кабелю на устройство отображения (монитор). Название объясняется тем, что эти системы не связаны с широковещательным телевидением и используются для решения конкретных задач (обнаружение, идентификация, диагностика, управление, документирование и т.д.).

Телевизионные системы видеонаблюдения — это комплекс устройств, количество и сложность которых определяется многими параметрами (вид объекта, структура объекта, необходимость архивирования и т.д.).

Обычно в TV-систему наблюдения входят:

- устройства, позволяющие преобразовывать изображение в электрический сигнал: видеокамеры;
- устройства отображения информации: мониторы, дисплеи;
- устройства передачи видеосигнала: по коаксиальному кабелю, оптико-волоконной линии, телефонной линии, радиоканалу;

- устройства управления видеокамерой: поворотные механизмы; механизмы, изменяющие угол наклона; устройства, изменяющие параметры объектива видеокамеры (фокусное расстояние, диафрагму); обогреватели, стеклоочистители;
- устройства управления режимами отображения: последовательные коммутаторы, квадраторы, мультиплексоры;
- устройства регистрации изображения: спецвидеомагнитофоны, видеопринтеры;
- устройства записи на диски: видеорегистраторы.

По типу используемого оборудования системы видеонаблюдения делятся на аналоговые и цифровые [63].

1. *Аналоговые системы видеонаблюдения* используют там, где необходимо организовать наблюдение на небольшом количестве объектов и информацию с видеокамер записывать на видеомагнитофон. Будучи исторически первыми, и сейчас аналоговые системы видеонаблюдения еще пользуются большой популярностью в силу невысокой стоимости и оптимальности с точки зрения соотношения цена/качество. Кроме того, они отличаются простотой конструкции и надежностью, которая проверена временем.

Построение аналоговых систем видеонаблюдения базируется на использовании непосредственно камер видеонаблюдения, представляющих собой оптические устройства, ПЗС-матрицы которых формируют видеосигнал из светового потока, проходящего через объектив и группу линз и попадающего на эту матрицу. В условиях необходимости масштабирования системы аналоговые камеры видеонаблюдения могут быть модернизированы посредством подключения блока преобразования аналогового видеосигнала в цифровой. Такие камеры видеонаблюдения уже можно подключать в цифровые системы видеонаблюдения (рис. 1.5).

2. *Цифровые системы видеонаблюдения*, интегрируемые в комплексные системы, необходимы для обеспечения безопасности особо ответственных или территориально распределенных объектов. В качестве устройств видеонаблюдения используют цифровые IP-камеры, которые подключаются к сети с помощью модема, сотового телефона, беспроводного модема или напрямую через точку доступа локальной сети объекта. IP-камеры работают без какого-либо дополнительного оборудования, а видеоинформация оперативно передается по сети без существенных задержек (с учетом правильной организации пропускной способности каналов связи), тем самым обеспечивая бесперебойную работу на всех временных отрезках (рис. 1.6).

CCTV широко используются в системах безопасности объектов и в качестве самостоятельных систем, и в составе единой интегриро-

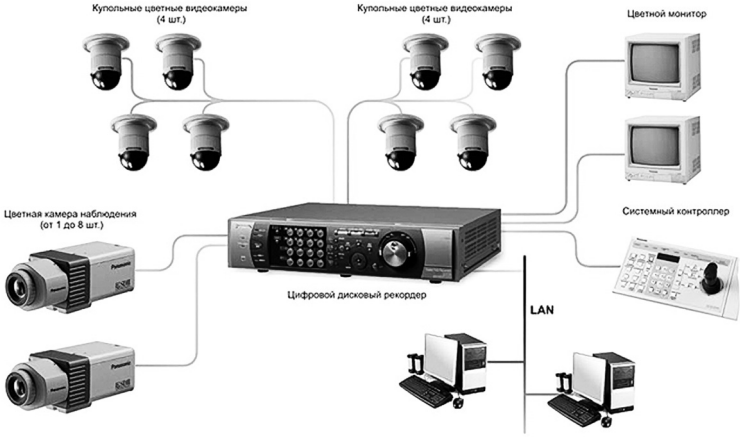


Рис. 1.5. Структурная схема системы видеонаблюдения на базе видеорегистратора

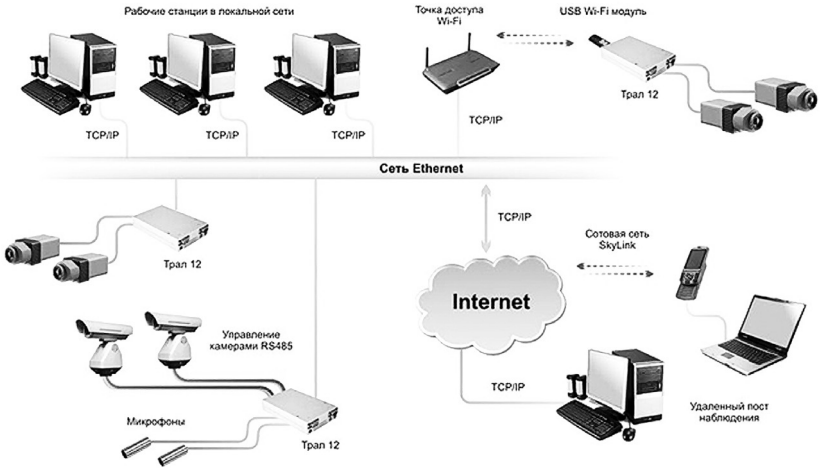


Рис. 1.6. Структурная схема системы видеонаблюдения на базе локальной компьютерной сети подразделения

ванной системы безопасности. *Системы охранного видеонаблюдения, работающие в составе интегрированной системы охраны*, должны обладать эксплуатационной, информационной, аппаратной и программной совместимостью с другими системами и средствами, входящими в эту систему.

В ОВД накоплен большой опыт применения систем видеонаблюдения. Так, они широко использовались подразделениями вневедомственной охраны для целей контроля установленного режима на открытых территориях и в отдельных помещениях.

Другим немаловажным направлением является *производство досмотровых работ на рубежах безопасности* (на контрольно-пропускных пунктах, таможенных постах, в процессе контроля почтовых отправлений). Здесь телевизионные системы используются совместно с рентгеновской аппаратурой. *Рентгенотелевизионные установки* позволяют быстро обнаруживать запрещенные к провозу (проносу) предметы (взрывоопасные, легковоспламеняющиеся вещества, оружие, боеприпасы и т.д.).

С помощью данных систем удается передавать в дежурные части ОВД видеоинформацию о ситуации на улицах, площадях, остановках общественного транспорта, рынках и прилегающих территориях, с вокзалов, из аэропортов и других общественно значимых мест. Руководители и дежурные смены ОВД, наблюдая в режиме реального времени за ситуацией в городе, принимают своевременные меры по предотвращению преступлений.

Применение систем кабельного телевидения и специальных программ позволяет считывать государственные номера автомобилей, определять их скорость, распознавать цвет и тип автотранспортных средств, автоматически фиксировать нарушение правил дорожного движения, осуществлять мониторинг особо ценных и специально перевозимых грузов.

Одним из перспективных направлений является *совершенствование информационных систем, построенных на базе видеотехнологий. Базовым сегментом для такого рода систем является подсистема видеонаблюдения*. Она выполняет основную функцию — отображать и фиксировать видеоинформацию о внешней среде, при этом выполняя в автоматическом режиме и ряд других функций, а именно:

- контроль «безопасной территории» по заранее заданным в системе границам и зонам;
- распознавание лиц и непрерывное сравнение на основе портретной идентификации с банком данных лиц, находящихся в розыске;
- распознавание номерных знаков, фиксация нарушений правил дорожного движения, ретроспективный анализ маршрутов движения разыскиваемого транспорта;
- анализ поведения объектов, то есть определение позиции или ориентации реального объекта (руки, головы, туловища; оставленных предметов) в виртуальной среде;

– хранение и обработка видеоинформации, предоставление удаленного санкционированного доступа к видеоархиву, обеспечение возможности восстановления хода событий на основе архивированных видеоматериалов.

Подсистема видеонаблюдения — это фундаментальная составляющая современных АИС, применяемых в деятельности ОВД (например АПК «Безопасный город» — см. о нем подробно в подразд. 2.3). Видеоизображение является очень важным источником объективной информации о текущей ситуации, которая, в свою очередь, позволяет принимать решения в соответствии с быстро меняющейся обстановкой современного города, оптимизируя затраты времени на поиск признаков идентификации правонарушения или преступления. В реалиях сегодняшнего дня эти функции невозможны без применения современных интеллектуальных технологий видеоаналитики.

Исходя из анализа прикладных направлений в области применения интеллектуальных видеосистем различных производителей, можно отметить, *что современные технологии видеоаналитической автоматизации для городских систем видеонаблюдения должны включать следующий минимальный набор функций* с представлением результатов, что позволит наблюдающему лицу своевременно и эффективно принимать решения:

– детектирование (целей, объектов движения);
– распознавание (образов, поведения объектов);
– классификация и индексация (соотнесение разных признаков распознавания);
– реагирование (подача управляющей команды как реакция на событие лица, принимающего решения, или как автоматизированный процесс);
– поддержка расследования (проведения процессуальных действий);
– документирование (фиксация доказательств) [55].

По мнению экспертов и сотрудников ОВД, применяющих видеоаналитические системы, они дают возможность быстрого анализа огромного объема информации, важной для обеспечения безопасности и адекватности реагирования на возникающие угрозы за счет индексации и распараллеливания поиска.

В настоящее время ведется широкое внедрение в программное обеспечение видеосистем интеллектуальных модулей распознавания, оборудование объектов контроля современными видеокамерами, которые *должны отвечать требованиям Экспертно-криминалистического центра МВД России*. Среди таких требований и критериев — качество видеоматериалов, пригодных для проведения идентификационных

исследований, первичная обработка видеосигналов, стандартизация и унификация оборудования и т. д.

Все это превращает камеры в реальные источники информации и предлагает законченный интеллектуальный продукт для видеоаналитики. «Умная начинка» дает возможность в огромных видеопотоках распознавать человеческие лица, номера автомобилей, фиксировать нарушение правил дорожного движения, осуществлять трекинг целей и анализировать поведение объектов.

Сейчас в ОВД применяются как аналоговые, так и цифровые интеллектуальные камеры, в том числе определяющие биометрические параметры лица человека. Несмотря на это многообразие, существующие системы видеонаблюдения в должной мере не позволяют обеспечить необходимый уровень безопасного функционирования даже некоторых крупных городов одного региона, не покрывая территорию полно и всесторонне.

Это привело к *расширению функционала подсистем видеонаблюдения в целях эффективного применения в составе АИС ОВД по следующим направлениям*:

1) расширение зон, охватываемых подсистемами видеонаблюдения:
- оснащение системами видеонаблюдения общественных мест (остановки, парки, скверы, жилые комплексы, улицы микрорайонов, дорожная сеть, аэропорты, вокзалы и т. п.);
- интеграция объектовых систем видеонаблюдения в единую среду (больницы, образовательные учреждения, объекты ЖКХ, торговые центры и т. д.), а также в АПК, например для фиксации нарушений правил дорожного движения его участниками;

2) плановая модернизация существующих систем (переход от аналоговых систем к цифровым IP-системам, повышение качества изображения, перенесение части вычислительных функций на камеры и т. д.);

3) активное использование видеоаналитики:
- контролирование оставленных предметов (бесхозных сумок, багажа);
- фиксация пересечения контрольных зон (зон дорог, границы которых важны в рамках соблюдения правил дорожного движения, границ охраняемых объектов организаций и др.);
- распознавание лиц и действий (лиц, находящихся в розыске, признаков преступлений);
- видеоаналитика для работы с архивом (индексированный поиск) [58].

В рамках первого направления интересным решением, отражающим процесс интеграции, объединения автономных систем в единую среду управления деятельностью ОВД, выступает *соединение под-*

системы видеонаблюдения и геоинформационной подсистемы (см. об этом подробнее ниже в части «Геоинформационные системы»).

Что касается второго направления, *плановой модернизации, сопровождающегося одновременно интеграцией*, то его можно проследить на примере деятельности компаний. Так, одни из первых отечественных разработчиков интеллектуальных систем в сфере безопасности — московские компании ISS [См. подробнее: 89] и Vocord [см. подробнее: 92] — прошли целый путь от аналоговых камер и видеорекордеров до цифровых систем с интеллектуальным программным обеспечением.

Компания ISS выпустила новую улучшенную по техническим параметрам версию модуля распознавания автомобильных номеров, кроме уже имеющихся модулей интеллектуальной автоматизации.

Компания Vocord предлагает использование на каждой точке установки камеры собственного мини-сервера, который позволяет производить запись данных с камер на локальный носитель, а при восстановлении канала связи видеоархив самостоятельно восполняет пробелы в записи за счет считывания данных с мини-сервера.

Примерами *программных продуктов и решений на базе интегрированной среды безопасности SecurOs* компании ISS являются *интеллектуальные системы распознавания* автомобильных номеров «Авто-Инспектор», распознавания лиц «Face-Инспектор», анализа траекторий движения и обнаружения оставленных предметов «Модуль трекинга целей среды SecurOS» и т.д.

В последнее время в практике ОВД получили распространение программные продукты компании Macroscop (Пермь) [см. подробнее: 90], представляющие собой *профессиональное программное обеспечение для IP-камер и выполняющие обработку, анализ, хранение, отображение видеоданных*. Благодаря данному программному продукту можно построить эффективную систему видеонаблюдения любого масштаба как с помощью нескольких IP-камер, так и объединяя множество серверов и рабочих мест мониторинга.

В настоящее время применяются три конфигурации, отличающиеся количеством камер, рабочих мест мониторинга и поддержкой интеллектуальных модулей. Самая мощная и функциональная версия Macroscop позволяет выстроить систему IP-видеонаблюдения с неограниченным количеством IP-камер, неограниченным количеством серверов и рабочих мест. В версию уже включены модули обнаружения лиц, интерактивного поиска и «перехвата» похожих объектов, трекинга, возможно подключение других интеллектуальных модулей: подсчета и распознавания лиц, распознавания автомобильных номеров, обработки потоков аудиоданных и т.д.

Так, *интеллектуальный модуль трекинга позволяет отслеживать движущиеся объекты*. Задается контрольная линия или зона произвольной формы, о пересечении которой оповещает монитор. Модуль обнаружения лиц позволяет автоматически узнавать их в видеопотоке. Выбираются камеры и время, за которое необходимо просмотреть все лица, попавшие в поле их зрения. На этой основе формируется база лиц. Выбрав заинтересовавшее лицо, можно просмотреть все отрезки архива, где оно фиксировалось.

Применение модуля интерактивного поиска отражает такое направление, как использование видеоаналитики для работы с архивом. Модуль позволяет значительно ускорить и упростить поиск объекта в архиве, а функция перехвата объектов позволяет «перехватить» интересующий объект. Для этого нужно задать его параметры (размер, цвет), выбрать образец из архива или загрузить фото. Как только этот или похожий объект появится в поле зрения одной из камер, система подаст сигнал. Функция интерактивного поиска на основе фотографии объекта (человек, автомобиль, любой движущийся объект) или указания его цвета, размера, положения в кадре выдает все похожие объекты, содержащиеся на архивных видеозаписях всех камер.

Долговременное архивирование видеоинформации телевизионных систем наблюдения позволяет в дальнейшем проводить ее анализ и использовать также для криминалистических экспертиз.

Так, для *биометрической идентификации личности по изображению лица* предназначен мобильный АПК биометрической идентификации личности «Сова» (ЗАО «Проминформ», Пермь). Комплексы экстренной связи гражданин — полиция, позволяющие своевременно получать информацию от граждан о совершении того или иного преступления, становятся более востребованными, если кроме речевого трафика позволяют получать и видеоизображение обратившегося.

Активно *применяется аналитика и в рамках решения такой актуальной проблемы, как обеспечение безопасности дорожного движения*.

Водители транспортных средств часто не соблюдают скоростной режим, требования дорожной разметки, правила проезда перекрестков и пешеходных переходов, выезжают на встречную полосу.

Эта проблема решается внедрением на дорогах страны *системы автономных и стационарных комплексов фото-, видеофиксации*.

К наиболее популярным комплексам автоматической фото-, видеофиксации нарушения правил дорожного движения, разработанным отечественными производителями, относят:

- «Кречет» (ЗАО «Ольвия», Санкт-Петербург);
- «Кордон» (ООО «Симикон», Санкт-Петербург);
- «Интегра-КДД» (Консорциум «Интегра-С», Самара).

Комплексы «Кордон» и «Кречет» контролируют соблюдение скоростного режима, одновременно отслеживая пересечение линий дорожной разметки с выездом на полосу встречного движения и движение транспортных средств по полосе, выделенной для общественного транспорта.

Комплекс «Интегра-КДД» фиксирует нарушение правил дорожного движения водителями транспортных средств на перекрестках и нерегулируемых пешеходных переходах.

Инновационные передовые технологии, примененные при разработке и изготовлении указанных комплексов, позволяют контролировать соблюдение требований дорожных знаков, дорожной разметки, сигналов светофора, а также предоставление преимущества пешеходам на нерегулируемых пешеходных переходах. Комплексы работают круглосуточно при любых погодных условиях. Процесс фиксации нарушения, обработки полученной информации и подготовки постановления об административном правонарушении происходит в автоматическом режиме.

Установка данных автоматических комплексов и объединение их в единую сеть с действующими электронными системами обеспечения безопасности и базами данных переводит уровень информационного обеспечения деятельности ГИБДД на кардинально новый уровень. Так, контроль соблюдения правил дорожного движения всеми его участниками приводит к существенному снижению аварийности на определенных участках автодорог [76, кн. 1].

Комплексы, работающие в автоматическом режиме, позволяют высвободить сотрудников ДПС для оперативного реагирования на изменяющуюся дорожную обстановку, разбора дорожно-транспортных происшествий, регулирования вручную в местах временного скопления автотранспорта и т.д. Круглосуточный мониторинг транспортных потоков дает возможность вносить коррективы в регулирование схем движения автотранспорта и автоматически производить поиск машин, находящихся в розыске.

Внедрение и эксплуатация таких систем контроля дорожной обстановки способствуют повышению эффективности деятельности подразделений ГИБДД по обеспечению безопасности на дорогах.

Подводя итог всему сказанному выше, *можно представить подсистемы видеонаблюдения в виде совокупности нескольких систем функционирования, которые должны быть технически готовы к выполнению актуальных правоохранительных задач.*

В соответствии с этим приведем *примерный перечень функций таких систем*:

1) функции системы распознавания противоправных действий:

- обнаружение признаков преступлений;
- обнаружение проникновения на охраняемые объекты;
- передача на автоматизированное рабочее место[1] оператора ситуационного центра управления текстового сообщения и звукового сигнала об обнаружении противоправных действий;
- наблюдение за развитием ситуаций, связанных с противоправными действиями, в режиме реального времени;
- сохранение информации о противоправных действиях в базе данных системы и ее быстрый поиск;
- формирование отчетов в соответствии с заданными параметрами;

2) функции системы идентификации личности:
- биометрическая идентификация личности по базам данных оперативных учетов ОВД;
- передача на АРМ оператора дежурной части ОВД текстового сообщения и звукового сигнала об обнаружении личности, проходящей по оперативным учетам;
- наблюдение за обнаруженным физическим лицом в режиме реального времени, контроль за его перемещениями по территории региона;

3) функции системы распознавания тревожных ситуаций:
- обнаружение предметов, оставленных в местах массового скопления людей;
- обнаружение агрессивно настроенных групп граждан;
- обнаружение падающего или лежащего человека;
- передача на АРМ оператора дежурной части ОВД текстового сообщения и звукового сигнала об обнаружении тревожной ситуации;
- наблюдение за развитием тревожных ситуаций в режиме реального времени;
- формирование отчетов в соответствии с заданными параметрами.

Особое требование должно предъявляться к видеотракту подсистемы видеонаблюдения с целью *обеспечения следующих показателей качества изображения*:
- изображения должны отображать максимально возможное число признаков, идентифицирующих объекты;
- видеотракт подсистемы с цифровым видеонакопителем должен аппаратно обеспечивать получение кадра с разрешением не ниже 720 × 576 пикселей;
- режим записи должен быть 25 кадров в секунду (по каждому каналу при максимальном качестве видеоданных);

[1] Далее используется сокращение АРМ.

- видеоинформация должна быть представлена в виде последовательных статических фотографических изображений с параметрами не меньше указанных;
- допускается использование как аналоговых, так и цифровых IP-видеокамер, тепловизионных и комбинированных типа день/ночь;
- видеоматериалы, полученные с помощью подсистемы, должны быть пригодны для проведения идентификационных исследований.

Видеоподсистема должна позволять использование оборудования различных производителей, а архитектура обеспечивать возможность масштабирования.

Геоинформационные системы (географические информационные системы)[1] — это информационные системы, обеспечивающие сбор, хранение, обработку, анализ и отображение пространственных данных и связанных с ними иных сведений, а также получение на их основе информации и знаний о географическом расположении объектов.

Современные ГИС расширили использование электронных (цифровых) карт за счет хранения графических данных в виде отдельных тематических слоев, а также качественных и количественных характеристик составляющих их объектов в виде баз данных. Такая организация данных при наличии гибких механизмов управления ими дает принципиально новые аналитические возможности.

В структуре ГИС основными компонентами технологий являются графические и тематические (атрибутивные) базы данных, обладающие модельными и расчетными функциями для принятия на этой основе разнообразных решений и контроля их исполнения. В графических базах данных хранится метрическая основа компьютерной карты. Атрибутивные базы данных содержат в себе описания территории и дополнительную информацию. Для работы с этими данными имеется одна или две *системы управления базами данных*[2]. Функции СУБД — поиск, сортировка, добавление и исправление информации в базах данных.

ГИС могут применяться в правоохранительной деятельности для решения следующих задач:

- планирования специальных операций и мероприятий;
- моделирования при возникновении различных ситуаций;
- навигации мобильных подразделений ОВД;
- принятия оптимальных управленческих решений на основе анализа пространственных данных.

На практике хорошо себя зарекомендовали такие ГИС, как ArcInfo и ArcViewGIS (разработка США) и отечественная система «Панорама».

---

[1] Далее используется сокращение ГИС.

[2] Далее используется сокращение СУБД.

Наиболее интересным направлением развития ГИС является интеллектуальная поддержка. ГИС с интеллектуальной поддержкой обеспечивает отображение на интерактивной карте города информации об объектах. Можно увидеть, где расположены видеокамеры, объекты, имеющие значение для принятия решения дежурным, зафиксированы места происшествий, находятся мобильные отряды, узнать сводную и адресную информацию. ГИС представляет собой масштабируемую детализированную электронную карту города, содержащую множество тематических слоев с информацией, поступающей от других подсистем. Пример такой ГИС представлен на рис. 1.7.

Основной тип электронной карты, который используется в ГИС, — *векторная электронная карта*. Ее структура представлена на рис. 1.8.

Она представляет собой совокупность объектов, характеристики которых задаются классификатором, связанным с ней. Среди этих характеристик: метрика (координаты, размеры, тип объекта); семантика — набор типичных для данного объекта характеристик, связанных с ним (например материал постройки, адрес и т.д.).

В наиболее общем виде логическая структура ГИС включает четыре основных элемента:

1) СУБД, обеспечивающую хранилище вспомогательных данных и реализующую часть бизнес-логики;

2) модули, отвечающие за взаимодействие с другими системами;

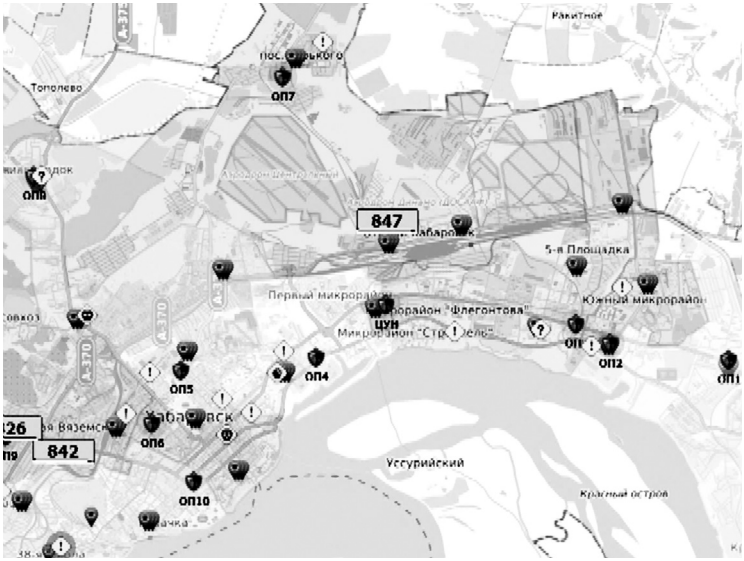


Рис. 1.7. Отображение объектов на карте города

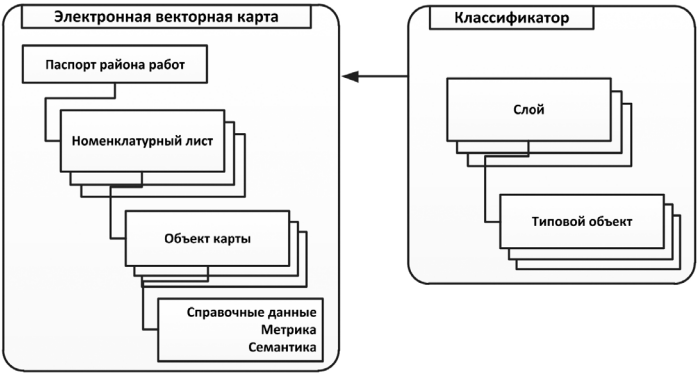


Рис. 1.8. Структура векторной карты

3) модуль отображения картографической информации, служащий также для вывода вспомогательной информации на карту;

4) модуль администрирования ГИС для управления справочниками и вспомогательными таблицами данных, а также администрирования СУБД.

Характерный для современных реалий процесс интеграции, объединения автономных систем в единую среду управления деятельностью подразделений ОВД, о котором мы говорили выше, проявляющийся в данном случае как *использование одновременно ГИС и систем видеонаблюдения*, например в рамках АПК «Безопасный город» (см. об этом в подразд. 2.3), дает должностным лицам, ответственным за обеспечение безопасности, эффективный набор инструментов для оценки складывающейся оперативной обстановки, принятия обоснованных решений и их выполнения в едином регламентном цикле управления.

С одной стороны, участники процесса управления обеспечены информацией о расположении мест происшествий, о передвижении мобильных объектов, дислокации сил и средств ОВД и иной картографической информацией, а с другой — актуальными видеоданными о том, что происходит. Иными словами, лицо, принимающее решение, может увидеть картину ситуации как в целом (с помощью ГИС), так и в деталях (с помощью системы видеонаблюдения). Одна из ключевых возможностей систем видеонаблюдения — фиксация видеоданных — позволяет оперативно реконструировать произошедшие события и использовать эту информацию для раскрытия и расследования преступлений.

В свою очередь, распространенные сегодня картографические системы и среды позволяют встроить компоненты ГИС в состав специализированных АРМ и АИС.

1.5. Интегрирование информационных технологий в составе ситуационных центров

В продолжение рассуждений об интеграции различных ресурсов для решения задач ОВД как одной из современных тенденций в этой части пособия рассмотрим еще один ее вариант.

Еще раз подчеркнем, что современный период существования общества характеризуется стремительным развитием технологий в области телекоммуникаций, что позволяет использовать новые формы организации управления на основе ИТ. Повышение эффективности принятия управленческих решений, в том числе и в ОВД, обеспечивается консолидацией информационных ресурсов в единое целое. Примером служат центры ситуационного управления.

Ситуационный центр[1] — это комплекс современных средств коммуникаций (видео-конференц-связь, конференц-связь и другие средства интерактивного представления информации), предназначенный для оперативного управления, контроля и мониторинга различных объектов, ситуаций и др.

В СЦ создается комплекс специально организованных рабочих мест для персональной и коллективной аналитической работы.

Концепцию СЦ в 70-е гг. XX в. предложил английский кибернетик Стаффорд Бир, и такой центр для первых лиц государства был создан под его руководством уже в конце 70-х гг.

Основной задачей СЦ была поставлена поддержка процесса принятия стратегических решений на основе визуализации и углубленной аналитической обработки оперативной информации. Эффективность СЦ выражается в том, что он позволяет включить резервы образного, ассоциативного мышления. Образное представление ситуации дает возможность «сжимать» информацию, обеспечивая обобщенное восприятие происходящих событий.

В настоящее время эта концепция СЦ как комплексной информационно-аналитической системы поддержки и принятия управленческих решений весьма популярна. Сейчас в мире существуют несколько сотен СЦ. В основном ими пользуются правительства разных стран, а также руководители крупных корпораций. Так, президента США обслуживают четыре СЦ. Несколько десятков центров существуют в Европе. Один из самых технически оснащенных находится в распоряжении правительства Германии и служит для углубленного анализа социальных, экономических и политических проблем [72].

В России одним из первых прообразов СЦ стал оперативный штаб по ликвидации последствий чернобыльской катастрофы в 1986 г.

[1] Далее используется сокращение СЦ.

На основе его решений был создан СЦ руководства Министерства по чрезвычайным ситуациям. Он обеспечивает визуализацию текущего и прогнозируемого состояния анализируемой ситуации, показывает наличие сил и средств, варианты их возможного использования. В результате принимаются решения, которые с помощью имеющихся в СЦ средств доводятся до спасателей.

Другой СЦ, который эффективно функционирует и сейчас, был создан в 1994 г. в Совете безопасности Российской Федерации. Он позволяет проводить мониторинг, моделировать последствия, анализировать события, которые происходят в экономической и социальной сфере, в области национальной безопасности, что помогает вырабатывать решения.

В феврале 1996 г. был введен в строй СЦ в резиденции президента Российской Федерации. В нем развернут достаточно сложный программно-мультимедийный комплекс: 3 экрана размером 1,5 × 2 м, более 10 рабочих станций (студий нелинейного монтажа, графических станций, компьютеров для подготовки презентаций), мощный сервер, который хранит огромные объемы информации, а также набор различных инструментальных средств, позволяющих обрабатывать и представлять информацию. При анализе ситуации материал оперативно дополняется новыми данными, на экранах выводятся результаты моделирования. Принимаемые решения доводятся до исполнителей средствами того же СЦ.

Сегодня СЦ используются федеральными органами государственной власти, органами исполнительной власти субъектов Российской Федерации и органов местного самоуправления, крупными промышленными предприятиями, различными государственными и частными организациями, включая образовательные, и, конечно, подразделениями ОВД.

Управление обстановкой «по ситуации» становится нормой как для крупных коммерческих компаний, так и для правоохранительных структур, в том числе МВД России. СЦ создаются не только в центральном аппарате, но и в управлениях МВД по субъектам Российской Федерации, где в целях принятия коллективного наиболее правильного решения проходят совещания, подводятся итоги работы, разбираются сложные ситуации.

СЦ позволяют реализовать новый формат управления. В них создается особое информационное пространство для эффективного мониторинга, прогнозирования, принятия решений и контроля за их исполнением.

Основными предпосылками создания СЦ являются:

1) усложнение и расширение круга задач управления, решаемых руководителями высшего звена.

Руководителям все чаще приходится принимать взвешенные решения при жестком дефиците времени. При выработке решений требуется всесторонне оценивать возможные риски достижения целей при различных вариантах развития ситуации, включая конфликтные;

2) увеличение объемов поступающей информации, способов ее представления и обработки.

Лицу, принимающему решения, очень важно быстро получать информацию по запросу как в обобщенном виде, так и с необходимой детализацией. Она может поступать в режиме реального времени с различной степенью достоверности. Поэтому ее поиск, извлечение и обработка требуют согласованной работы всего состава СЦ;

3) повышение требований к оперативности принятия и реализации управленческих решений.

Сегодня критическими параметрами управления являются скорость реакции на быстрое изменение обстановки и высокая степень ответственности за результат. Для успешного выполнения решений также требуется отлаженное взаимодействие с подчиненными, вышестоящими и внешними структурами с помощью современных технологических средств.

Современные СЦ позволяют руководителям успешно решать *различные задачи контроля и управления* как в штатных, так и в кризисных ситуациях. Прежде всего это:

1) сбор информации по заданным критериям из различных источников, ее обработка и хранение;

2) мониторинг обстановки (состояния объекта управления) и представление руководителю обобщенной и детализированной информации;

3) прогнозирование развития ситуации на основе поступающей информации и выбор лучшего варианта управляющего воздействия после оценки достоверности прогноза, возможных рисков и других параметров или, иными словами, моделирование последствий управленческих решений на базе использования информационно-аналитических систем;

4) управление в кризисной ситуации, планирование, координация и контроль исполнения принятых решений;

5) экспертная оценка и оптимизация решений.

Основу логической модели типового СЦ составляют подсистемы ситуационного анализа, поддержки принятия решения и управления.

Подсистема ситуационного анализа решает такие задачи:

1) сбор, обработка данных от источников информации на основе формализованных сигналов тревоги, оповещения и сообщений;

2) ситуационная оценка информации, в процессе которой заполняется формуляр критической ситуации;

3) идентификация угроз по совокупности признаков, выявление основных характеристик угрозы;

4) разработка сценария развития кризисной ситуации.

Далее на основе разработанной модели развития кризисной ситуации в рамках *подсистемы поддержки принятия решения и управления* выполняются следующие задачи:

1) анализируются возможности и выбирается типовой сценарий применения сил и средств обеспечения безопасности (подразделений МЧС, МВД, ФСБ России, Росгвардии и др.);

2) осуществляется его доработка до реального и организуется выполнение принятого решения;

3) в соответствии с принятым решением подаются информационные сообщения, указания и команды силам и средствам, участвующим в мероприятиях по разрешению ситуаций;

4) в режиме реального времени принимаются все сообщения и доклады о развитии критической ситуации, осуществляется оперативное управление.

В числе *типовых элементов технического оснащения* таких центров выделяют:

- экран коллективного пользования для мультиэкранного отображения данных различного вида (видеоизображений, электронных карт, графиков, диаграмм, текстовой информации и т.д.);
- средства видео-конференц-связи, обеспечивающие проведение коллективных совещаний с удаленными пользователями, участвующими в обсуждении;
- систему звуковой связи для проведения групповых обсуждений;
- вспомогательное оборудование ввода и отображения графических данных (интерактивные доски, документ-камеры);
- интегрированные системы управления, отвечающие за взаимодействие всех элементов технического оснащения.

Что касается сферы образовательной деятельности, то в ней нашли применение *учебные СЦ*.

Применение новых технологий, используемых в СЦ, является очередным шагом на пути повышения качества образовательного процесса, соответствующего модернизации образования в стране.

Сегодня учебные СЦ имеются не везде. Такие центры действуют в Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Московском государственном институте международных отношений и ряде других организаций.

Характеризуя их, нужно сказать, что они могут носить универсальный и направленный характер. В первом случае центры предназначены для получения общих навыков работы с технологиями, программным и аппаратным обеспечением. Во втором случае либо дублируют существующий рабочий аналог, либо позволяют изучить отдельные транспортируемые компоненты (например, программное обеспечение).

Кроме того, действующие СЦ могут выступать в качестве учебных за счет использования специального «холостого» (тренировочного) режима.

Сосредоточение в учебных СЦ указанных выше типов ресурсов и средств позволяет образовательным организациям, включая ведомственные, использовать их:

- для поддержки разнообразных активных форм проведения занятий;
- обучения использованию современных информационных, аналитических и технологических средств;
- проведения деловых игр и стендовой отработки интеллектуальных ИТ;
- создания рабочих прототипов технологий, например, ОВД.

В Дальневосточном юридическом институте МВД России, например, СЦ является основным сегментом многофункционального информационно-аналитического центра (см. об этом в подразд. 3.4).

В заключение отметим, что *управление по ситуации является одним из ключевых направлений повышения эффективности управления в ОВД*. И оно в полной мере реализуется через использование СЦ, которые, повторимся, обеспечивают процесс управления средствами для эффективного мониторинга, прогнозирования, принятия решений и контроля за их исполнением.

С учетом сказанного цель создания СЦ в любой сфере — повышение эффективности и качества управленческих решений, предотвращение и устранение кризисных и чрезвычайных ситуаций. Обязательным условием работы СЦ является информационно-аналитическая поддержка процедур и процессов, позволяющих оперативно анализировать, моделировать, прогнозировать сценарии развития ситуации и динамично вырабатывать эффективные решения.

Контрольные вопросы

1. Какие из свойств управленческой информации можно назвать одними из самых важных?

2. В чем заключается основная функция любой системы управления?

3. Что относится к основным компонентам информационной системы ОВД?

4. Какой из этапов информационного обеспечения управления позволяет ответить на вопрос «Почему так происходит»?

5. Что является основным недостатком системы информационного обеспечения ОВД, негативно влияющим на эффективность взаимодействия сотрудников?

6. Какие подсистемы выделяют в архитектуре ИСОД МВД России?

7. Какие возможности ЦОД обеспечивают повышение эффективности принятия решений?

8. Существуют ли направления развития ИТ, альтернативные ИСОД МВД России?

9. Какие информационные задачи могут быть решены в дежурных частях ОВД на основе применения аналитических средств класса BI?

10. В чем состоят основные отличия моделей предоставления услуг в рамках облачных технологий?

11. Какие свойства облачных вычислений отвечают требованиям, предъявляемым к информационному обеспечению ОВД?

12. В чем состоят основные преимущества цифровых систем видеонаблюдения по сравнению с аналоговыми?

13. Возможно ли с помощью подсистемы видеоаналитики обеспечить сопровождение объекта наблюдения по маршруту движения?

14. Какие требования предъявляются к составляющим системы видеонаблюдения?

15. В чем заключается основное преимущество ГИС по сравнению с традиционными цифровыми картами?

16. Каким объектам деятельности ОВД могут соответствовать слои ГИС?

17. Какие задачи контроля и управления в штатных и кризисных ситуациях позволяют решать современные ситуационные центры?

18. Какие задачи решает подсистема ситуационного анализа типового ситуационного центра?

ГЛАВА 2.
ОСНОВЫ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

2.1. Понятие, принципы работы информационно-телекоммуникационных сетей. Создание и развитие интегрированной мультисервисной телекоммуникационной сети МВД России

При физическом соединении двух или более компьютеров образуется **компьютерная сеть**. В общем случае для ее создания необходимо специальное аппаратное обеспечение (*сетевое оборудование*) и специальное программное обеспечение (*сетевые программные средства*).

Все компьютерные сети без исключения имеют одно назначение — обеспечение совместного доступа к общим ресурсам. Слово *ресурс* — очень удобное. В зависимости от назначения сети в него можно вкладывать тот или иной смысл. Ресурсы бывают трех типов: 1) аппаратные, 2) программные, 3) информационные.

Например, устройство печати (принтер) — это *аппаратный ресурс*, точно так же, как объемы информации, записываемой на жесткие диски. Когда все участники небольшой компьютерной сети пользуются одним общим принтером, это значит, что у них общий аппаратный ресурс. То же можно сказать и о сети, имеющей один компьютер с увеличенной емкостью жесткого диска (*файловый сервер*), на котором все участники сети хранят архивы и результаты работы.

Кроме аппаратных ресурсов компьютерные сети позволяют совместно использовать *программные ресурсы.* Так, например, для выполнения очень сложных и продолжительных расчетов можно подключиться к удаленному высокопроизводительному компьютеру (суперкомпьютеру) и отправить вычислительное задание на выполнение, а по окончании расчетов таким же образом получить результат обратно.

Данные, хранящиеся на удаленных компьютерах, образуют *информационный ресурс.* Роль этого ресурса сегодня видна наиболее ярко на примере Интернета, который воспринимается прежде всего как гигантская информационно-справочная система.

Однако деление ресурсов на аппаратные, программные и информационные достаточно условно. На самом деле, при работе в компьютерной сети любого типа одновременно происходит совместное использование всех типов ресурсов. Так, например, обращаясь к удаленной справочной системе, базе данных или учету, мы, безусловно, используем аппаратные средства других компьютеров, на которых работают специальные программы, обеспечивающие обработку и поставку затребованных нами данных.

Для обеспечения необходимой совместимости как по аппаратуре, так и по программам в компьютерных сетях действуют специальные стандарты, называемые *протоколами.* Они определяют характер аппаратного взаимодействия компонентов сети (*аппаратные протоколы*) и характер взаимодействия программ и данных (*программные протоколы*). Физически функции поддержки протоколов исполняют аппаратные устройства (*интерфейсы*) и программные средства (*программы поддержки протоколов*).

В соответствии с используемыми протоколами компьютерные сети принято разделять на локальные (*LAN* — local area network) и глобальные (*WAN* — wide area network). Компьютеры *локальной сети* преимущественно используют единый комплект протоколов для всех участников. По территориальному признаку локальные сети отличаются компактностью. Они могут объединять компьютеры одного помещения, этажа, здания, группы рядом расположенных сооружений. *Глобальные сети* имеют, как правило, большие с точки зрения географии соединений размеры. Они могут объединять как отдельные компьютеры, так и отдельные локальные сети, в том числе и использующие различные протоколы.

Группы сотрудников, работа которых требует обмена данными и совместного использования информации в рамках локальной сети, называются *рабочими группами.* В рамках одной локальной сети их может быть несколько. У участников рабочих групп могут быть разные права доступа к общим ресурсам сети. Совокупность приемов разделения и ограничения прав участников компьютерной сети — это *политика сети.* Управление сетевой политикой (которая может различаться в одной сети) понимается как *администрирование сети.* Лицо, управляющее организацией работы участников локальной компьютерной сети, — это *системный администратор.*

Создание локальных сетей характерно для отдельных подразделений или небольших территориальных органов. Если подразделение (или территориальный орган) занимает большую территорию, то отдельные локальные сети могут объединяться в глобальные с помощью любых традиционных каналов связи (кабельных, спутниковых, радиоканалов и т. п.).

Для связи нескольких локальных сетей, работающих по разным протоколам, служат специальные средства, называемые *шлюзами.* Шлюзы могут быть как аппаратными, так и программными. Например, это может быть специальное устройство (*шлюзовый сервер*), а может быть и компьютерная программа (*шлюзовое приложение*). В последнем случае компьютер может выполнять не только функцию шлюза, но и какие-то иные функции, типичные для рабочих станций.

При подключении локальной сети подразделения к глобальной сети важную роль играет понятие *сетевой безопасности.* В частности, должен быть ограничен доступ в локальную сеть для посторонних лиц извне, а также выход за пределы локальной сети для сотрудников подразделения, не имеющих соответствующих прав. Для решения проблемы сетевой безопасности между локальной и глобальной сетью устанавливают так называемый *брандмауэр.* Это может быть специальный компьютер или компьютерная программа, препятствующая несанкционированному перемещению данных между сетями.

Все компьютерные сети работают в одном принятом для них стандарте — **стандарте OSI — Open Systems Interconnection** (взаимодействие открытых систем).

Как людям, чтобы взаимодействовать, нужен общий язык, так и компьютерам, объединенным в сеть, для взаимодействия требуются соответствующие средства. Для единого представления данных в линиях связи, по которым передается информация, Международной организацией по стандартизации (англ. ISO — International Standards Organization) в 1984 г. была разработана базовая модель OSI. Эта модель является международным стандартом для передачи данных. Она содержит семь уровней (рис. 2.1).

Каждый уровень имеет заранее заданный набор функций, которые он должен выполнять, чтобы связь могла состояться [78].

Рис. 2.1. Уровни стандарта OSI

Уровень 7 (уровень приложений). Это самый близкий к пользователю уровень модели OSI. Он отличается от других тем, что не предоставляет услуги ни одному другому уровню модели OSI и только обслуживает прикладные процессы, находящиеся вне пределов модели. Примерами таких прикладных процессов могут служить программы работы с электронными таблицами, текстовые процессоры и программы работы банковских терминалов.

Уровень приложений идентифицирует и устанавливает доступность предполагаемых партнеров для связи, синхронизирует совместно работающие прикладные программы, а также устанавливает договоренность о процедурах восстановления после ошибок и контроля целостности данных.

Уровень приложений также определяет степень достаточности ресурсов для налаживания предполагаемой связи.

Уровень 6 (уровень представлений). Отвечает за то, чтобы информация, посылаемая из уровня приложений одной системы, была читаемой для уровня приложений другой системы. При необходимости уровень преобразовывает форматы данных путем использования общего формата представления информации.

Уровень 5 (сеансовый уровень). Как указывает его название, сеансовый уровень устанавливает сеансы взаимодействия приложений, управляет ими и завершает их. Сеансы состоят из диалога между двумя или более объектами представления. Сеансовый уровень синхронизирует диалог между объектами уровня представлений и управляет обменом информации между ними. В дополнение к основным функциям сеансовый уровень предоставляет средства для синхронизации участвующих в диалоге сторон, обеспечивает класс услуг и средства формирования отчетов об особых ситуациях, возникающих на сеансовом уровне, а также на уровнях приложений и представлений.

Уровень 4 (транспортный уровень). Сегментирует и повторно собирает данные в один поток. Если уровень приложений, сеансовый уровень и уровень представлений заняты прикладными вопросами, то четыре нижних уровня решают задачу транспортировки данных. Транспортный уровень пытается обеспечить услуги по транспортировке данных таким образом, чтобы скрыть от верхних уровней детали процесса передачи данных. В частности, задачей транспортного уровня является решение таких вопросов, как выполнение надежной транспортировки данных через многосетевой комплекс. Предоставляя надежные услуги, транспортный уровень обеспечивает механизмы для установки, поддержания и упорядоченного завершения действия виртуальных каналов, обнаружения и устранения неисправностей транспортировки, а также управления информационным потоком (с целью

предотвращения переполнения одной системы данными от другой системы).

Уровень 3 (сетевой уровень). Это комплексный уровень, обеспечивающий соединение и выбор маршрута между двумя конечными системами, которые могут находиться в сетях разных географических точек.

Уровень 2 (канальный уровень). Обеспечивает надежный транзит данных через физический канал. Выполняя эту задачу, канальный уровень решает вопросы физической адресации (в противоположность сетевой или логической адресации), топологии сети, дисциплины в канале связи (то есть отвечает за то, каким образом конечная система использует сетевой канал), уведомления об ошибках, упорядоченной доставки кадров, а также вопросы управления потоком данных.

Уровень 1 (физический уровень). Определяет электротехнические, механические, процедурные и функциональные характеристики активизации, поддержания и деактивации физического канала между конечными системами, то есть такие характеристики, как уровни напряжения, временные параметры изменения напряжения, скорость физической передачи данных, максимальные расстояния передачи информации, физические разъемы и др.

Развитие сетевых технологий, доступность и широкое распространение телекоммуникационных и технологических решений позволяют создавать на их основе большие внутриведомственные сети, а также обеспечивать соответствующий режим защиты внутриведомственной информации. Такой способ организации сети получил название **интранет (intranet)**.

Итак, *интранет* — это та же глобальная компьютерная сеть, но организованная и работающая в рамках отдельной организации (корпорации, ведомства). Именно поэтому его и называют современной корпоративной сетью.

Существуют различные типы сервисов (услуг) и ресурсов, которые могут обеспечиваться в интранете.

Почтовые сервисы. Интранет предоставляет возможность организовать для пользователей корпорации функционирование электронной почты.

Файловые сервисы. При наличии в корпоративной сети выделенного файл-сервера появляется возможность организации приема/передачи файлов между пользователями интранета.

Web-сервисы. Самый популярный вид в рамках интранета. Ради возможности использования данного сервиса внутри большой организации и началось развитие интранет-сетей. Web-сервис может обеспечиваться в корпорации или отдельным web-сервером, или уже существующим файловым сервером. Для эффективной работы необходимо программное обеспечение web-сервера.

Аудиосервис. Одним из преимуществ интранета является надежность и доступность сетевого диапазона. Это дает возможность предоставления, например, таких услуг, как передача аудиоданных по сети или услуг IP-телефонии.

Видеосервис. Для организации в интранете качественного видеосервиса необходимо выделение специального видеосервера. Видеосервис не ограничен диапазоном интранета. Видеосерверы могут поддерживать несколько видеопотоков, что обеспечивает реализацию видеоконференц-связи.

Еще одна особенность интранета состоит в том, что данная сеть *позволяет объединять компьютеры с различными аппаратными платформами и различными операционными системами*. Это в сочетании с перечисленными достоинствами интранет-сетей определяет их перспективность для массового использования в различных организациях, в том числе и в правоохранительных органах.

На протяжении всего периода информатизации ОВД с начала 1990-х предпринимались не всегда успешные попытки объединить отдельные компьютеры и локальные сети подразделений в единую корпоративную сетевую инфраструктуру.

С 2005 г. в МВД России стали проводить **комплекс мероприятий по созданию единой современной информационно-телекоммуникационной инфраструктуры информационного обеспечения ОВД**. Она была призвана способствовать повышению эффективности деятельности ОВД по защите прав и свобод граждан, соблюдению законности, правопорядка и общественной безопасности путем реконструкции и оборудования объектов ОВД новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий.

В 2009 г. была утверждена *Концепция информатизации органов внутренних дел Российской Федерации и внутренних войск МВД России до 2012 года*, на основании которой началось формирование интегрированных банков данных. Они включают централизованные оперативно-справочные, криминалистические и разыскные учеты, банки биометрической, статистической, научно-технической и архивной информации, ориентированные на использование подразделениями ОВД, а также интегрируются с помощью сетевых технологий в информационные ресурсы специального назначения, ориентированные на использование в подразделениях ОВД по направлениям оперативно-служебной деятельности [26].

К настоящему времени в ОВД создана и успешно функционирует *единая целостная информационно-телекоммуникационная инфра-*

структура, которая обладает требуемым комплексом современных технических и технологических возможностей и включает:

1) инфраструктуру единого информационного пространства системы МВД России, которая к настоящему времени успешно трансформировалась в ИСОД МВД России;

2) ИМТС МВД России;

3) автоматизированные интегрированные и распределенные банки данных общего пользования;

4) развитую инфраструктуру информационной безопасности.

Единое информационное пространство в МВД России создавалось на основе использования принципов сервисно ориентированной архитектуры построения информационных систем. Это позволило размещать информацию на общедоступных для пользователей средствах, иными словами, в виде информационных программных и аппаратных сервисов ИСОД МВД России.

Пройдя достаточно сложный период формирования, **телекоммуникационная составляющая ИМТС МВД России** к настоящему времени стала играть ключевую роль в информационном обеспечении ОВД.

Сегодня ИМТС МВД России *является важнейшим элементом ИСОД МВД России*, представляя собой универсальную телекоммуникационную транспортную среду, позволяющую обеспечить взаимодействие компонентов единой системы информационно-аналитического обеспечения деятельности в целях предоставления комплекса услуг связи подразделениям системы МВД России.

Структура ИМТС МВД России представляет собой совокупность коммутационных и опорных узлов, узлов мультисервисной транспортной сети ОВД, каналов передачи данных.

В структуру входят следующие элементы:

1) главный коммуникационный узел;

2) опорные коммутационные узлы ИМТС МВД России федеральных округов Российской Федерации;

3) региональные коммутационные узлы ИМТС МВД России территориальных органов МВД России на региональном уровне [29].

Взаимодействие главного, опорных и региональных коммутационных узлов осуществляется с использованием магистральных каналов передачи данных по радиальному принципу.

В местах, где организация каналов связи по каким-то причинам невозможна, применяется сеть спутниковой связи ОВД. Такая сеть является составной частью ИМТС МВД России, построена на базе геостационарных спутников-ретрансляторов, состоит из центральной земной станции спутниковой связи и спутниковых терминалов, установленных по месту дислокации ОВД.

Физическая основа ИМТС МВД России — транспортная среда. Она представляет собой сеть передачи данных и распределения локальных вычислительных сетей.

Компонентами ИМТС МВД России выступают:

- компьютеры разных типов;
- системное и прикладное программное обеспечение;
- мультиплексоры, концентраторы, коммутаторы и маршрутизаторы;
- волоконно-оптические и медные кабельные системы;
- радиосистемы передачи данных.

К магистральному и межрегиональному компонентам транспортной среды относится сеть из коммуникационных узловых центров, обеспеченных высокопроизводительным и отказоустойчивым телекоммуникационным оборудованием.

Организуются магистральные цифровые каналы путем:

- заключения договоров на оказание услуг (аренды каналов) в системе цифровых территориально распределенных наземных магистралей;
- создания наложенных цифровых сетей связи на базе существующих телефонных сетей общего пользования;
- строительства цифровых линий связи с применением волоконно-оптических линий связи, радиорелейных средств;
- заключения соответствующих договоров на оказание услуг спутниковой связи.

Магистральная сеть передачи данных — это сеть с коммуникацией пакетов. Опыт и многочисленные исследования показали, что для пульсирующего компьютерного трафика метод коммутации пакетов дает наилучшие результаты по показателю наибольшей общей производительности сети при удовлетворительном качестве.

Первичная структура каналов связи организуется на базе первичной сети коммутаторов цифровых каналов на уровне региональных коммутационных узлов. Локальные вычислительные сети являются распределенной транспортной средой в пределах административного здания. Применяемая в них технология Ethernet (до 1 000 Мбит/с) предполагает использование различных типов оборудования и предъявляет различные требования к структурированным кабельным системам. Вариантами их могут быть как оптоволоконные, так и медные кабельные системы.

Локальные вычислительные сети проектируются и строятся с учетом требований и рекомендаций, указанных в стандартах, описывающих используемые технологии, в целях обеспечения максимальной пропускной способности сети, равномерности распределения трафика, рационального использования ресурсов, возможности доступа к разделяемому ресурсу магистральной сети передачи данных.

Система управления включает в себя специализированное и общесистемное программное обеспечение различных уровней. Оконечные средства передачи данных ИМТС МВД России представляют собой аппаратные комплексы, замыкающиеся на каналы связи и поддерживающие необходимые для функционирования ИМТС МВД России протоколы, интерфейсы и стандарты.

Отдельным направлением ИМТС МВД России является организация мобильного доступа сотрудников ОВД, входящих в состав нарядов патрульно-постовой службы полиции, дорожно-патрульной службы ГИБДД МВД России, участковых уполномоченных полиции к информационным ресурсам ИСОД МВД России с использованием сетей операторов связи поколения 3G/4G либо систем спутниковой связи.

Доступ к информации, поступающей со средств видеонаблюдения и контроля, предоставляется дежурным частям территориальных подразделений МВД России. Если такие средства не находятся на балансе подразделений МВД России, можно организовать путь к ним посредством шлюза между ИМТС МВД России и узлом подключения этих средств на основании соглашений, заключаемых с балансодержателями.

Для *организации внешнего голосового взаимодействия МВД России с гражданами и организациями* обеспечивается шлюз между ИМТС МВД России и телефонной сетью общего пользования Российской Федерации. Несколько иная технология применяется для организации *внешнего информационного взаимодействия МВД России с гражданами и организациями*. Оно обеспечивается защищенным шлюзом между ИМТС МВД России и информационно-телекоммуникационной сетью Интернет.

В заключение следует отметить, что сетевые компьютерные технологии стали неотъемлемой составляющей современных ИТ. Практически все государственные структуры, в том числе и ОВД, имеют в распоряжении ведомственные телекоммуникационные системы, работа которых невозможна без сетевой инфраструктуры.

ИМТС МВД России в полной мере обеспечивает доступ к ведомственным информационным ресурсам. Разработка, внедрение и дальнейшее развитие ИСОД МВД России стали возможны только на основе соответствующей системы телекоммуникаций, которой, безусловно, является ИМТС МВД России.

2.2. 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 информа-

ционно-аналитического обеспечения деятельности МВД России в 2012—2014 годах», или ИСОД МВД России, было принято решение о создании единой информационной системы ЦОД для информационно-аналитической поддержки деятельности подразделений МВД России [28].

О **причинах создания и месте ИСОД МВД России** в информационном обеспечении деятельности ОВД мы уже говорили в подразд. 1.3, но считаем необходимым еще раз акцентировать на этом внимание.

Напомним, что одной из основных причин было отсутствие единых архитектурных решений и системного подхода к внедрению автоматизированных систем.

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 [65].

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

- организовывать электронное взаимодействие между ними и предоставлять разграничений доступ 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 [28].

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) ИМТС МВД России (см. подразд. 2.1);

2) подсистема базового информационно-технологического обеспечения, включающая в свой состав подсистему 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 [28].

Подсистемы 3—8 имеют непосредственное отношение к пользователю и реализуются в составе прикладных сервисов ИСОД [9; 10; 12—18; 22; 24].

Прикладные сервисы ИСОД МВД России представлены на рис. 2.2.

Рис. 2.2. Состав прикладных сервисов ИСОД МВД России

1. *Прикладные сервисы обеспечения повседневной деятельности подразделений МВД России* — это шесть сервисов:

1) СЭП — сервис электронной почты МВД России. 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) СЭД — сервис электронного документооборота. 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) СВКС—М — сервис видео-конференц-связи МВД России. Предназначен для оптимизации и ускорения процесса получения и обработки информации для принятия управленческих решений, а также оперативной связи между сотрудниками МВД России;
4) СУДИС — сервис управления доступом к информационным системам и ресурсам. Необходим для централизованного управления доступом пользователей и сервисов к сервисам ИСОД МВД России;
5) ВИСП — ведомственный информационно-справочный портал.

Обеспечивает:

- доступ сотрудников к внутренней ведомственной информации, связанной с ИСОД МВД России;
- доступ сотрудников к сведениям об организационно-штатной структуре МВД России;
- доступ сотрудников к адресно-телефонному справочнику МВД России;
- информирование сотрудников о мероприятиях, связанных с ИСОД МВД России [84].

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 Интернета 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.

2. *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 (см. о нем подробнее ниже);
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 ресур-

су ИСОД МВД России [84]. 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. Здесь можно отметить, что технологической особенностью является создание облачной архитектуры, особенности которой мы рассматривали в подразд. 1.3.

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 центров обработки данных. 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.

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* (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. 2.3).

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.

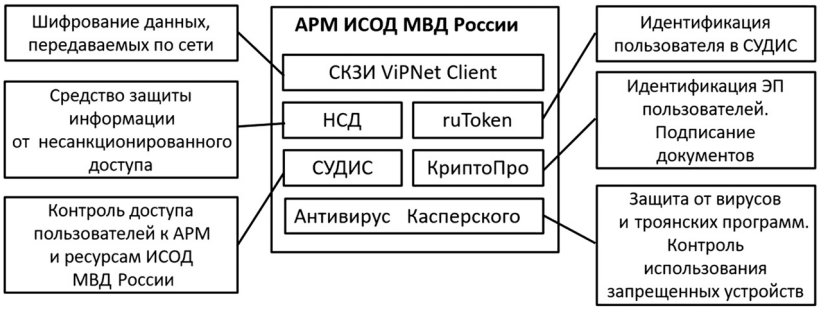


Рис. 2.3. Состав системы защиты АРМ ИСОД МВД России

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 [См. подробнее: 80] 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 [85].

Рутокен (ruToken) [См. подробнее: 83] 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 (СКЗИ) ViPNet Client [См. подробнее: 88] 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 центра обработки данных МВД России и развернуты центры управления региональными защищенными сетями.

В качестве иллюстрации основных принципов построения и базовых технологий использования прикладных сервисов остановимся на наиболее популярных. Это один из сервисов обеспечения повседневной деятельности — СЭД, а также один из сервисов обеспечения оперативно-служебной деятельности — специальное программное обеспечение ФИС ГИБДД-М.

1. *Сервис электронного документооборота (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 (SOA). *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 [84].

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 авторизации в зависимости от роли пользователя (руководитель, делопроизводитель, исполнитель) предлагается выбор одного из документационных сервисов. Так, при запуске сервиса «Документы», который предназначен для обработки данных о регистрационных карточках документов, на экране отображается пользовательский интерфейс прикладного сервиса (рис. 2.4).

При выборе конкретного документа в журнале документов отображается полная информация о документе (рис. 2.5).

Порядок работы с сервисом соответствует особенностям организации делопроизводства, изложенным в Инструкции по делопроизводству в органах внутренних дел Российской Федерации, утвержденной приказом МВД России от 26 июня 2012 г. № 615. СЭД может быть использован только для управленческой (административной) деятельно-

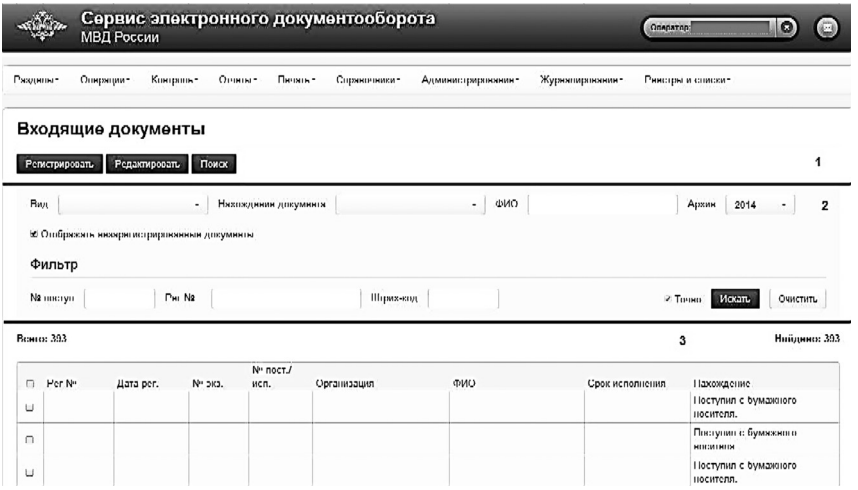


Рис. 2.4. СЭД. Интерфейс пользователя для сервиса «Документы», раздел «Входящие документы»

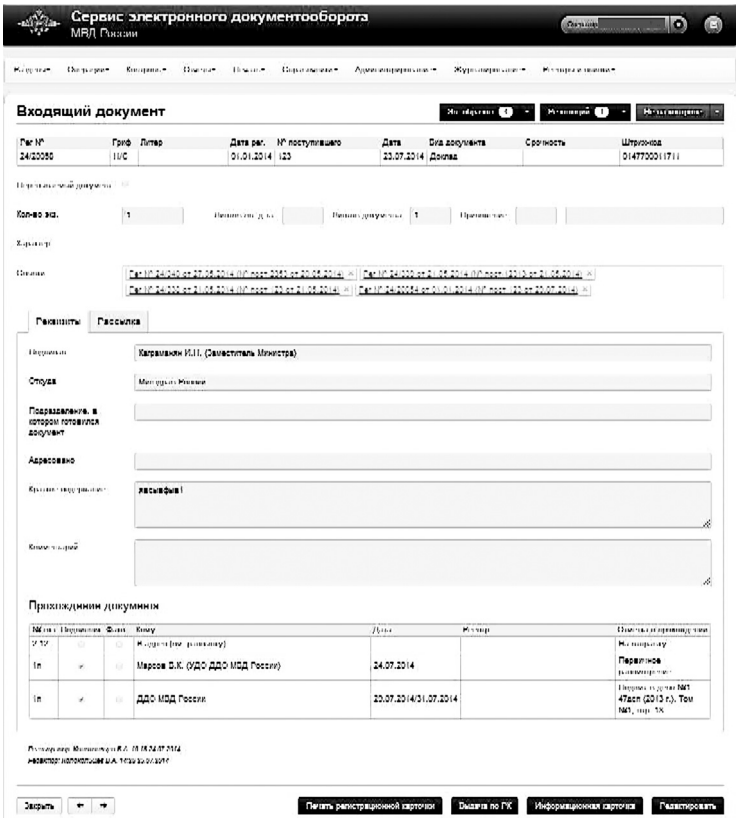


Рис. 2.5. СЭД. Регистрационно-контрольная форма входящего документа

сти подразделений ОВД, связанных с документационным обеспечением ОВД и представлением юридического значимого документооборота.

2. *Сервис специального программного обеспечения Федеральной информационной системы Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации (ФИС ГИБДД-М).*

Это специальное программное обеспечение было 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 [22].

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.

После авторизации в сервисе появляется стартовое окно (рис. 2.6).

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

Рис. 2.6. Стартовое окно ФИС ГИБДД-М

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 (рис. 2.7).

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 [84], где для каждого сервиса в разделе «Документы» представлены подробные инструкции и регламенты по использованию всех видов программного обеспечения.

Конечно, развитие и совершенствование сетевой инфраструктуры ИСОД в части, относящейся к ИМТС МВД России, продол жается и основывается на передовых технологиях, учитывающих **основные принципы построения и объединения телекоммуникационных сетей**, как технические, так и экономические.

К ним относятся:

1) *принцип структурности* — разбиение телекоммуникационных систем на части и подсистемы, каждая из которых выполняет

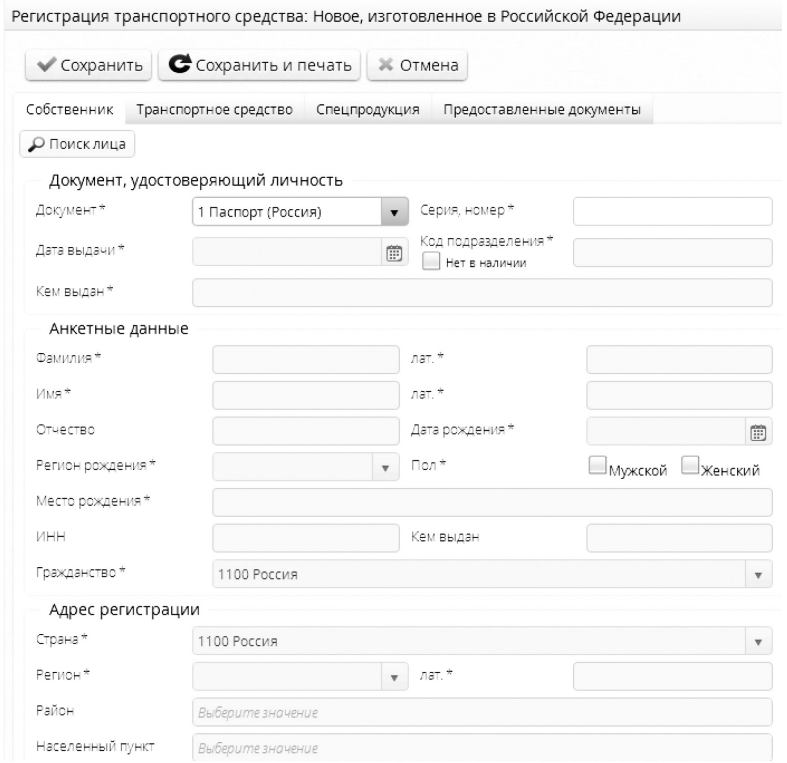


Рис. 2.7. Форма для ввода данных о собственнике при регистрации транспортного средства

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 [78].

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.

Проведенные авторами пособия научные исследования позволили определить первоочередные направления, к которым можно отнести:

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.

2.3. Особенности построения аппаратно-программного комплекса «Безопасный город» на базе современной информационно-коммуникационной инфраструктуры

Актуальность обеспечения комплексной безопасности города в части обеспечения правопорядка — сферы деятельности ОВД — связана с угрозами террористических действий, возрастанием активности преступных формирований, а также с негативной тенденцией роста дорожно-транспортных происшествий, квартирных краж, угонов автомобилей.

Сегодня в рамках развития системы обеспечения общественной безопасности, правопорядка и безопасности среды обитания в муниципальных образованиях внедрены различные АПК, в целом справляющиеся с решением возложенных на них задач, демонстрируя высокую эффективность.

Одна из моделей системы «Безопасный город», разработанная МВД России, формировалась на базе уже функционировавших в различных российских регионах отдельных элементов и комплексов. Эта *модель представляет собой масштабную сложноорганизованную систему безопасности на универсальной программно-аппаратной платформе*.

Так, например, первая попытка внедрения в Хабаровском крае (г. Хабаровске) АПК «Безопасный город» в виде комплексной автоматизированной информационно-аналитической системы [30] показала на практике эффективность выполнения *главной задачи* — предоставления лицам, принимающим решения, эффективного инструмента управления вверенными силами и средствами с возможностью контроля за выполнением руководящих указаний.

В настоящее время МВД России активно взаимодействует с федеральными органами исполнительной власти и органами государственной власти субъектов Российской Федерации в части выработки общих подходов для построения и развития современной информационно-коммуникационной инфраструктуры технических средств АПК «Безопасный город» [25].

Длительное время отсутствовал единый концептуальный подход к реализации мероприятий по созданию и развитию АПК «Безопасный город», до конца не был выработан и закреплен в документах федерального уровня. Предлагались или проектные решения в рамках концепций определенного сегмента (например правоохранительного), или в рамках отдельных аспектов концепций, действовавших в субъектах Российской Федерации и учитывавших только специфику региона без единых, унифицированных требований. Кроме этого, в ходе эксплуатации АПК отмечались затруднения, возникавшие при информационном взаимодействии между ведомствами, использующими данные комплексы. Основной причиной такой ситуации прежде всего было отсутствие правил, стандартов и средств для взаимодействия [57].

Ситуация изменилась после принятия постановления Правительства Российской Федерации от 20 января 2014 г. № 39 «О Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств ″Безопасный город″» [5].

11 февраля 2014 г. прошло первое заседание комиссии, по итогам которого были определены 17 пилотных регионов для развертывания систем АПК «Безопасный город».

К настоящему времени разработана **Концепция построения и развития аппаратно-программного комплекса «Безопасный город»** [7] на период до 2020 г.

Согласно базовому положению этого документа, *основными задачами построения и развития АПК «Безопасный город»* являются:

1) формирование коммуникационной платформы для органов местного самоуправления с целью устранения рисков обеспечения общественной безопасности, правопорядка и безопасности среды обитания на базе межведомственного взаимодействия;

2) разработка единых функциональных и технических требований к аппаратно-программным средствам, ориентированным на идентификацию потенциальных точек уязвимости, прогнозирование, реагирование и предупреждение угроз обеспечения безопасности муниципального образования;

3) обеспечение информационного обмена между участниками всех действующих программ соответствующих федеральных органов исполнительной власти в области обеспечения безопасности через единое информационное пространство с учетом разграничения прав доступа к информации разного характера;

- обеспечение информационного обмена на федеральном, региональном и муниципальном уровнях через единое информационное пространство с учетом разграничения прав доступа к информации разного характера;

4) создание дополнительных инструментов на базе муниципальных образований для оптимизации работы существующей системы мониторинга состояния общественной безопасности;

5) построение и развитие систем ситуационного анализа причин дестабилизации обстановки и прогнозирования существующих и потенциальных угроз для обеспечения безопасности населения муниципального образования [7].

Для решения указанных задач предназначена информационно-коммуникационная инфраструктура комплекса «Безопасный город». Она простроена по *модульному принципу* с возможностью включения в единый контур управления и информационного обмена (от муниципального до федерального уровня) элементов уже существующей инфраструктуры муниципальных образований в рамках реализации федеральными органами исполнительной власти собственных программ, обеспечивающих общественную безопасность, правопорядок и безопасность среды обитания.

Современная инфраструктура АПК «Безопасный город» *базируется на единых* для всех муниципальных образований *функциональных и технических требованиях к компонентам комплекса и форматах обмена данными* между ее элементами.

Инфраструктура АПК строится из *отдельных инфраструктурных элементов каждого из уровней* (муниципального, регионального, федерального) и включает:

1) телекоммуникационную инфраструктуру, предназначенную для обеспечения процессов передачи информации между территориально распределенными компонентами АПК «Безопасный город»;

2) комплекс периферийных устройств: оконечные устройства, аппаратное и программное обеспечение, телекоммуникационное оборудование, дающие возможность приема, распределенной обработки и передачи данных;

3) информационно-вычислительную инфраструктуру: интеграционную платформу обмена данными, интеграционную платформу управления видеопотоками, геоинформационную интеграционную платформу, единую систему электронного документооборота и контроля поручений, систему обработки и хранения данных, прикладные функциональные системы, предназначенные для обеспечения эффективного решения управленческих задач пользователей, пользовательские прикладные информационные решения;

4) инженерную инфраструктуру, предназначенную для обеспечения устойчивого функционирования компонентов комплекса «Безопасный город»;

5) комплекс информационной безопасности, в состав которого входят аппаратные и программные средства защиты информации, мониторинга качества каналов и услуг связи.

Главным *координатором* по вопросам внедрения и развития АПК «Безопасный город» в субъектах Российской Федерации, а также главным распорядителем бюджетных средств, направленных на реализацию Концепции построения и развития, на федеральном уровне является МЧС России. МВД России, согласно этому документу, может являться *соисполнителем* мероприятий по построению и развитию АПК «Безопасный город» на федеральном уровне.

Согласно приказу МВД России от 9 декабря 2015 г. № 1149 «Об организационных мероприятиях по участию органов внутренних дел Российской Федерации в создании и развитии аппаратно-программного комплекса ″Безопасный город″» некоторые структурные подразделения центрального аппарата МВД России обеспечивают взаимодействие на постоянной основе с территориальными органами (подразделениями) федеральных органов исполнительной власти, органами государственной власти субъектов Российской Федерации и органами местного самоуправления, субъектами транспортной инфраструктуры, общественными объединениями и организациями по вопросам создания и развития правоохранительного сегмента АПК «Безопасный город» [25].

Следует отметить, что МВД России к тому времени уже был накоплен достаточный опыт развертывания необходимых компонентов (подсистем) для создания безопасной городской инфраструктуры и обеспечения общественной безопасности и правопорядка на территории муниципального образования в рамках реализации соответствующих программ субъектами Российской Федерации [30]. Поэтому 17 января 2017 г. на одном из заседаний рабочей группы для обеспечения рабочего взаимодействия при реализации плановых мероприятий работы Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город», было решено, что МВД России и ФСБ России, в том числе с учетом имеющегося опыта, представят предложения по разработке единых методических рекомендаций в части внедрения систем правоохранительного сегмента АПК «Безопасный город» [40].

Кроме того, в 2015—2016 гг. в рамках работы Межведомственной комиссии МЧС России, совместно со всеми федеральными органами исполнительной власти выработали комплекс научных, организационных и методических документов по реализации АПК «Безопасный город» [31; 34; 37; 39].

С учетом отмеченных в документах положений **архитектура АПК** может быть представлена следующим образом.

Функциональная структура АПК «Безопасный город» включает в себя, как мы уже отмечали, *три уровня*: уровень федеральных округов, региональный уровень и муниципальный уровень.

Федеральное и региональное звенья АПК представлены комплексом средств автоматизации[1] «Региональная платформа». В муниципальное звено входят КСА Единого центра оперативного реагирования[2]: КСА ЕЦОР функциональных блоков, например, «Безопасность населения и муниципальной (коммунальной) инфраструктуры», КСА «Безопасность на транспорте» и КСА «Экологическая безопасность».

При создании КСА функциональных блоков АПК «Безопасный город» на территории субъекта Федерации могут использоваться *централизованная, децентрализованная и гибридная схемы, определяющие техническую и системную архитектуру КСА* [37].

Типовой вариант функциональной структуры АПК «Безопасный город» представлен на рис. 2.8.

1. *КСА «Региональная платформа»* предназначен для обеспечения органов исполнительной власти субъектов Российской Федерации опе-

[1] Далее используется сокращение КСА.

[2] Далее используется сокращение ЕЦОР.

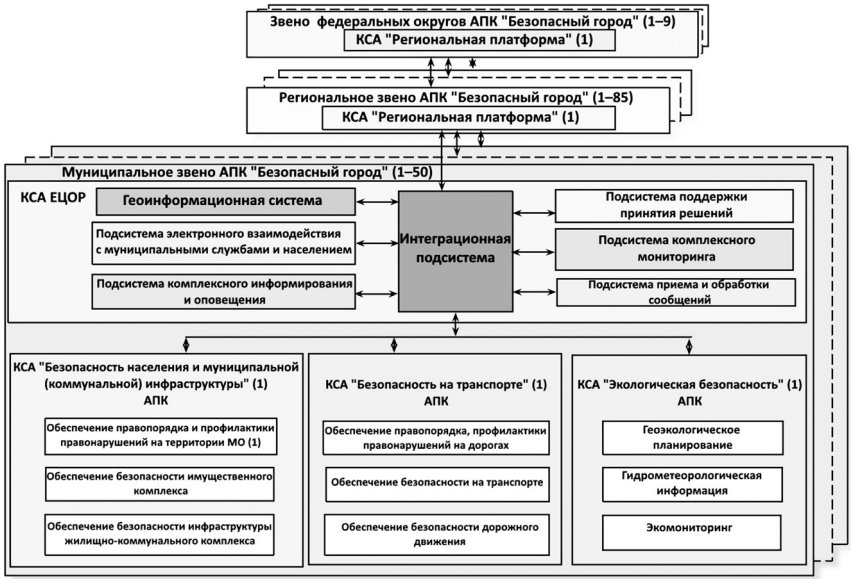


Рис. 2.8. Типовой вариант функциональной структуры АПК «Безопасный город»

ративной и достоверной информацией о ситуации в регионе, координации межведомственного взаимодействия на региональном уровне, предоставления оперативной информации экстренным и дежурным службам при угрозе возникновения или возникновении критических ситуаций, в том числе в сфере правопорядка.

К *основным функциям* «Региональной платформы» относят:

1) сопряжение всех КСА ЕЦОР муниципальных образований, входящих в регион; агрегация информации от них;

2) агрегация необходимой информации от федеральных и региональных КСА в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

3) предоставление органам исполнительной власти субъекта Федерации информации о событиях в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания в регионе в целом и в отдельно взятом муниципальном образовании в частности;

4) обеспечение доступа к необходимым информационным ресурсам АПК «Безопасный город» в соответствии с регламентами взаимодействия и предоставления информации.

В состав КСА «Региональная платформа» входят подсистема интеграции данных, геоинформационная подсистема и подсистема электронного взаимодействия с должностными лицами.

Подсистема интеграции данных обеспечивает информационный обмен между федеральными и региональными КСА и КСА ЕЦОР муниципальных образований, ведение, хранение и резервное копирование информации о федеральных и региональных КСА, целостность данных и авторизованный доступ к ним по установленным регламентам доступа и взаимодействия и др.

Геоинформационная подсистема предназначена для отображения информации из федеральных и региональных КСА, КСА ЕЦОР муниципальных образований в виде семантических слоев, отражающих природно-географические, социально-демографические, экономические характеристики территории, а также объектов инженерной, транспортной и социальной инфраструктуры муниципальных образований, относящихся к региону. Наряду с позиционированием объектов и событий, указанием мест происшествий возможности подсистемы позволяют добавлять новые слои и атрибуты — параметры потенциально опасных и критически важных объектов, социально значимых объектов, объектов (мест) массового скопления людей.

Подсистема электронного взаимодействия отвечает за предоставление пользователям актуальной информации о критических событиях, информирование должностных лиц о необходимых мероприятиях при реагировании на события в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания. Также на эту подсистему возложены задачи передачи в Интернет актуализированной информации о событиях, связанных с безопасностью жизнедеятельности на территории региона.

2. *КСА ЕЦОР* служат для решения задач оперативного реагирования на угрозы общественной безопасности, правопорядка и безопасности среды обитания, а также обеспечения эффективного взаимодействия и координации органов повседневного управления, служб экстренного реагирования и муниципальных служб.

КСА ЕЦОР функционального блока «Координация работы служб и ведомств» включает в свой состав функциональные и обеспечивающие подсистемы. Функциональные отвечают за реализацию основных функций этого блока — прием и обработку сообщений, поддержку принятия решений, мониторинг событий и их отображение на электронной карте геоинформационной подсистемы, а также за взаимодействие с муниципальными службами и информирование и оповещение населения. Обеспечивающие подсистемы отвечают за работоспособность КСА в целом и решают задачи обеспечения информационной безопасности, надежного хранения и администрирования.

Учитывая ведомственный характер данного учебного пособия, рассмотрим **функционал КСА ЕЦОР применительно к задачам, возложенным на ОВД**.

Так, в сфере обеспечения правопорядка *КСА ЕЦОР должны обеспечивать*:

1) прием и регистрацию сообщений о событиях правопорядка по доступным каналам связи;

2) комплексный мониторинг правопорядка посредством сбора и агрегации данных, полученных от средств мониторинга;

3) категоризацию правонарушений;

4) автоматическое предоставление сценария реагирования на правонарушения;

5) моделирование различных сценариев возникновения потенциальных угроз общественной безопасности муниципального образования, включая построение прогнозов их развития и отображение на электронной карте результатов моделирования;

6) оценку сложившейся обстановки и динамическую актуализацию результатов моделирования с учетом поступающих данных с сегментов АПК «Безопасный город».

Значительный вес имеют и функции обеспечения координации и взаимодействия как между дежурными и экстренными службами, так и между сегментами АПК. К этой категории относятся доступ к справочной информации (объекты инфраструктуры города), автоматическое формирование поручений соответствующим службам и подразделениям, контроль за их выполнением. Задача взаимодействия решается за счет формирования единого информационного и справочного пространства АПК «Безопасный город», защищенного доступа к информации с использованием средств криптографической защиты информации, автоматического хранения видеоинформации, отчетной информации о событиях и всей сопутствующей информации.

Как было отмечено выше, в состав КСА ЕЦОР включены такие функциональные блоки, как КСА «Безопасность населения и муниципальной (коммунальной) инфраструктуры», КСА «Безопасность на транспорте» и КСА «Экологическая безопасность». На решение задач обеспечения правопорядка и общественной безопасности — задач, возложенных на ОВД, — в основном ориентированы КСА «Безопасность населения и муниципальной (коммунальной) инфраструктуры» и КСА «Безопасность на транспорте», поэтому остановимся более подробно на составе и особенностях данных комплексов.

1. *КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»* включает несколько АПК. С решением задач, возложенных на ОВД, связан АПК *обеспечения правопорядка и профилактики правонарушений на территории муниципального образования*. В состав этого блока входят подсистемы интеллектуального видеонаблюдения, оценки качества деятельности,

подсистема позиционирования мобильных объектов, обеспечения экстренной связи, управления мобильными подразделениями, управления подразделениями территориальных органов.

Сегмент обеспечения правопорядка и профилактики правонарушений на территории муниципального образования выполняет существенный *перечень функций*, среди которых наиболее важны:

1) *видеонаблюдение и видеоанализ*. В рамках этой функции решаются задачи получения видеоизображения с объектов и его передачи на устройства отображения, записи видеопотоков, их хранения с возможностью поиска, доступа к видеоинформации и управлению видеокамерами посредством выбора мнемоник на электронной карте.

Также следует отметить возможности современной видеоаналитики — это идентификация и распознавание лиц, сопоставление их с данными о лицах, находящихся в розыске, обнаружение скопления людей, выявление фактов движения человека с высокой скоростью (бегущий человек), оставленных предметов, появление человека или автомобиля в зоне наблюдения (улицы, площади, перекрестки, парки);

2) *позиционирование подвижных объектов*. Помимо отображения положения объектов на электронной карте решается задача построения оптимальных маршрутов передвижения с учетом данных о фактической загруженности дорог, погодных и других условиях;

3) *обеспечение функций информирования и получения отзывов от населения о работе представителей территориальных органов*. Сюда относят сбор статистической информации об обращениях граждан, о статусах их исполнения, предоставление населению возможности оценивать качество деятельности представителей территориальных органов МВД России посредством заполнения размещенных на интернет-портале анкет, подготовку сводных аналитических отчетов о результатах деятельности ОВД.

В рамках этой функции также решаются задачи информирования населения о качестве деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания.

Информационное взаимодействие сегмента обеспечения правопорядка и профилактики правонарушений на территории муниципального образования с ресурсами Интернета помогает выявлять фактов целенаправленного негативного информационного воздействия на население, провоцирования социальной, межнациональной, религиозной напряженности через средства массовой информации и Интернет.

2. В *КСА функционального блока «Безопасность на транспорте»* входят следующие *АПК, связанные с решением задач, возложенных*

на ОВД: 1) сегмент обеспечения правопорядка, профилактики правонарушений на дорогах; 2) сегмент обеспечения безопасности дорожного движения. В составе данных комплексов находятся функциональные подсистемы фото-, видеофиксации событий (правонарушений, дорожно-транспортных происшествий, нарушения правил парковки и др.) на дорогах, мониторинга объектов транспортной инфраструктуры и транспортных средств, управления видеопотоками и видеоанализа происшествий, контроля и управления экипажами ДПС ГИБДД МВД России, мониторинга дорожной ситуации, интеллектуального управления светофорами, видеонаблюдением, видеоанализа событий на дорогах, анализа и прогнозирования дорожной ситуации и др.

Актуальным остается **вопрос интеграции, сопряжения КСА АПК «Безопасный город» с единой безопасной средой функционирования сервисов ЦОД ИСОД МВД России**.

24 ноября 2016 г. на совещании рабочей группы для обеспечения рабочего взаимодействия при реализации плановых мероприятий работы Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город», было отмечено, что в будущем ИСОД МВД России может стать одним из основных потребителей информации, поступающей из систем АПК. Главное условие такого взаимодействия в части организации оперативного обмена данными — открытые протоколы для систем, входящих как в ИСОД МВД России, так и в АПК «Безопасный город» [41].

В то же время сопряжение систем АПК «Безопасный город» с ИСОД МВД России должно осуществляться в соответствии с требованиями подсистемы обеспечения информационной безопасности ИСОД МВД России. При этом доступ к оборудованию информационно-коммуникационной инфраструктуры правоохранительного сегмента АПК «Безопасный город» должен быть организован по согласованию с территориальным подразделением МВД России.

Опыт создания комплексных систем безопасности в регионе и существующий концептуальный подход к построению и развитию единой инфокоммуникационной инфраструктуры АПК «Безопасный город» позволяют авторам пособия предложить **проект доверенной среды правоохранительного сегмента комплекса на основе применения современных ИТ**.

В качестве доверенной среды правоохранительного сегмента АПК «Безопасный город» выступает *модель развертывания частного облака инфраструктуры комплексной системы обеспечения безопасности*[1] *на базе ЦОД ИСОД МВД России, созданной по технологии*

[1] Далее используется сокращение КСОБ.

виртуализации основных программных интерфейсов, приложений, операционных систем и специальных сервисов системы.

Для проведения успешной интеграции среды АПК «Безопасный город» с ИСОД МВД России предлагается сформировать специальный (оперативно-служебный) сервис — *сервис КСОБ «Безопасный город»* [56].

Учитывая многообразие исходной информации, необходимость в поддержке и принятии решений, задействование различных подсистем АПК «Безопасный город», потребуется наделить сервис функциональными возможностями, которые позволят выполнять *следующие задачи*:

1) консолидация разнородной информации (видеоинформация, аудиоинформация, текстовые и графические данные) из различных источников в банке данных КСОБ через СПГУ;

2) обеспечение единой точки доступа пользователей к информации через СУДИС ИСОД МВД России;

3) поиск по различным критериям информации в банке данных КСОБ;

4) совместная обработка разнородной информации КСОБ;

5) формирование срочных донесений, информационных сообщений, справок, отчетов и других документов;

6) обмен информацией между пользователями КСОБ посредством СЭД, СЭП, СВКС—М;

7) обозначение (нанесение) сил и средств на электронной карте местности;

8) поддержка процессов формирования решений и доведения их до соответствующих органов управления;

9) поддержка процессов подготовки и проведения заседаний администрации субъекта [56].

Следующим шагом по интеграционному сопряжению доверенной среды виртуализации системы «Безопасный город» является обязательное подключение сервиса КСОБ «Безопасный город» к СУДИС ИСОД МВД России [44].

Такое подключение обеспечит выполнение требований по регистрации и учету пользователей в целях:

1) идентификации и аутентификации пользователей сервиса ИСОД МВД России;

2) управления учетными записями пользователей сервиса ИСОД МВД России (заведение, активация, блокирование и удаление);

3) разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование сервиса ИСОД МВД России;

4) сбора, записи и хранения информации о событиях безопасности [43].

Сервис ИСОД МВД России выступает в роли поставщика услуг. Сервис управления доступом выступает в роли доверенного поставщика идентификации.

Поставщику услуг (сервис КСОБ «Безопасный город») должны быть известны параметры подключения (протокол, адреса вызовов, сертификат и т.д.) к поставщику идентификации. Указанные параметры описываются в метаданных поставщика идентификации. В свою очередь, поставщику идентификации должны быть известны параметры подключения к поставщику услуг, которые должны быть описаны в метаданных поставщика услуг.

Таким образом, для подключения сервиса ИСОД МВД России к СУДИС необходимо: разработать программный интерфейс поставщика услуг, сформировать метаданные поставщика услуг и передать их поставщику идентификации, загрузить метаданные поставщика идентификации.

Взаимодействие сервисов ИСОД МВД России с СУДИС осуществляется посредством электронных сообщений, основанных на стандарте SAML 2.0 с использованием шифрования и электронной подписи на основе алгоритмов ГОСТ 28147—89, ГОСТ Р 34.10—2012, ГОСТ Р 34.11—2012.

Развертывание существующих облачных моделей представления данных на базе ЦОД ИСОД МВД России с учетом правил формирования современных сервисов ИСОД МВД России позволяет адекватно обеспечить процесс включения новых единых систем функционирования АПК «Безопасный город» в состав сервисов ИСОД через технологии доверенной (безопасной) среды виртуализации.

Для демонстрации реального состояния и возможностей развития функциональных подсистем АПК «Безопасный город» рассмотрим **рабочую модель безопасности, созданную на базе центра управления нарядами (функционально-технологической площадки) УМВД России по г. Хабаровску**.

В целях информационного обеспечения автоматизации процессов управления силами и средствами УМВД России по г. Хабаровску для оперативного принятия решений, координации, контроля действий, сбора, обработки и анализа информации на улицах и в других общественных местах города Дальневосточным специализированным центром безопасности информации «МАСКОМ» был разработан АПК, позволяющий объединить самые разнообразные автоматизированные подсистемы обеспечения безопасности в единое информационное пространство. Это означает, что информация от всех систем города пере-

дается через единые каналы связи и аккумулируется в архиве центра обработки данных.

В соответствии с решением Министра внутренних дел Российской Федерации от 17 октября 2011 г. № 1/8901 технические средства АПК «Безопасный город», не предназначенные для оснащения подразделений полиции, переданы с баланса ОВД на баланс учреждений и организаций, наделенных с 1 января 2012 г. полномочиями получателя средств соответствующих бюджетов на внедрение и эксплуатацию технических средств АПК «Безопасный город». Поэтому администрацией города Хабаровска при участии Правительства Хабаровского края был реализован ряд проектов по созданию отдельных площадок с задействованием переданных технических средств для выполнения задач, определенных программой построения и развития АПК «Безопасный город» в части функционирования правоохранительного сегмента. Так, в Хабаровске появилось восемь «территорий безопасности» на городских прудах, площадях и в жилмассивах. Кроме того, в 2016 г. был введен в эксплуатацию городской центр безопасности и управления дорожным движением, который на тот момент аккумулировал видеопотоки от 107 фоторадарных камер на 25 перекрестках городской улично-дорожной сети и 378 видеокамер, осуществлявших охранные функции и функции по соблюдению общественного порядка.

Эти обстоятельства определили необходимость в технологическом изменении процедуры доступа пользователей центра управления нарядами к системам комплекса. Были организованы отдельные физически разделенные каналы связи с дополнительным закрытием на уровне шифрования трафика, которые позволяют через выделенную сеть и ИМТС МВД России в рамках полномочий обмениваться информацией с СЦ.

Для получения информации развернута масштабная сеть технических устройств мониторинга, к которым относятся камеры видеонаблюдения, аппаратура экстренной связи, модули навигации, детекторы и прочее оборудование, установленное на объектах наблюдения — в точках мониторинга.

Комплекс имеет определенную телекоммуникационную инфраструктуру и представлен рядом подсистем, основные из которых представлены на рис. 2.9.

Телекоммуникационная инфраструктура АПК «Безопасный город» реализована на основе регионального сегмента ИМТС МВД России. Созданная сеть позволяет передавать информацию между всеми участниками информационного обмена без потери качества сигнала, а также увеличивать количество необходимых точек доступа. Пропускная способность сети на каждом участке составляет от 1 до 10 Гбайт/с.

Схематично она представлена на рис. 2.9 в виде линий, соединяющих основные *подсистемы АПК*.

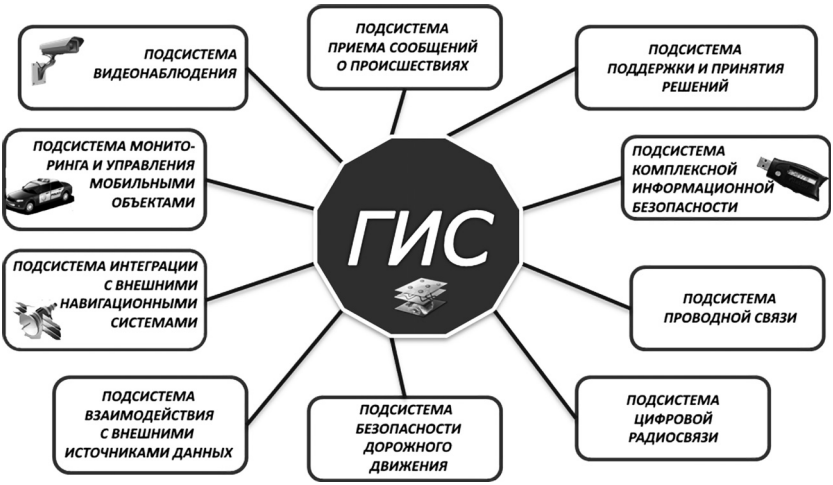


Рис. 2.9. Состав подсистем АПК «Безопасный город» УМВД России по г. Хабаровску

1. *Подсистема видеонаблюдения с технологией интеллектуальной поддержки*. Видеоизображение является очень важным источником объективной информации о текущей ситуации, дающим возможность принимать правильные решения в быстро меняющейся обстановке современного города. Создание распределенной сети видеокамер дает возможность охватить все основные магистрали движения автотранспортных средств и основные улицы города. Интеллектуальные технологии, применяемые в подсистеме видеонаблюдения, позволяют субъекту управления (дежурному по управлению нарядами) освободиться от неотлучного слежения за меняющейся обстановкой и сконцентрироваться на принятии решений и координации усилий всех сил и средств для достижения максимального результата. Распознав нештатную ситуацию, система сигнализирует об этом дежурному, который выступает в качестве эксперта, либо подтверждая оценку системы, либо отвергая ее. Распознав объект: человека, группу людей, автомобиль, — система сопровождает его, создавая условия для распознавания.

2. *Подсистема приема сообщений о происшествиях*. Предназначена для автоматизации работы центра приема сообщений (службы 02) по регистрации сообщений от граждан о происшествиях и по передаче информации в дежурные части отделений полиции УМВД России

по г. Хабаровску. После ввода сообщение сохраняется в базе данных и на его основе создается карточка события подсистемы поддержки принятия решений, отображающаяся на рабочих местах оперативных дежурных отделений полиции.

3. *Подсистема поддержки и принятия решений*. Является аналогом книги учета сообщений о происшествиях и предоставляет оперативному дежурному механизм для выбора одного из возможных решений.

4. *Подсистема мониторинга и управления мобильными объектами*. Позволяет вести контроль за мобильными отрядами, их техническим оснащением, графиками дежурств. Назначение подсистемы — сбор и подготовка данных, необходимых для подсистемы поддержки принятия решений и геоинформационной подсистемы.

5. *Подсистема интеграции с внешними навигационными системами*. Необходима для получения информации о расположении мобильных объектов из внешних навигационных систем, оборудованных приемниками ГЛОНАСС/GPS. Подсистема не зависит от технологической платформы подключаемой системы навигации и предоставляет унифицированный интерфейс различным подсистемам для получения данных о навигации и телеметрии неведомственных мобильных объектов.

6. *Геоинформационная подсистема с поддержкой отображения интерактивной карты города*. Обеспечивает отображение информации об объектах на интерактивной карте города. Как мы уже отмечали в подразд. 1.5, когда подробно рассматривали ГИС, с ее помощью можно увидеть, где расположены видеокамеры, объекты, имеющие значение для принятия решения дежурным, зафиксированы места происшествий, находятся мобильные отряды, узнать сводную и адресную информацию.

Геоинформационная подсистема представляет собой масштабируемую детализированную электронную карту города, содержащую множество тематических слоев, на которых воспроизводится информация, поступающая от других подсистем.

7. *Подсистема проводной связи*. Дает возможность организовывать селекторные аудио- и видеоконференции, а также телефонные переговоры.

8. *Подсистема взаимодействия с внешними источниками данных*. Предназначена для получения данных из внешних информационных систем (например из пунктов централизованной охраны управлений вневедомственной охраны Росгвардии), отвечает за регламентированный доступ к ним.

9. *Подсистема обеспечения комплексной безопасности*. Обеспечивает физическую и информационную безопасность объектов инфра-

структуры системы и конфиденциальность при получении данных, в том числе аудит событий в АПК «Безопасный город». Основное направление — защита информации от хищения, утраты, утечки, уничтожения, искажения и подделки в результате несанкционированного доступа и специальных воздействий.

10. *Подсистема цифровой радиосвязи*. Предназначена для организации цифровой радиосвязи с использованием современных стандартов взаимодействия между корреспондентами единой дислокации сил и средств, участвующих в обеспечении общественного порядка.

11. *Подсистема безопасности дорожного движения*. Представляет собой комплекс технических средств для решения задач фото-, видеофиксации нарушений правил дорожного движения, дорожно-транспортных происшествий, видеонаблюдения за событиями на дорогах, анализа и прогнозирования дорожной ситуации.

Несмотря на успехи в использовании функциональных возможностей АПК «Безопасный город», имеется **ряд направлений расширения и развития комплекса**, дальнейшего внедрения в межведомственное информационное пространство МВД России и других ведомств, участвующих в обеспечении безопасности города.

К таковым относятся:

1) развитие телекоммуникационной инфраструктуры АПК «Безопасный город», включая системы беспроводной связи;

2) развитие подсистемы видеонаблюдения и технологий видеоанализа;

3) дополнение подсистемы приема сообщений о происшествиях функциями определения места происшествия по значимым объектам (остановки, памятники, магазины и т.д.), по сотовому телефону, по ключевым словам;

4) развитие системы управления и поддержки принятия решений за счет более глубокого, в том числе с применением интеллектуальных аналитических технологий, анализа статистической информации с нанесением результатов на карту города;

5) развитие геоинформационной подсистемы с учетом возможностей определения зон, подверженных риску вследствие возникновения чрезвычайных ситуаций, техногенных аварий, совершения террористических актов, и отображения снимков местности по данным космической и аэрофотосъемки;

6) развитие подсистемы защиты информации — переход на новый уровень контроля за событиями информационной безопасности в условиях неточности, неопределенности и сложности формализации угроз, возникающих в процессе обработки, хранения, передачи информации между хостовыми и сетевыми объектами инфокоммуникационной инфраструктуры.

Это может быть достигнуто за счет разработки и внедрения новых систем и моделей адаптивного интеллектуального контроля за состоянием информационной среды, а также применения интеллектуальных механизмов идентификации угроз безопасности и активации необходимых модулей защиты.

Ядром системы может стать распределенный интеллектуальный АПК, вокруг которого и сформируется вся ее инфраструктура. Основанная на интеллектуальном ядре комплексная система приобретет новые качества, расширяя функции безопасности по целому ряду направлений. Фактически изменится сама модель безопасности. Вместо плоской структуры система приобретет многомерную за счет единого интеллектуального механизма управления всеми компонентами безопасности. Многомерность, в частности, проявится в пространственном подходе к видеонаблюдению, когда к плоскости стационарных видеокамер добавляются высотные (беспилотные летательные аппараты) и наземные мобильные (патрульные автономные роботы) компоненты. Ядро системы также обеспечит технологическую инфраструктуру для интеграции в единое информационное пространство всех АПК различных решений и систем.

Интеллектуальные средства подобных АПК предусматривают автоматическое информирование всех заинтересованных служб о зарегистрированных системой чрезвычайных ситуациях. Таким образом, например, информация о дорожно-транспортных происшествиях автоматически будет поступать в службы оказания экстренной помощи, существенно повышая оперативность их реагирования.

Обобщая рассмотренные выше положения, можно сказать, что внедрение АПК «Безопасный город» во многих крупных городах России предоставляет полиции современные технические средства, с помощью которых правоохранительная деятельность переходит на новый этап развития.

К **основным результатам внедрения и использования АПК «Безопасный город»** относят:

1) сокращение времени формирования и предоставления оперативной информации;

2) сокращение времени принятия решения по факту изменения оперативной обстановки;

3) увеличение числа раскрытых преступлений, совершенных в местах массового скопления людей;

4) сведение к минимуму угроз проведения террористических актов и совершения преступных действий с особо тяжкими последствиями;

5) обеспечение имущественной неприкосновенности хозяйствующих субъектов различной организационно-правовой формы и формы собственности, общественных, иных организаций и населения.

Анализ продуктивности действия правоохранительного сегмента АПК «Безопасный город» показал, что только в 2016 г. в результате взысканий по административным протоколам, составленным в режиме фото- и видефиксации нарушений правил дорожного движения, в бюджет Хабаровского края поступило свыше 98 млн. рублей. Кроме того, за последние три года на 39,1% снизилось количество грабежей, на 16,7% — убийств, почти на 50% уменьшилось количество автомобильных угонов [33].

С учетом высокой эффективности от внедрения системы применение механизмов интеллектуального управления в подсистемах безопасности при решении таких оперативно важных задач, как распознавание образов, оперативная и аналитическая оценка совершаемых преступлений, информационно-аналитический анализ криминальной обстановки на территории города, оценка угроз безопасности для информационных банков данных ОВД и управление необходимым набором механизмов защиты, позволит лицу, принимающему решения, своевременно и эффективно обеспечить должную реакцию на возникающие противоправные события.

2.4. Навигационно-мониторинговые системы в информационно-аналитическом обеспечении деятельности органов внутренних дел

В современных условиях действия подразделений МВД России должны характеризоваться высокой динамичностью и маневренностью сил, широким применением новых технических средств. Состояние и перспективы развития, уровень организационного и технического обеспечения автоматизированных систем управления силами и средствами являются важнейшими показателями готовности структур ОВД к выполнению возложенных на них обществом задач.

Одно из основных направлений совершенствования такого управления — широкое применение современных технических средств, в том числе навигационно-мониторинговых систем[1], работа которых основана на использовании глобальных навигационных спутниковых систем[2] (ГЛОНАСС, GPS) и телекоммуникационных технологий. *Системы мониторинга позволяют* повысить эффективность управления силами и средствами, сократить время реагирования на происшествия, усилить контроль за выполнением задач патрулирования, конвоирования, сопровождения специальных перевозок, охраны объектов, опти-

[1] Далее используется сокращение НМС.

[2] Далее используется сокращение ГНСС.

мизировать реализацию оперативных планов, наладить эффективное взаимодействие силовых структур, обеспечить рациональное использование транспортных средств.

Для повышения эффективности реагирования мобильных подразделений ОВД на те или иные события, а также контроля за оперативной обстановкой возникает необходимость **оснащения ведомственного автотранспорта аппаратурой спутниковой навигации**[1].

Для этих целей ранее применялась и успешно эксплуатировалась *ГНСС GPS (Global Positioning System) производства США*.

В целом по точности определения местонахождения объектов и по набору сервисных услуг GPS вполне соответствует требованиям, предъявляемым в ОВД к системам подобного класса. Однако, учитывая, что в целях обеспечения национальных интересов США сигналы GPS могут селективно отключаться в пределах отдельного региона, использование такой системы в интересах органов государственной власти Российской Федерации, в частности МВД России, не может быть признано целесообразным.

В соответствии с изложенным 17 мая 2007 г. вышел Указ Президента Российской Федерации № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации». В нем установлено, что для обеспечения безопасности Российской Федерации аппаратура спутниковой навигации, приобретаемая для нужд федеральных органов исполнительной власти и подведомственных им организаций, должна функционировать с использованием сигналов *отечественной глобальной навигационной спутниковой системы (ГЛОНАСС)*. В связи с этим встал вопрос о модернизации действующих в ОВД систем навигационно-временного обеспечения с целью их перевода для работы с оборудованием ГЛОНАСС.

Системы ГЛОНАСС и GPS отличаются структурами орбитальных группировок космических аппаратов (по 8 аппаратов на трех орбитах в ГЛОНАСС и по 4 аппарата на шести орбитах в GPS), способом разделения навигационных сигналов (частотный в ГЛОНАСС и кодовый в GPS), сроками активного существования космических аппаратов (в GPS сроки больше, чем в ГЛОНАСС) [38].

Разработка ГЛОНАСС началась на рубеже 70—80-х гг. прошлого века. Первый спутник, оснащенный необходимой радиотехнической аппаратурой, был запущен на орбиту в 1982 г. (высота — 19 100 км, наклонение — 64,5 °). В 1995 г. ГЛОНАСС была развернута в полном объеме (24 космических аппарата с трехлетним сроком активного су-

[1] Далее используется сокращение АСН.

ществования). Точность определения местонахождения объектов обеспечивалась не хуже, чем в GPS.

В соответствии с Федеральной целевой программой «ГЛОНАСС», утвержденной Правительством Российской Федерации в 2001 г., были проведены работы по модернизации космических аппаратов ГЛОНАСС в целях обеспечения срока их активного существования от 7 до 10 лет. В настоящее время проводятся работы по увеличению точности обсервации, повышению надежности, доступности, достоверности и других важных характеристик ГЛОНАСС.

По состоянию на май 2016 г. в составе орбитальной группировки использовались по целевому назначению 23 космических аппарата, что обеспечивает полное покрытие территории Российской Федерации. Тем не менее, в настоящее время точность определения местонахождения абонентов и набор сервисных услуг, предоставленных системой ГЛОНАСС, не вполне отвечают требованиям ОВД. Поэтому на текущем этапе *принято решение о применении комбинированного способа определения объектов*. Суть заключается в использовании абонентских приемников, работающих *одновременно с сигналами ГЛОНАСС и GPS.*

В ряде территориальных органов служб МВД России (ГИБДД, служба конвоирования, ППС и т.д.) и других структур (Росгвардия) в настоящее время активно применяется аппаратура спутниковой навигации GPS.

Как показывает практика, сотрудники ОВД **применяют АСН для** управления мобильными силами, раскрытия преступлений, обеспечения безопасности перевозок и решения специальных задач.

В деятельности сотрудников полиции общественной безопасности АСН используются для управления мобильными силами и обеспечения безопасности перевозок грузов, спецконтингента, охраняемых лиц.

Сотрудникам подразделений уголовного розыска АСН помогают в раскрытии преступлений («машины-ловушки», аппаратура для скрытого наблюдения за подвижными объектами и т.д.) [21].

В целях борьбы с кражами и угонами автотранспорта ОВД сотрудничают с организациями — операторами спутниковых противоугонных систем. Для упорядочения указанных взаимоотношений были разработаны и внедрены в практику правила стандартизации МВД России ПР 78.01.0019—2007 «Спутниковые противоугонные системы. Использование для предотвращения краж и угонов автотранспорта при сотрудничестве органов внутренних дел Российской Федерации с организациями-операторами». Правила содержат основные технические требования, специальные технические требования, нормативно-правовые требования к спутниковым противоугонным системам и методику их испытаний.

Основными проблемами, возникающими в ходе использования НМС в регионах, являются отсутствие актуальных электронных карт, несовместимость применяемых систем, недостаточное информирование о возможностях систем и работах по внедрению аппаратуры спутниковой навигации и т. д. [50].

Навигационно-временное обеспечение *приобретает все большее значение* в повседневной деятельности подразделений МВД России. Одной из главных *задач* является управление мобильными нарядами полиции. Наличие привязанных к единому картографическому ресурсу объективных сведений о расстановке сил и средств, статусе нарядов, информации о происшествиях значительно повышает эффективность оценки оперативной обстановки, принятия управленческих решений и контроля за их исполнением.

Навигационно-временное обеспечение важно в документировании происшествий. В частности, приказом МВД России от 1 апреля 2011 г. № 154 «Об утверждении формы справки о дорожно-транспортном происшествии» с 1 января 2012 г. введено новое требование к справке о дорожно-транспортном происшествии, которое предписывает указывать информацию о координатах (широте, долготе) места происшествия, полученную с помощью навигационной аппаратуры ГЛОНАСС.

Важными характеристиками навигационно-временного обеспечения являются:

- доступность навигационных данных;
- точность показателей навигационных определений;
- наличие информации о целостности навигационных полей, а также об индустриальных и преднамеренных помехах.

Современные спутниковые навигационные технологии позволяют с высокой точностью определять местоположение подвижных и стационарных объектов. Например, методы дифференциальной коррекции предусматривают внесение в навигационную аппаратуру дифференциальных поправок. Для дорогостоящей навигационной аппаратуры геодезического класса точность позиционирования может достигать единиц миллиметров, а для недорогих одночастотных приемных устройств, устанавливаемых на большинстве транспортных средств, эта величина может составлять менее 1 м.

Отечественные системы функциональных дополнений ГНСС (система высокоточного определения эфемерид и временных поправок — СВОЭВП, система дифференциальной коррекции и мониторинга — СДКМ) значительно улучшают возможности навигационного определения и оперативного информирования пользователей ГНСС о состоянии орбитальных группировок ГЛОНАСС и GPS. Разработана специальная аппаратура мониторинга условий навигации (АМУН), по-

зволяющая обеспечить навигационной корректирующей информацией и информацией об условиях навигации.

Развитие технических средств обеспечения деятельности МВД России тесно связано с государственными программами создания системы вызовов экстренных оперативных служб через единый номер 112 (система-112), системы экстренного реагирования при авариях «ЭРА-ГЛОНАСС» и АПК «Безопасный город», *включающими навигационно-мониторинговый сегмент*.

Сотрудники МВД России решают различные оперативно-служебные задачи, проводят специальные мероприятия и операции. Управление силами и средствами должно поддерживаться проведением единой технической политики в области навигационно-временного обеспечения. Одним из способов является информационно-техническое обеспечение НМС ОВД.

Действия специальных подразделений МВД России могут проводиться в районах, где отсутствует покрытие служебной УКВ-связи или сетей сотовой связи. В таких условиях *актуальность приобретают вопросы использования абонентской аппаратуры (аварийных радиобуев) международной спутниковой системы поиска и спасания КОСПАС—САРСАТ, а также вопросы оперативного получения сообщений о терпящих бедствие на объектах МВД России*. Современные НМС должны строиться с учетом возможности интеграции с вышеуказанными системами.

Неотъемлемым атрибутом НМС является **картографическое обеспечение**. Сегодня в этой сфере существуют *проблемы объективного характера*, свойственные практически всем ведомствам. Основной является отсутствие актуальных электронных карт либо несвоевременное проведение работ по их актуализации.

Вместе с тем многие регионы создают на местном уровне инфраструктуры пространственных данных, по сути — *региональные ГИС*. (Особенности геосистем мы подробно рассматривали в подразд. 1.4.) Картографическая информация, имеющаяся на местном уровне, по сравнению с другими источниками является более детальной и характеризуется высокой степенью актуализации.

В качестве примера можно привести региональные ГИС Калужской и Ярославской областей. Здесь достигнуты соглашения между администрациями регионов и управлениями МВД России в части обеспечения территориальных подразделений актуальной картографической информацией.

Одним из направлений реализации единой технической политики в области создания, внедрения и интеграции НМС является создание единой инфраструктуры навигационно-временного обеспечения спе-

циальных подразделений ОВД России. Сегодня оно идет в тесной взаимосвязи с развитием и внедрением в МВД России прогрессивных ИТ.

К настоящему времени выполнена **опытно-конструкторская работа с шифром «Центр-НМС» по созданию типовых центров многоуровневой системы контроля и управления подвижными объектами и системы информационной поддержки территориальных органов МВД России** [45].

В ее рамках разработаны проекты:

- типового центра мониторинга федерального уровня (ТЦМ-Ф);
- типового центра мониторинга регионального уровня (ТЦМ-Р);
- типового центра мониторинга муниципального уровня (ТЦМ–М);
- специального оперативного мобильного центра (СОМЦ);
- системы обеспечения потребителей МВД России информацией о состоянии навигационных полей, корректирующей информацией и сведениями для актуализации картографической информации (СОП).

Назначение ТЦМ всех уровней и СОМЦ — навигационно-информационное обеспечение деятельности подразделений МВД России. Они собирают, обрабатывают и отображают навигационную и другую информацию о контролируемых подвижных объектах на основе технологий спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS для навигационного обеспечения задач управления силами и средствами МВД России.

ТЦМ являются базовыми элементами многоуровневой системы контроля и управления подвижными объектами (МСКУ) и СОП.

Основными *функциями ТЦМ как базового элемента многоуровневой системы контроля и управления подвижными объектами* являются:

1) прием информации с навигационно-информационных комплектов, установленных на контролируемых подвижных объектах, и управление их работой;

2) контроль и управление подвижными объектами: отображение их текущего местоположения, параметров движения и состояния, формирование и контроль прохождения маршрутов движения, зон контроля и еще целый ряд навигационно-мониторинговых функций;

3) ввод и изменение пользовательских объектов на электронной карте;

4) формирование справочной информации и отчетов, в том числе о происшествиях, истории движения объектов;

5) информационное взаимодействие между ТЦМ разного уровня (а также между ТЦМ и СОМЦ) для обмена навигационной, справочной, служебной информацией;

6) информационное сопряжение с НМС МВД России на основе унифицированных протоколов информационного обмена со спутниковой системой поиска и спасания КОСПАС—САРСАТ.

Основными функциями ТЦМ как базового элемента СОП являются:

1) информационное сопряжение с комплексом функциональных дополнений ГЛОНАСС (СВОЭВП, СДКМ), со специальными центрами силовых ведомств (ППЦСИО Минобороны России);

2) возможность использования навигационного приемника геодезического класса (с анализатором спектра) для получения корректирующей навигационной информации, а также информации, необходимой для контроля качества (целостности) навигационных полей систем ГЛОНАСС и GPS, определения условий навигации (наличия помех в спектре принимаемых сигналов ГНСС) в районах расположения ТЦМ;

3) оценка возможности использования ГНСС в районе расположения ТЦМ;

4) выдача потребителям корректирующей информации и информации о качестве навигационных полей и условиях навигации;

5) высокоточная постобработка навигационной информации потребителей;

6) сбор и доведение до потребителей актуальной картографической информации.

В рамках МСКУ и СОП ТЦМ обеспечивают мониторинг функционирования подчиненных центров мониторинга и безопасность обрабатываемой информации (разделение доступа, шифрование, защита информации от несанкционированного доступа).

Схема информационного взаимодействия разработанных в опытно-конструкторской работе с шифром «Центр-НМС» АПК представлена на рисунке 2.10.

МСКУ и СОП строятся как многоуровневые системы, включающие три сегмента: федеральный, региональный и муниципальный.

ТЦМ-Ф обеспечивает взаимодействие с ТЦМ-Р и управляет работой всей распределенной многоуровневой системы (МСКУ и СОП), а также отвечает за выполнение задач навигационно-информационного обеспечения потребителей. На федеральном уровне ими являются подразделения центрального аппарата МВД России.

ТЦМ-Ф позволяет принимать, обрабатывать и анализировать агрегированную информацию, получаемую от нижестоящих центров. На федеральном уровне требуются в основном обобщенные навигационно-мониторинговые сведения от территориальных подразделений, представление о криминогенной обстановке, мерах реагирования и другая статистическая информация. В исключительных случаях

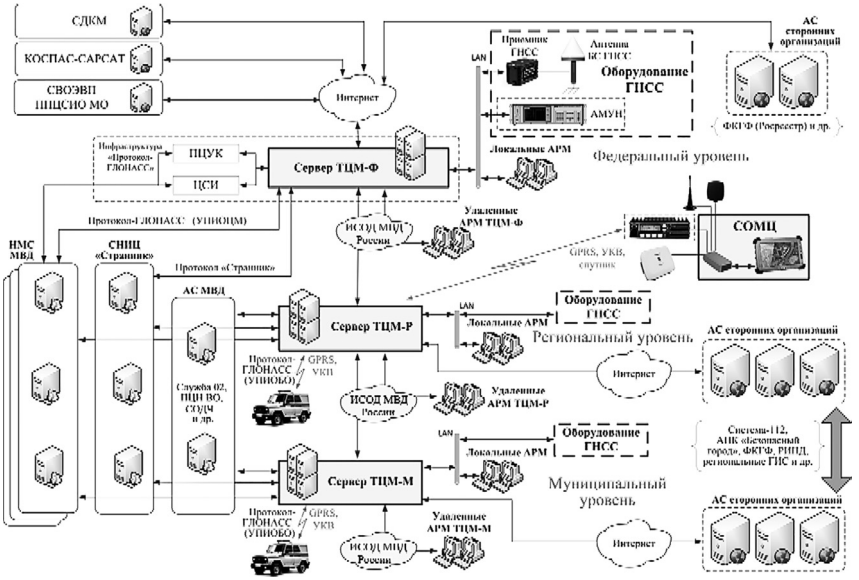


Рис. 2.10. Схема информационного взаимодействия АПК, представленных в опытно-конструкторской работе (шифр «Центр-НМС»)

может потребоваться решение задач непосредственного мониторинга и управления подвижными объектами МВД России.

ТЦМ-Р выполняет задачи навигационно-информационного обеспечения органов МВД России регионального уровня — главных управлений (управлений) МВД России по субъектам. Основные функции в части использования НМС: управление нарядами, специальными группами подразделений, входящих в структуру регионального органа; управление силами и средствами подчиненных ОВД на основе навигационно-мониторинговой информации, поступающей от нижестоящих ТЦМ; аналитическая деятельность.

ТЦМ-Р обеспечивает информационное взаимодействие с ТЦМ-Ф, включая передачу необходимой навигационно-мониторинговой информации о контролируемых объектах, сводок о происшествиях, отчетов, справочных данных и другой служебной информации.

ТЦМ-М могут устанавливаться выборочно, например, в крупных районных центрах или закрытых административно-территориальных образованиях. Они также обеспечивают подключение удаленных АРМ, расположенных в подчиненных территориальных подразделениях.

Взаимодействие ТЦМ между собой осуществляется по ведомственной сети (ИМТС МВД России) в контуре передачи конфиденциальной информации.

Основными потребителями навигационно-мониторинговой информации, предоставляемой ТЦМ всех уровней, являются дежурные части территориальных органов (на федеральном уровне — дежурная часть МВД России), дежурные части и должностные лица строевых подразделений (ГИБДД, ППСП) и др.

ТЦМ всех уровней содержат интерфейсы сопряжения с внешними источниками и потребителями навигационно-мониторинговой информации.

Одним из источников навигационно-мониторинговой информации на федеральном уровне является система КОСПАС—САРСАТ. На региональном и муниципальном уровнях ТЦМ имеют техническую возможность подключения к различным информационным системам МВД России и других ведомств. В частности, за счет использования универсальной интеграционной шины может быть обеспечена гибкость подключения ТЦМ к службе 02, системе-112 (для получения карточки вызова).

СОМЦ обеспечивает информационное взаимодействие с ТЦМ-Р по каналам связи (GSM, УКВ или спутниковая связь); прием от ТЦМ общих справочных данных для их актуализации.

СОП, используя аппаратно-программные средства ТЦМ, обеспечивает:

1) информационное сопряжение (получение информации) и обработку получаемой от внешних навигационных систем информации о целостности навигационных полей, корректирующей информации, информации об условиях навигации и доведение ее до потребителей МВД России;

2) сбор из различных источников и хранение актуальной картографической информации, а также доведение ее до потребителей МВД России.

СОП представляет собой иерархическую систему. На федеральном уровне (федеральный сегмент) она строится на основе ТЦМ-Ф, включая серверное оборудование, общее программное обеспечение, на региональном уровне (региональный сегмент) — на основе ТЦМ-Р, а на муниципальном уровне (муниципальный сегмент) — на основе ТЦМ-М.

Специальное программное обеспечение использует основные компоненты ТЦМ-Ф. Такая конфигурация СОП позволяет получать актуальную картографическую информацию из федеральных источников геопространственной информации и региональных ГИС. Также имеется возможность создания локальной дифференциальной подсистемы и подсистемы мониторинга условий навигации на базе ТЦМ любого уровня.

Таким образом, применение НМС является необходимым условием повышения эффективности деятельности ОВД и оперативности принятия решений. При этом в целях обеспечения национальной безопасности предпочтение отдается системе ГЛОНАСС. Кроме этого, данная система по ряду показателей превосходит систему GPS. Следует также учитывать важный аспект применения НМС — параметры интерфейса между картографической подсистемой и навигационными блоками, обеспечивающими передачу геопозиции от мобильных объектов в базу данных НМС. Эти параметры должны отвечать требованиям к современным технологиям обмена данными по скорости, безопасности и надежности. Предполагается включение в состав ИСОД МВД России специализированного навигационного сервиса, что позволит обеспечить универсальность технологии предоставления данной услуги и дать навигационную информацию для других сервисов.

Контрольные вопросы

1. Какие виды ресурсов и в каком порядке используются при обращении к базе данных, расположенной на удаленном компьютере?
2. Как называется группа сотрудников, работающая над одним проектом в рамках локальной сети?
3. Какие аппаратно-программные средства применяются для решения задач обмена данными между разными сетями и для обеспечения сетевой безопасности?
4. Как называется уровень модели OSI, отвечающий за подключение с использованием имени пользователя и пароля?
5. Какие структурные элементы выделяют в составе ИМТС МВД России?
6. Что представляет собой физическая основа ИМТС МВД России?
7. Какие сервисы выделяют в составе ИСОД МВД России?
8. Какое условие необходимо выполнить пользователю для получения доступа к информационным ресурсам ИСОД МВД России?
9. Как называется принцип развития ИМТС МВД России, который обеспечивает возможность быстрой адаптации ИМТС МВД России под конкретные потребности?
10. Какие задачи защиты информации решены в среде ИСОД МВД России?
11. Что было основной причиной затруднений, возникших в ходе эксплуатации комплексов «Безопасный город» на первом этапе?
12. Какие территориальные уровни выделяют в составе АПК «Безопасный город»? Какие комплексы средств автоматизации им соответствуют?

13. Как называется комплекс средств автоматизации АПК «Безопасный город», предназначенный для сопряжения муниципальных образований и агрегации информации?

14. Как называются и в состав каких комплексов средств автоматизации АПК «Безопасный город» входят АПК, обеспечивающие решение задач, возложенных на ОВД?

15. Какие возможные направления развития АПК «Безопасный город» имеются для подсистемы поддержки принятия решений?

16. Почему применение в деятельности ОВД НМС ГЛОНАСС является предпочтительным по сравнению с GPS?

17. Какова величина точности позиционирования для одночастотных приемных устройств, устанавливаемых на большинстве транспортных средств?

18. Какие компоненты входят в состав многоуровневой системы контроля и управления подвижными объектами и системы информационной поддержки территориальных органов МВД России?

19. Как соотносятся ТЦМ федерального, регионального и муниципального уровней и СОП МВД России?

ГЛАВА 3.
РЕШЕНИЕ ЗАДАЧ УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА БАЗЕ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ

3.1. Системы поддержки принятия решений и современные методы анализа данных в решении задач управления

Информационно-аналитическая деятельность в решении задач управления в ОВД предполагает сбор, обработку и анализ информации в среде сложных систем (которым присущи параметры многофакторности, самоорганизации и саморазвития). Такая деятельность ведется созданными для этого группами из специалистов-аналитиков, обладающих для этого специальными знаниями и навыками и использующих определенные методы и средства (формальные и неформальные) для моделирования (описания) социальных процессов или их фрагментов.

Ввиду того, что на современном этапе рассматриваемый уровень организационно-управленческих задач характеризуется, как правило, слабой структурированностью, многокритериальностью в условиях неполноты или избыточности исходной многомерной информации, то *практическое их решение предполагает наличие компьютерных систем поддержки принятия решений*[1] *и использование современных методов анализа и объяснения данных*. Это позволяет реализовать в диалоговом режиме подходы к сбору и обработке информации, а также объяснить логику проводимого анализа и смысл получаемых результатов на языке, привычном и понятном пользователю.

Поэтому *необходимы специалисты, способные оказывать помощь лицу, принимающему решения, беря на себя роль организатора процесса принятия решений* (хотя выбор самого решения вместе с несением ответственности за этот выбор остается за лицом, его принимающим). Речь идет о *специалистах-аналитиках***.** Они обеспечивают и организуют уточнение постановки задачи; выявляют активную группу людей, которые имеют к задаче интерес и возможность в той или иной мере

[1] Далее используется сокращение СППР.

влиять на ее решение. Кроме того, в случае необходимости, они привлекают к работе *экспертов* — специалистов-профессионалов по отдельным аспектам решаемой проблемы.

Для принятия сложных и ответственных решений требуется надлежащее *информационно-аналитическое обеспечение*, предполагающее сбор массивов необходимых данных и обработку собранной информации для представления лицу, принимающему решения, в наглядном, удобном и понятном ему виде. Требуется *технологическое обеспечение*, помогающее лицу, принимающему решения, опереться на опыт, накопленный при рассмотрении подобных проблем.

Современный уровень развития инфокоммуникационных технологий обеспечивает доступ к большим массивам данных, которые можно использовать для решения задач обработки и анализа. Однако в машинной форме они содержат информацию, необходимую человеку, в скрытом виде — для ее извлечения нужны *специальные методы анализа данных*.

Большой объем информации, с одной стороны, позволяет получить более точные расчеты и анализ, с другой — превращает поиск решений в сложную задачу. Неудивительно, что первичный анализ данных был переложен на компьютер. Именно на решение задач первичного анализа направлена работа программных систем, призванных облегчить работу аналитиков. Поэтому такие системы принято называть *системами поддержки принятия решений* — СППР (Decision Support System, DSS).

Математические модели и методы анализа и программные средства, позволяющие осуществлять помощь в процессе принятия решений, входят в состав СППР. Процесс работы лица, принимающего решения, с такой системой протекает в диалоговом режиме с компьютером, который становится в определенном смысле партнером человека в принятии решений. Обеспечение лица подходящей СППР и обучение работе с ней также являются задачей аналитика (консультанта) [70].

Для выполнения анализа СППР должна накапливать информацию, обладая средствами ее ввода и хранения. Можно выделить три **основные задачи, решаемые в СППР**:

1) ввод данных;
2) хранение данных;
3) анализ данных.

Таким образом, *СППР — это* системы, обладающие средствами ввода, хранения и анализа данных, относящихся к определенной предметной области, с целью поиска решений [47].

Ввод данных в СППР осуществляется либо автоматически с помощью датчиков, характеризующих состояние среды или процесса, либо человеком-оператором. В первом случае данные накапливаются путем

циклического опроса либо по сигналу готовности, возникающему при появлении информации. Во втором случае СППР должны предоставлять пользователям удобные средства ввода данных, контролирующие их корректность и выполняющие сопутствующие вычисления. Если ввод осуществляется одновременно несколькими операторами, то система должна решать проблемы параллельного доступа и модификации одних и тех же данных.

Постоянное накопление данных приводит к непрерывному росту их объема. В связи с этим на СППР ложится задача обеспечить надежное хранение больших объемов данных. На СППР также могут быть возложены задачи предотвращения несанкционированного доступа, резервного хранения данных, архивирования и т. п.

Основная задача СППР — предоставить аналитикам инструмент для выполнения анализа данных. Необходимо отметить, что для эффективного использования СППР ее пользователь — аналитик должен обладать соответствующей квалификацией. Система не генерирует правильные решения, а только предоставляет аналитику данные в соответствующем виде (отчеты, таблицы, графики и т. п.) для изучения и анализа, именно поэтому такие системы обеспечивают выполнение функции поддержки принятия решений. Очевидно, что, с одной стороны, качество принятых решений зависит от квалификации аналитика. С другой — рост объемов анализируемых данных, высокая скорость обработки и анализа, а также сложность использования машинной формы представления данных стимулируют исследования и разработку интеллектуальных СППР [47; 67].

Обобщенная **архитектура СППР** может быть представлена следующим образом (рис. 3.1).

В СППР входят три основных подсистемы:

1) *подсистема ввода данных*. В таких подсистемах, называемых OLTP (online transaction processing), ведется операционная (транзакционная) обработка данных. Для этого используют обычные СУБД, которые мы рассматривали в подразд. 1.4;

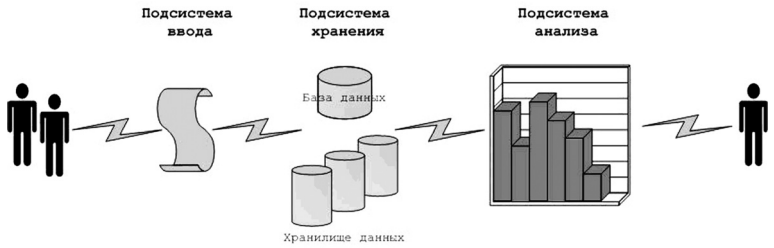


Рис. 3.1. Обобщенная архитектура системы поддержки принятия решений

2) *подсистема хранения*. Для ее работы используют современные СУБД и концепцию хранилищ данных;

3) *подсистема анализа*. Может быть построена на основе:

- подсистемы информационно-поискового анализа на базе реляционных СУБД и статических запросов с использованием языка SQL (Structured Query Language — языка структурированных запросов);
- подсистемы оперативного анализа на базе технологии оперативной аналитической обработки данных OLAP (online analytical processing), использующей концепцию многомерного представления данных;
- подсистемы интеллектуального анализа, реализующей методы и алгоритмы Data Mining (см. о них в подразд. 3.2).

Сегодня существует **ряд критериев (требований) к СППР** [67; 70]. К основным относятся следующие.

1. *Высокая степень детализации хранимых данных*. Для анализа требуется работа сразу с большим количеством сведений, их группировка и обобщение (суммирование, агрегирование и т. п.), которые невыполнимы без достаточно подробного и детального представления данных. Так, например, для анализа состояния криминологической обстановки может потребоваться выполнение запросов, связанных с определением общего числа преступлений по территориям и объектам, по видам, наиболее или наименее распространенных, обобщение по степени тяжести, суммирование по величине нанесенного ущерба и т. д.

2. *Высокое качество данных*. Некорректные данные при анализе могут привести к неверной оценке ситуации, неправильным выводам и принятию ошибочных решений.

3. *Приведение данных к единому формату хранения*. Одни и те же данные в разных информационных системах представляются в различном виде и могут не совпадать (например, данные о лице, совершившем правонарушения, проходившем по разным отделам и службам, могут не совпадать в информационных массивах этих подразделений).

В процессе анализа такие различия чрезвычайно усложняют работу, поэтому необходимо приведение данных к единому формату. Как правило, требуется, чтобы он был оптимизирован для анализа. Часто этого достигают и за счет избыточности и дублирования данных.

4. *Разрешение избыточности данных*. Аналитические запросы к базам данных очень трудно формулируются и крайне неэффективно выполняются, поскольку содержат в себе представления (view), объединяющие большое количество таблиц. При проектировании систем анализа стараются максимально упростить схему базы и уменьшить количество таблиц, участвующих в запросе. С этой целью часто допускают денормализацию (избыточность данных).

5. *Возможность управления данными*. Данные в системах анализа меняются редко. Единожды попав туда, они уже практически не изменяются. Ввод новых данных, как правило, носит эпизодический характер и выполняется в периоды низкой активности системы (например, раз в неделю по выходным). Поэтому система анализа должна обеспечивать возможность периодического добавления данных, контроля вводимой информации и последующего обновления информационных массивов системы без ущерба основным процессам обработки.

6. *Максимально возможное количество хранимых данных*. Системе анализа может потребоваться анализ динамики процессов и явлений. По этой причине для анализа данных необходимы сведения за максимально большой интервал времени.

7. *Произвольный характер запросов к данным*. Для СППР невозможно заранее определить необходимые запросы, поэтому к ним предъявляется требование обеспечить формирование произвольных запросов аналитиков к базам данных.

8. *Не строго ограниченное время обработки обращений к данным*. В системах анализа обычно выдвигают значительно менее жесткие требования ко времени выполнения запроса. Аналитик может потратить больше времени для проверки своих гипотез. Его запросы могут выполняться в диапазоне от нескольких минут до нескольких часов.

9. *Внушительная вычислительная нагрузка на систему*. Аналитик при работе с системой анализа обращается к ней для проверки некоторых своих гипотез и получения отчетов, графиков, диаграмм и т. п. При выполнении запросов степень загрузки системы высокая, так как обрабатывается большое количество данных, выполняются операции суммирования, группирования и т. п.

10. *Приоритетность определенных характеристик системы*. Для систем анализа более приоритетными являются задачи обеспечения гибкости системы и независимости работы пользователей, другими словами, то, что необходимо аналитикам для анализа данных.

В зависимости от наличия функций, позволяющих выполнять отдельные умственные операции, свойственные человеку, или степени интеллектуальности обработки данных при анализе, выделяют **три класса задач, решаемых современными СППР**:

1) *информационно-поисковый класс*. СППР осуществляет поиск необходимых данных. Характерной чертой такого анализа является выполнение заранее определенных запросов;

2) *оперативно-аналитический класс*. В этом случае СППР группирует и обобщает данные в любом виде, необходимом аналитику. В отличие от информационно-поискового анализа здесь невозможно заранее предсказать необходимые аналитику запросы;

3) *интеллектуальный класс*. СППР осуществляет поиск функциональных и логических закономерностей в накопленных данных, по-

строение моделей и правил, которые объясняют найденные закономерности и/или (с определенной вероятностью) прогнозируют развитие некоторых процессов [47].

Что касается первого класса задач — задач информационного поиска, следует отметить, что такие СППР успешно применяются в аналитической работе ОВД, например, это обращение с запросами к информационным массивам интегрированных банков данных МВД России, в том числе к отдельным подсистемам (рис. 3.2), и формирование на основе результатов специальных аналитических таблиц.

СППР для задач второго класса уже разработаны и начинают применяться. Это, например, сервис по сбору и обработке информации о состоянии преступности, расследованию уголовных дел и иной оперативно-служебной деятельности ОВД «МОСТ» (рис. 3.3) на базе программного обеспечения для анализа Prognoz Platform [см. подробнее: 46].

Говоря о задачах третьего класса, следует отметить, что к настоящему времени в практике аналитической работы ОВД примеров реализации таких СППР нет. В то же время в Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012—2014 годах отмечено, что применение средств и

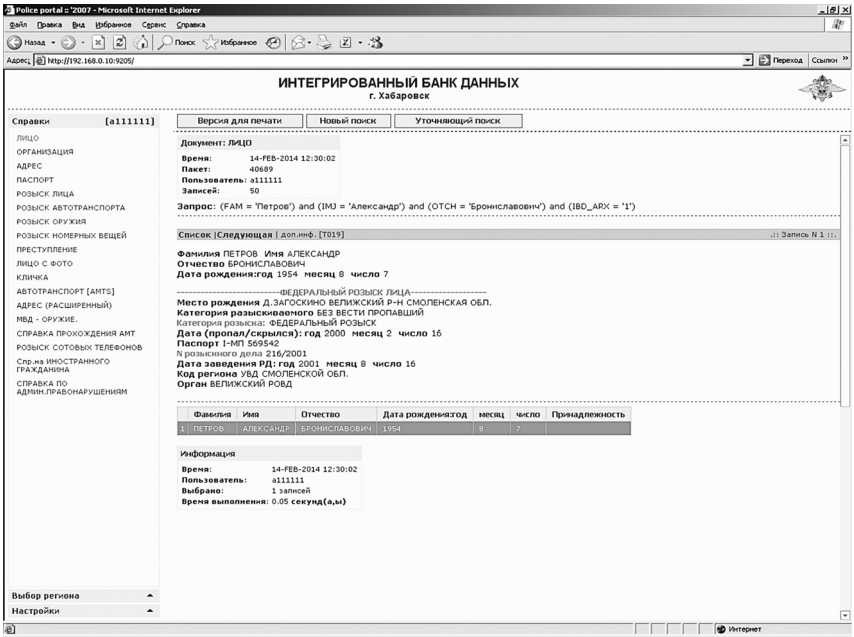


Рис. 3.2. Иллюстрация результата запроса к интегрированному банку данных

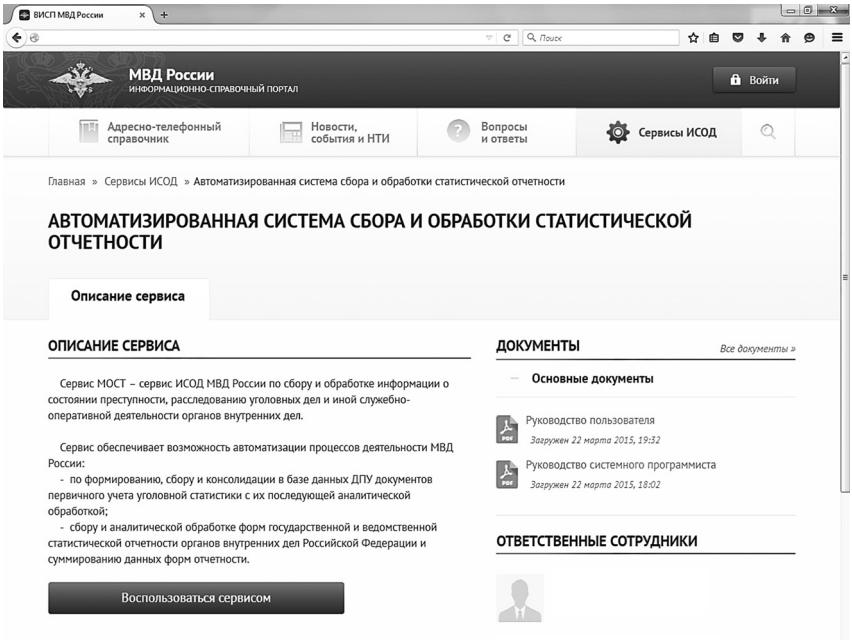


Рис. 3.3. Главная страница сервиса «МОСТ» на ВИСП ИСОД МВД России

методов интеллектуального анализа данных является одной из ключевых задач совершенствования аналитики в ОВД [28].

СППР, имеющие в своем составе математические модели, методы анализа и программные средства, позволяют лицу, принимающему решения, организовать этот процесс в интерактивном (диалоговом) режиме. При этом следует учитывать, что традиционные СППР не формулируют полностью готового решения, в лучшем случае предлагая варианты, а в основном обеспечивают лицо необходимой информацией. Это связано с тем, что основной задачей традиционных СППР является прежде всего предоставление пользователю набора специальных инструментов, а пользователь должен обладать соответствующей квалификацией для их применения. Однако результаты развития ИТ обеспечивают на современном этапе создание и использование так называемых интеллектуальных СППР, функционал которых значительно шире традиционных и дает возможность не только предоставить необходимую аналитическую информацию в удобном для принятия решений виде, но и решить такие задачи, как выявление закономерностей, построение моделей, прогнозирование развития ситуаций.

3.2. Особенности и направления применения информационных технологий интеллектуального анализа в правоохранительной деятельности

Основным назначением любой аналитической системы является предоставление аналитику специального инструментария для проверки гипотез при анализе данных. Основной задачей аналитика при этом является генерация гипотез. Он решает ее, основываясь на своих знаниях и опыте. Однако необходимым уровнем и объемом знаний обладают далеко не все сотрудники, в то время как проанализировать данные и принять адекватное решение необходимо в максимально короткий срок. Для обращения к квалифицированному специалисту-аналитику, передачи ему данных и получения результатов необходимо определенное время, которое в ходе мероприятий ОВД часто ограничено и минимально, особенно при антитеррористических операциях, поддержании общественного порядка при проведении массовых мероприятий и др.

В качестве возможного способа решения проблем такого рода *предлагается использование автоматизированных информационно-аналитических систем*, которые в режиме реального времени будут обрабатывать данные о состоянии оперативной обстановки, выявлять взаимосвязи, уточнять модели и разрабатывать прогнозы развития ситуации. При этом *наиболее интересными вариантами для работы подобных систем являются технологии интеллектуального анализа, основанные на специальных методах автоматического анализа Data Mining.*

Data Mining (буквально «добыча данных») — исследование и обнаружение машиной (программными средствами, реализующими специализированные алгоритмы, в том числе искусственного интеллекта) в исходных данных скрытых знаний, которые ранее не были известны, нетривиальны, практически полезны, доступны для интерпретации человеком [67].

Такие **обнаруженные знания обладают следующими свойствами**:

1) *новизна,* так как ценность представляют именно новые, ранее неизвестные знания;

2) *нетривиальность,* которая проявляется в неочевидности полученных закономерностей в данных, составляющих так называемые скрытые знания;

3) *практическая полезность,* состоящая в том, что найденные закономерности будут подтверждены и новыми данными с достаточно высокой степенью достоверности;

4) *понятность человеку,* которая заключается в возможности логической интерпретации, в противном случае существует вероятность случайности, а не закономерности. Здесь также важно, чтобы полученные результаты были представлены в понятном для человека виде [47].

В результате обработки исходных данных с помощью средств и методов Data Mining на основе полученных знаний **формируются модели**. Структура и виды моделей зависят от того, какие методы Data Mining применяются для их создания. Наибольшее распространение получили модели *в виде правил, деревьев решений, кластеров и математических функций*.

Методы Data Mining помогают решить многие задачи, с которыми сталкивается аналитик. Основными из них являются классификация, регрессия, поиск ассоциативных правил и кластеризация [67].

Задача классификации сводится к определению класса объекта по его характеристикам. До начала решения задачи формируется определенное множество классов, к которым будет отнесен исследуемый объект.

Задача регрессии, как и задача классификации, позволяет определить по известным характеристикам исследуемого объекта значение его ключевого параметра. Но в качестве параметра выступает не критерий отнесения к одному из классов, а величина, принимающая конкретное числовое значение из множества действительных чисел.

При *поиске ассоциативных правил* целью является нахождение частых зависимостей (или ассоциаций) между объектами или событиями. Найденные зависимости представляются в виде правил и могут быть использованы как для лучшего понимания природы анализируемых данных, так и для предсказания появления событий.

Задача кластеризации заключается в поиске независимых групп (кластеров) и их характеристик во всем множестве анализируемых данных. Ее решение помогает лучше понять данные. Кроме того, группировка однородных объектов позволяет сократить их число, а следовательно, и облегчить анализ.

В свою очередь, указанные задачи по назначению делятся на описательные и предсказательные.

Описательные (descriptive) задачи способствуют лучшему пониманию анализируемых данных. Ключевой момент в таких моделях — легкость и прозрачность результатов для восприятия человеком. Возможно, обнаруженные закономерности будут специфической чертой именно конкретных исследуемых данных и больше нигде не встретятся, но это все равно может быть полезно и потому должно быть известно. К такому виду задач относятся кластеризация и поиск ассоциативных правил.

Решение *предсказательных (predictive) задач* разбивается на два этапа. На первом на основании набора данных с известными результатами строится модель. На втором она используется для предсказания результатов на основании новых наборов данных. При этом, естественно, требуется, чтобы построенные модели работали максимально точ-

но. К данному виду задач относят задачи классификации и регрессии. Сюда можно отнести и задачу поиска ассоциативных правил, если результаты ее решения могут быть использованы для предсказания того, что произойдут некоторые события.

По способам решения задачи разделяют на supervised learning (обучение с учителем) и unsupervised learning (обучение без учителя). Такое название произошло от термина machine learning (машинное обучение), часто используемого в англоязычной литературе и обозначающего все технологии Data Mining.

В случае *supervised learning* задача анализа данных решается в несколько этапов. Сначала с помощью какого-либо алгоритма Data Mining строится модель анализируемых данных — *классификатор*. Затем классификатор подвергается обучению. Другими словами, проверяется качество его работы и, если оно неудовлетворительно, происходит дополнительное обучение классификатора. Так продолжается до тех пор, пока не будет достигнут требующийся уровень качества или не станет ясно, что выбранный алгоритм не работает корректно с данными либо же сами данные не имеют структуры, которую можно выявить. К этому типу задач относят задачи классификации и регрессии.

Unsupervised learning объединяет задачи, выявляющие описательные модели, например закономерности в покупках, совершаемых клиентами большого магазина. Очевидно, что если эти закономерности есть, то модель должна их представить, и неуместно говорить о ее обучении. Отсюда и название — unsupervised learning. Достоинством таких задач является возможность их решения без каких-либо предварительных знаний об анализируемых данных. К ним относятся кластеризация и поиск ассоциативных правил.

Теперь рассмотрим **суть решения основных задач Data Mining на примере правоохранительной деятельности**.

1. *Задачи классификации и регрессии*. При анализе часто требуется определить, к какому из известных классов относятся исследуемые объекты, то есть классифицировать их. Например, при приеме на службу в полицию сотрудник кадровой службы должен принять решение, обладает ли кандидат необходимыми качествами или нет. Очевидно, что оно принимается на основании данных об исследуемом объекте (в данном случае человеке): о его предыдущем месте работы, учебы, возрасте, составе семьи, психологических и физических параметрах, состоянии здоровья и т.п. В результате анализа этой информации сотрудник кадрового аппарата должен отнести потенциального кандидата к одному из двух известных классов — «может работать в полиции» и «не может работать в полиции».

Другим примером решения задачи классификации является фильтрация сообщений о происшествиях. В этом случае программа филь-

трации должна отнести сообщение к тому или иному уровню важности и оперативности принятия решения. Здесь основанием будет частота появления в сообщении определенных слов и словосочетаний, например «выстрелы», «наркотики», «лежит человек» и т.п.

В общем случае количество классов в задачах классификации может быть более двух. Например, в задаче распознавания номера транспортного средства таких классов может быть достаточно много (по количеству цифр и букв в регистрационном номере). Тогда объектом классификации является матрица пикселов, представляющая образ распознаваемой цифры или буквы. При этом цвет каждого пиксела является характеристикой анализируемого объекта.

В Data Mining задачу классификации рассматривают как задачу определения значения одного из параметров анализируемого объекта на основании значений других параметров. Определяемый параметр часто называют *зависимой переменной*, а параметры, участвующие в его определении, — *независимыми переменными*.

В рассмотренных примерах независимыми переменными стали:

- возраст, образование, состояние здоровья, психофизиологическая оценка и т.д.;
- частота определенных слов;
- цвет пикселов матрицы.

Зависимыми переменными в этих же примерах явились:

- способность кандидата работать в полиции (возможные значения этой переменной «да» или «нет»);
- тип сообщения (возможные значения этой переменной «важно» или «неважно»);
- цифра или буква номера транспортного средства (возможные значения этой переменной 0, 1… 9, А, Б… Я).

Необходимо обратить внимание на то, что во всех рассмотренных примерах независимая переменная принимала значение из конечного множества значений: {да, нет}, {важно, неважно}, {0, 1… 9, А, Б… Я}. Если значениями независимых и зависимой переменных являются действительные числа, то задача называется *задачей регрессии*. Примером может служить задача определения численности полицейских для охраны общественного порядка в зависимости от ряда условий.

Задачи классификации и регрессии решаются в *два этапа*.

На первом выделяется *обучающая выборка*. В нее входят объекты, для которых известны значения как независимых, так и зависимой переменных.

В примерах выше такими обучающими выборками могут быть:

- информация о кандидатах, которых ранее принимали в ОВД, и информация о прохождении ими службы;
- сообщения, классифицированные вручную как важные или как неважные;

– распознанные ранее номера автомобилей.

На основании обучающей выборки строится *модель определения значения зависимой переменной*. Ее часто называют функцией классификации или регрессии.

Для получения максимально точной функции *к обучающей выборке предъявляются следующие основные требования*:

– количество объектов, входящих в выборку, должно быть достаточно большим. Чем больше объектов, тем построенная на ее основе функция классификации или регрессии будет точнее;
– в выборку должны входить объекты, представляющие все возможные классы в случае задачи классификации или всю область значений в случае задачи регрессии;
– для каждого класса в задаче классификации или каждого интервала области значений в задаче регрессии выборка должна содержать достаточное количество объектов.

На втором этапе построенную модель применяют в отношении анализируемых объектов (объектов с неопределенным значением зависимой переменной).

Основные проблемы, с которыми сталкиваются при решении задач классификации и регрессии, — это неудовлетворительное качество исходных данных, в которых встречаются как ошибочные данные, так и пропущенные значения, различные типы атрибутов — числовые и категорические, разная значимость атрибутов, а также так называемые проблемы *over fitting* и *under fitting*. Суть первой из них заключается в том, что классификационная функция при построении «слишком хорошо» адаптируется к данным и встречающиеся в них ошибки и аномальные значения пытается интерпретировать как часть внутренней структуры данных. Очевидно, что такая модель будет некорректно работать в дальнейшем с другими данными, где характер ошибок будет несколько иной. Термином *under fitting* обозначают ситуацию, когда слишком велико количество ошибок при проверке классификатора на обучающем множестве. Отсюда вытекает, что особых закономерностей в данных не было обнаружено и либо их нет вообще, либо необходимо выбрать иной метод их обнаружения.

2. *Задача поиска ассоциативных правил*. Поиск ассоциативных правил является одним из самых популярных приложений Data Mining. Суть задачи заключается в определении часто встречающихся наборов объектов в большом множестве таких наборов. Данная задача является частным случаем задачи классификации.

Первоначально она решалась при анализе тенденций в поведении покупателей в супермаркетах. Анализу подвергались данные о совершаемых ими покупках, которые покупатели складывают в тележку (корзину). Это послужило причиной второго часто встречающегося названия — анализ рыночных корзин (Basket Analysis).

При анализе этих данных интерес представляет прежде всего информация о том, какие товары покупаются вместе, в какой последовательности, какие категории потребителей какие товары предпочитают, в какие периоды времени и т. п. Такая информация позволяет более эффективно планировать закупку товаров, проведение рекламной кампании и т. д.

Например, из набора покупок, совершаемых в магазине, можно выделить следующие наборы товаров, которые покупаются вместе:

{чипсы, пиво};

{вода, орехи}.

Следовательно, можно сделать вывод, что если покупаются чипсы или орехи, то, как правило, покупаются пиво или вода соответственно. Обладая такими знаниями, можно разместить эти товары рядом, объединить их в один пакет со скидкой или предпринять другие действия, стимулирующие покупателя приобрести товар.

Сегодня задача поиска ассоциативных правил актуальна не только в сфере торговли. Например, в сфере обслуживания граждан в ГИБДД, разрешительной или миграционной службе интерес представляет, какими услугами граждане предпочитают пользоваться в совокупности. Для получения этой информации задача решается применительно к данным об услугах, к которым обращается гражданин в течение определенного времени (месяца, года). Это помогает решить, например, как наиболее выгодно составить график работы отделений, выполнить расстановку сотрудников, разработать план обслуживания и т. д.

В аналитической деятельности исследованию могут подвергаться условия совершения преступлений и характеристики преступников на той или иной территории обслуживания ОВД. В этом случае знания о том, какие сочетания условий и характеристик встречаются наиболее часто, помогают предотвратить преступления в будущем или хотя бы помочь в их раскрытии и расследовании.

При анализе часто вызывает интерес последовательность происходящих событий. При обнаружении закономерностей в таких последовательностях можно с некоторой долей вероятности предсказывать, какие события произойдут, что позволяет принимать более правильные решения. Такая задача является разновидностью задачи поиска ассоциативных правил и называется *сиквенциальным анализом.*

Основным отличием задачи сиквенциального анализа от поиска ассоциативных правил является установление отношения порядка между исследуемыми наборами. Данное отношение может быть определено разными способами. При анализе последовательности событий, происходящих во времени, объектами таких наборов являются события, а отношение порядка соответствует хронологии их появления.

Сиквенциальный анализ можно использовать, например, в организации дорожного движения, для анализа данных о совершении дорож-

но-транспортных происшествий на различных участках транспортной инфраструктуры города. Информация о последовательности событий, предшествовавших ДТП, может помочь в выявлении проблем в организации дорожного движения и предупреждении новых транспортных проблем.

Например, если известна последовательность событий, связанных с дорожным движением:

$$\{e_5, e_2, e_7, e_{13}, e_6 \ldots e_i\},$$

где e_i — событие с кодом i,

то на основании факта появления события e_2 можно сделать вывод о скором появлении события e_7. Зная это, можно предпринять профилактические меры, делающие возникновение события e_7 невозможным или маловероятным. Если дополнительно обладать и знаниями о времени между событиями, то можно предсказать не только факт его возникновения, но и время, что часто не менее важно.

3. *Задача кластеризации*. Задача состоит в разделении исследуемого множества объектов на группы похожих, близких, называемых кластерами. Слово *кластер* английского происхождения (cluster), переводится как «сгусток», «пучок», «группа». Родственные понятия, используемые в литературе, — класс, таксон, сгущение.

Часто решение задачи разбиения множества элементов на кластеры называют кластерным анализом.

Кластеризация может применяться практически в любой области, где необходимо исследование экспериментальных или статистических данных. Рассмотрим пример из области криминологии, где решается задача анализа криминогенной обстановки.

Концептуально она основана на предпосылке, что все преступления разные. У них разные условия, участники, предметы посягательства; преступники ведут себя по-разному в процессе подготовки к совершению преступления, в процессе совершения, в процессе сокрытия следов, в процессе использования результатов преступной деятельности. В связи с этим необходимо по-разному подходить к исследованию преступлений и преступников: рассматривать различные условия, различные характеристики преступников, различные способы совершения преступлений. Для того чтобы определить, чем отличаются преступники друг от друга и как эти отличия отражаются на особенностях совершения преступлений, и производится такой анализ.

В криминологии критериями (характеристиками) разделения территорий по криминогенности являются географическое местоположение, социально-демографические характеристики, мотивы совершения преступлений и т. п.

На основании результатов разделения криминолог может определить, например, такие характеристики преступности: каковы реальная

и потенциальная способность криминогенной части населения совершать преступления, какие виды преступлений совершаются на той или иной территории чаще, что относится к основным способам совершения преступлений и т. п. На основании этих параметров криминолог может сделать вывод о необходимости проведения конкретных профилактических мероприятий, планирования и проведения профилактической работы в целом в том или ином направлении, создания условий для предотвращения преступлений определенного вида.

Кластеризация отличается от классификации тем, что для проведения анализа не требуется иметь выделенную зависимую переменную. С этой точки зрения она относится к классу *unsupervised learning*. Эта задача решается на начальных этапах исследования, когда о данных мало что известно. Ее решение помогает лучше понять данные, и с этой точки зрения задача кластеризации является описательной.

Для задачи кластеризации характерно отсутствие каких-либо различий как между переменными, так и между объектами. Напротив, ищутся группы наиболее близких, похожих объектов. Методы автоматического разбиения на кластеры редко используются сами по себе, просто для получения групп схожих объектов. После определения кластеров применяются другие методы Data Mining, для того чтобы попытаться установить, а что означает такое разбиение, чем оно вызвано.

Кластерный анализ позволяет рассматривать достаточно большой объем информации и резко сокращать, сжимать большие массивы данных, делать их компактными и наглядными.

Отметим *ряд особенностей, присущих задаче кластеризации*.

Во-первых, решение сильно зависит от природы объектов данных (и их атрибутов). Так, с одной стороны, это могут быть однозначно определенные, четко количественно очерченные объекты, а с другой — объекты, имеющие вероятностное или нечеткое описание.

Во-вторых, решение значительно зависит также и от представления кластеров и предполагаемых отношений объектов данных и кластеров. Так, нужно учитывать такие свойства, как возможность/невозможность принадлежности объектов нескольким кластерам. Необходимо определение самого понятия принадлежности кластеру: однозначная (принадлежит/не принадлежит), вероятностная (может принадлежать), нечеткая (важна степень принадлежности).

С учетом рассмотренных особенностей решения задач анализа данных на основе методов Data Mining остановимся на **основных направлениях их использования в правоохранительной деятельности**.

Известные производители программного обеспечения, такие как IBM, Oracle, Microsoft, предлагают программные продукты, предназначенные для осуществления услуг и формирования решений в области *прогностической аналитики*. Основными функциями таких систем

являются сбор данных, моделирование, анализ текстов, статистический анализ, визуальный анализ.

Процесс прогностической аналитики включает этапы сбора данных, преобразования, статистического анализа, моделирования, прогнозирования, формирования решений и предложений.

Применение специализированных программных систем в качестве аналитических информационных систем позволяет в сфере деятельности ОВД эффективно решать такие задачи, как планирование оперативных ресурсов, предупреждение рецидивов, расследование преступлений, предупреждение тяжких преступлений, прогнозирование профессиональной пригодности сотрудников полиции [68].

Остановимся на указанных задачах подробнее.

1. *Планирование оперативных ресурсов*. На основе накопленных данных о правонарушениях по районам, о текущей оперативной обстановке (время суток, погода, количество людей, например массовое скопление), оперативных сигналов о готовящихся нарушениях строится прогноз о возможном месте, времени и характере потенциальных происшествий. В результате обработки, анализа полученной информации, построения и оценки прогнозов принимаются решения о направлении сотрудников патрульной службы на место, о предупреждении их о характере угроз и т.п., то есть полицейские направляются туда, где они будут необходимы.

Так, в 2006 г. подобная аналитическая система была внедрена в департаменте полиции г. Ричмонда (США). Основной целью при этом являлось повышение эффективности использования человеческих ресурсов и предотвращение тяжких преступлений. В качестве программного средства использовались *прогностические модели на основе технологий IBM SPSS*.

В наиболее общем виде функционирование такой системы можно представить следующим образом:

1) происходит сбор данных из различных источников: предпосылки (массовые мероприятия, выдача зарплаты, выходные), криминальная статистика (происшествия, преступники, дата/время, участки), влияющие факторы (погодные условия, присутствие полиции);

2) с помощью инструментария аналитической системы выполняется анализ и моделирование ситуаций на основе классификационных (скоринговых) моделей, в режиме реального времени при помощи специальных запросов производится классификация ситуации;

3) на основе результатов классификации (скоринга) осуществляется оперативное планирование и управление силами полиции, то есть усиливаются наряды, направляются патрули в места предполагаемых беспорядков, тем самым предотвращаются преступления и правонарушения.

Таким образом, при помощи указанной технологии осуществляется прогнозирование районов и времени совершения правонарушений и возникновения беспорядков. В течение первого года работы системы в Ричмонде на 32% снизилось число убийств, на 20% — число изнасилований, на 18% — число разбойных нападений.

Аналогичное решение было внедрено и в департаменте полиции г. Мемфиса (США). В результате без увеличения численности личного состава достигли существенного снижения уровня имущественных преступлений и преступлений, связанных с насилием, — на 15,8%. Также на основании результатов анализа и прогнозирования оперативной обстановки была осуществлена спецоперация, в ходе которой было произведено 50 арестов. Это дало снижение уровня преступности на 36,8% в отдельном микрорайоне Мемфиса.

2. *Прогнозирование профессиональной пригодности*. С помощью средств Data Mining, входящих в состав аналитических программных систем, возможно решать задачи определения степени профессиональной пригодности кандидатов на службу в ОВД или сотрудников, назначаемых на вышестоящие (или руководящие) должности в системе МВД России.

В качестве исходных данных для последующего анализа и прогнозирования можно использовать, например, результаты психологических тестов и данные послужных списков. В процессе анализа оценивают предполагаемую результативность работы, возможность превышения полномочий и др. Полученные оценки и данные прогнозов учитываются уже в подготовке и принятии управленческих решений по личному составу.

3. *Расследование преступлений*. С помощью аналитических систем на основе сведений, полученных при едином учете преступлений, можно не только формировать разнообразные отчеты. В частности, на основе данных по отдельным преступлениям и лицам, их совершившим, можно спрогнозировать (сузить круг) потенциальных преступников среди уже известных лиц с криминальным прошлым. Используя полученные данные, следует провести мероприятия по проверке таковых в первую очередь. Также можно исследовать так называемый почерк совершенного преступления, сравнивая с образом действий уже известных преступников, сведения о которых имеются в базах данных ОВД, и существенно сузить круг подозреваемых.

Так, в департаменте полиции West Midlands (Великобритания) была внедрена аналитическая система, реализующая технологии Data Mining. Работа этой системы направлена на выявление преступлений, которые были совершены одним и тем же преступником, на основе поиска закономерностей в раскрытых и сопоставления их с данными

о нераскрытых преступлениях и с описаниями преступников в базе данных.

4. *Предупреждение тяжких преступлений*. При решении этой задачи на основе данных о совершении мелких и крупных правонарушений и их привязке к конкретным преступникам и условиям производится расчет и строятся прогнозы трансформации существующих форм преступлений в более тяжкие, в частности с применением насилия, оружия, связанных с наркотическими средствами.

В результате проводится активная работа в отношении конкретных мелких преступлений для профилактики тяжких. Таким образом, основная идея здесь состоит в выявлении мелких преступлений, которые могут развиться в более серьезные.

5. *Предупреждение рецидивов*. Используя данные по каждому освободившемуся заключенному, а также сведения о совершенных им преступлениях, специфике пребывания в исправительном учреждении, наличии либо отсутствии рецидивов после выхода на свободу, можно оценить вероятность рецидива. В итоге действия полиции должны быть направлены на более строгий надзор за освободившимися, включение их в программы реабилитации и помощи в социальной адаптации, иными словами, — на эффективную профилактику совершения повторных преступлений.

Таким образом, одно из перспективных направлений интеллектуального анализа — методы Data Mining. Они в полной мере отвечают требованиям к современным аналитическим технологиям в условиях обработки большого объема данных. Такие задачи, как классификация и регрессия, являются наиболее распространенными для аналитиков. Инструменты интеллектуального анализа позволяют решать их в автоматическом режиме с использованием ряда апробированных алгоритмов. Так, методы и средства Data Mining дают возможность выполнить ряд задач в сфере деятельности ОВД. Это планирование расстановки сил и средств на обслуживаемой территории, оценка профессиональной пригодности сотрудников как при приеме на службу, так и при назначении на вышестоящие должности, определение похожих преступлений и выработка тактики их расследования, предупреждение преступлений.

Возможным направлением применения Data Mining в управлении подразделениями ОВД является включение в состав СППР функциональных компонентов интеллектуального анализа. Такое решение в состоянии обеспечить процесс принятия решений необходимой аналитической информацией, содержащей сведения о зависимостях между рассматриваемыми явлениями, результатах прогнозирования развития изучаемых процессов.

3.3. Программные средства интеллектуального анализа

Безусловно, использование методов Data Mining требует от аналитика серьезной, в том числе математической, подготовки. Однако к настоящему времени разработан ряд приложений — программных систем, реализующих алгоритмы Data Mining. Такие программы позволяют успешно решать задачи анализа данных специалисту, имеющему базовый уровень подготовки в области ИТ.

Мы рассмотрим две из таких систем.

1. Такое программное средство анализа данных на основе алгоритмов Data Mining, как **система See5** компании RuleQuest [См. подробнее: 91], предназначена для анализа больших баз данных, содержащих до сотни тысяч записей и до сотни числовых или номинальных полей. Результат работы выражается в виде деревьев решений и множества правил if… then (если… то). Система проста в обращении и не требует от пользователя специальных знаний в области прикладной статистики.

Проиллюстрируем процесс и основные результаты работы See5 на примере оценки состояния и прогнозирования оперативной обстановки деятельности правоохранительных органов по охране общественного порядка в условиях проведения массовых мероприятий (митинги, шествия, футбольные матчи и т.п.).

Исходные данные в рассматриваемом случае относятся к различным вариантам развития ситуаций, связанных с проведением массовых мероприятий.

Фрагмент исходных данных приведен в табл. 3.1.

Таблица 3.1

Фрагмент исходных данных развития ситуаций, связанных с проведением массовых мероприятий

Признак, имя переменной в системе	**Объект 1**	**Объект 2**
Ситуация, STN	Отдельные нарушения порядка (VLR)	Массовые беспорядки (CHS)
Возраст участников (средний), AGE	37 лет	40 лет
Количество участников, NUM	2700 чел.	9600 чел.
Площадь проведения мероприятия, SQR	0,08 км^2	0,06 км^2
Вид мероприятия, EVT	PCY (политическое)	PBL (культ-массовое)

Окончание табл. 3.1

Признак, имя переменной в системе	**Объект 1**	**Объект 2**
Время суток, DAY	Утро (MON)	День (AFN)
День проведения (выходной, праздник), KND	Праздник (SEL)	Выходной (WKD)
Фаза луны, MON	Полнолуние (FUL)	Убывающая луна (DES)
Погода, WTH	Ясно (CLR)	Осадки (RNS)
Уровень безработных в регионе, NWK	5,02	2,52
Доход (отношение средней зарплаты к прожиточному минимуму), INC	3,04	1,64
Пассивность — активность участников, ACT	0	2
Недовольство — лояльность участников, DCS	–2	–4
Численность сотрудников, FRS	279 чел.	548 чел.
Вооружение сотрудников, WPN	Слезоточивый газ «Черемуха» (GAS)	ПР-1 (RBR)

Это как раз тот вид данных, для обработки которых более всего подходит See5. Каждый объект (конкретное массовое мероприятие) здесь принадлежит к одному из небольшого числа классов (1 — не выходит за рамки закона, 2 — имеются отдельные случаи нарушения общественного порядка, 3 — имеют место массовые беспорядки) и описывается четырнадцатью разнотипными признаками.

Задача See5 состоит в предсказании диагностического класса какого-либо объекта по значениям его признаков. При этом, мы увидим, как See5 конструирует классификатор в виде *дерева решений*, которому, в свою очередь, может быть поставлено в соответствие некоторое множество логических правил.

Предварительный этап работы с системой требует подготовки исходных данных. Здесь имеется *ряд ограничений*.

Каждой задаче, решаемой в системе See5, необходимо присвоить собственное имя. Пусть в нашем случае это имя будет MAS (от **m**ass **a**ctions). В процессе решения See5 использует и формирует несколько файлов с одинаковым именем и различными расширениями. Очень важно точно соблюдать правила записи имен и расширений (система

различает строчные и прописные буквы). Кроме того, отметим, что See5 поддерживает *только латинские шрифты*.

Для работы See5 требуются два файла — файл имен переменных и файл данных.

В *файле имен переменных* с расширением *.names задаются названия используемых признаков и классов.

Файл имен переменных MAS.names применительно к нашей задаче выглядит следующим образом:

```
STN.    | the target attribute
STN:    STB,   VLR,  CHS
AGE:    continuous
NUM:    continuous
SQR:    continuous
EVT:    PCY,   SPT,  PBL
DAY:    MON,   AFN,  EVN,  NGT
KND:    WKD,   WND,  SEL,  CRS
MON:    NEW,   FUL,  GRW,  DES
WTH:    CLR,   CLD,  RNS
NWK:    continuous
INC:    continuous
ACT:    continuous
DSC:    continuous
FRS:    continuous
WPN:    RBR,   WTR,  GAS,  FIR
```

Целевой признак STN принимает три значения: STB — в классе «не выходит за рамки закона», VLR — в классе «имеются отдельные случаи нарушения общественного порядка» и CHS — «имеют место массовые беспорядки».

Количественные признаки: AGE (возраст), NUM (количество участников), SQR (площадь места проведения), NWK (уровень безработных), INC (показатель дохода как отношение средней зарплаты к прожиточному минимуму), ACT (показатель пассивности — активности участников по шкале от –5 до 5 соответственно), DCS (показатель недовольства — лояльности участников по шкале от –5 до 5 соответственно) и FRS (численность сотрудников, участвующих в охране порядка). Признак EVT (вид мероприятия) может иметь три значения: PCY (политическое), SPT (спортивное) и PBL (культурно-массовое); признак DAY (время суток) — четыре значения: MON (утро), AFN (день), EVN (вечер) и NGT (поздний вечер, ночь); признак KND (время суток) — четыре значения: WKD (рабочий день), WND (выходной), SEL (праздничный) и CRS (религиозный празд-

ник); признак MON (фаза луны) — четыре значения: NEW (новолуние), FUL (полнолуние), GRW (растущая луна) и DES (убывающая луна); признак WTH (погода) — три значения: CLR (ясно), CLD (пасмурно) и RNS (осадки); признак WPN (вооружение) — четыре значения: RBR (резиновая палка), WTR (водомет), GAS (слезоточивый газ) и FIR (огнестрельное оружие).

Важно также, что порядок записи имен переменных должен соответствовать их порядку в файле данных.

Вторым файлом, необходимым для работы See5, является *файл данных*. Он имеет расширение *.data. В нашем случае это файл MAS.data.

Каждому объекту в файле данных соответствует собственная строка. Если значение целевой переменной находится вверху файла имен переменных, то строка начинается со значения этой целевой переменной. Затем через запятую следуют значения всех остальных признаков. В случае если значения переменных отсутствуют (неизвестны), то вместо значения ставится знак «?».

На рис. 3.4 приводится фрагмент файла MAS.data, который мы будем использовать для демонстрации возможностей See5.

Помимо двух основных файлов в системе предусмотрена возможность использования *дополнительных тестовых данных* для проверки точности классификации и информации о стоимости ошибок классификации.

После запуска системы See5 на экране отображается главное окно (рис. 3.5.).

В верхней части окна программы располагаются *кнопки, реализующие основные действия*.

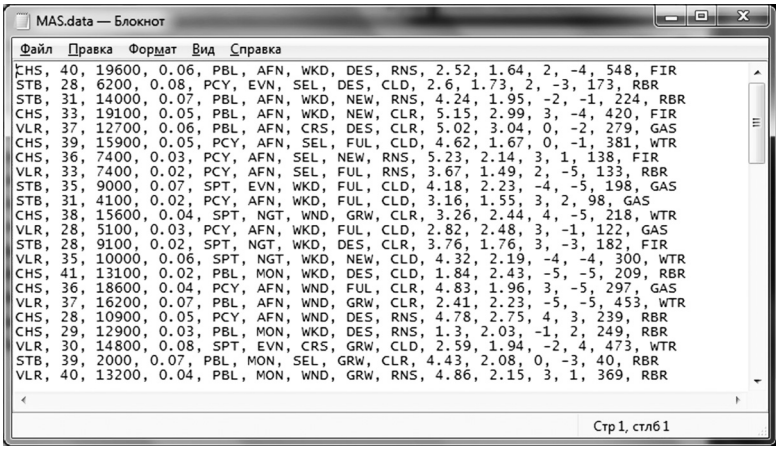


Рис. 3.4. Фрагмент файла MAS.data

Рис. 3.5. Главное окно системы See5

С помощью кнопки (Locate Data, местонахождение данных) вызывается окно для просмотра доступных файлов данных и их загрузки в систему.

Нажатием кнопки (Construct Classifier, построение классификатора) производится обращение к окну диалога для выбора типа классификатора и установки его параметров.

Кнопка (Stop, остановка) — предназначена для остановки процесса построения дерева решений.

Кнопка (Use Classifier, использование классификатора) запускает процесс интерактивной классификации одного или более объектов.

С помощью кнопки (Cross-Reference, перекрестная ссылка) вызывается окно, в котором наглядно раскрываются связи между объектами обучающей выборки и найденными правилами их классификации.

После загрузки данных с помощью кнопки и нажатия кнопки система выдает окно результатов, которое выглядят следующим образом (рис. 3.6).

В следующих строках отчета отображено построенное дерево решений. Его можно проинтерпретировать следующим образом:

ЕСЛИ **DAY** (время дня) равно NGT (поздний вечер) и
AGE (средний возраст участников) не больше 28, ТО класс
STB (все законно),
иначе

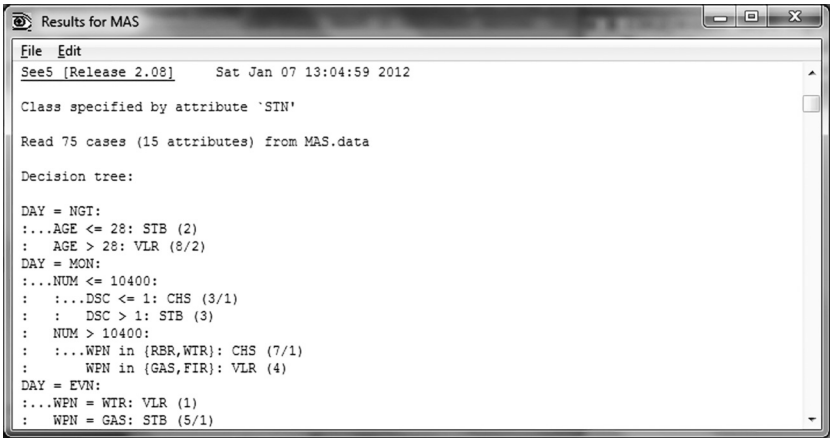


Рис. 3.6. Результаты работы See5 — построение дерева решений

ЕСЛИ **DAY** (время дня) равно NGT (поздний вечер) и **AGE** (средний возраст участников) больше 28, ТО класс **VLR** (отдельные нарушения порядка),

иначе

ЕСЛИ **DAY** (время дня) равно MON (утро) и **NUM** (количество участников) не больше 10400 и **DCS** (недовольство — лояльность) не больше 1, ТО класс **CHS** (массовые беспорядки),

и т. д.

Каждая ветка дерева заканчивается указанием *номера класса*, к которому она приводит. Сразу за номером следует запись вида (n/m). Например, самая первая ветка заканчивается записью STB (2). Это означает, что данной ветке соответствуют 2 объекта из опре
деленного (STB) класса. Вторая ветка заканчивается записью VLR (8/2), из чего следует, что эта ветка описывает класс VLR и сюда попадают 8 объектов, из которых 2 попадают ошибочно. Величины n или m могут оказаться дробными в случае, когда на какую-либо ветку придется некоторое число объектов с неизвестными значениями признаков.

В ряде случаев полученное дерево решений может оказаться слишком сложным для восприятия. Например, при решении задач с множеством параметров дерево нередко получается с большим числом ветвей и довольно запутанным. Вместо того чтобы «ползать» по каждой полученной ветке, в системе See5 предусмотрен *вариант преобразования дерева решений в набор правил if... then*.

Для этого в системе имеется возможность включения в отчет списка правил, соответствующих рассчитанному дереву решений. Приме-

нительно к рассматриваемым данным о массовых беспорядках такой список будет выглядеть, как на рис. 3.7.

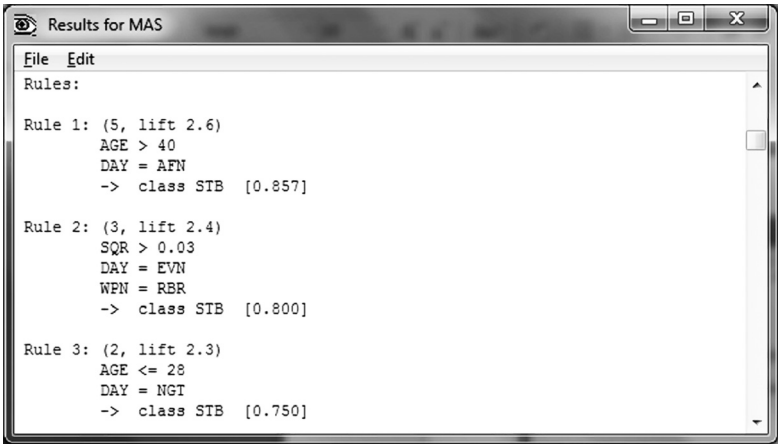


Рис. 3.7. Список правил if… then в окне результатов

Построенное множество правил применяется для принятия решения о принадлежности того или иного объекта к какому-либо классу. При этом бывают ситуации, когда один и тот же объект подпадает под действие сразу нескольких правил, в том числе правил, описывающих разные классы. Подобные *внутренние конфликты могут быть разрешены двумя способами*. При первом способе предпочтение отдается одному правилу, имеющему более высокую
степень доверия (более высокую точность). Второй способ связан с обобщением результатов разных правил для принятия окончательного решения.

В системе See5 принят второй способ: каждое сработавшее правило «подает голос» для отнесения какого-либо объекта к изучаемым классам. Голоса суммируются с весами, равными вычисленным степеням доверия, и объект считается принадлежащим к классу, для которого набирается наибольшая взвешенная сумма голосов.

Система имеет *ряд возможностей для улучшения качества классификации*. Это касается точности результатов, повышения их устойчивости к возможным флуктуациям значений признаков, изменения степени доверия правилам и т. д. Такие возможности делают систему более гибкой и универсальной.

После того как получен окончательный набор правил, пользователю предоставляется *возможность испытать этот вариант в интерактивном режиме на новых данных*. Для этого в главном окне See5 требуется нажать кнопку для запуска алгоритма классифика-

ции данных, соответствующего самому последнему варианту дерева решений. На экране появляется специальное окно для ввода значений поочередно предъявляемых признаков (рис. 3.8).

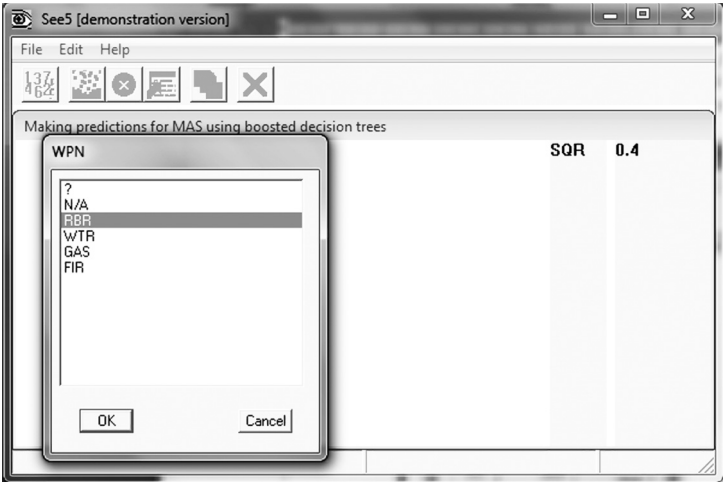


Рис. 3.8. Отображение в интерактивном режиме классификации данных

Следует обратить внимание на тот факт, что количество таких признаков может быть разным, ведь в зависимости от ответов реализуется та или иная ветвь дерева решений. После ввода всех затребованных значений на экран выдается окно, в котором указываются предсказанный класс и уровень доверия к результату классификации (рис. 3.9).

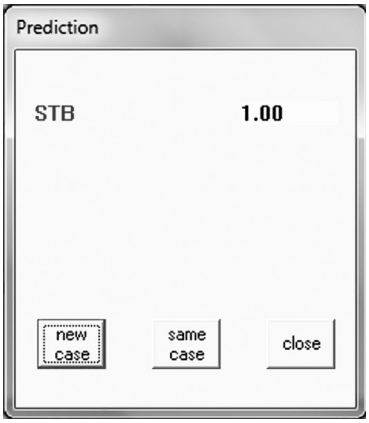


Рис. 3.9. Отображение результата классификации

2. Еще одним из инструментов Data Mining является **система WizWhy** компании WizSoft [см. подробнее: 93], функционирование которой основано на *ограниченном переборе*.

Алгоритмы ограниченного перебора были предложены в середине 60-х гг. XX в. М.М. Бонгардом для поиска логических закономерностей в данных. С тех пор они продемонстрировали эффективность при решении множества задач из самых различных областей [47; 67; 70].

Эти алгоритмы вычисляют частоты комбинаций простых логических событий в подгруппах данных. Примеры таких событий: $X = a$; $X < a$; $X > b$, $a < X < b$ и др., где X — какой-либо параметр, a и b — константы. Ограничением служит длина комбинации простых логических событий. На основании анализа вычисленных частот делается заключение о полезности той или иной комбинации для установления ассоциации в данных, для классификации, прогнозирования и т.п.

Наиболее важным результатом работы системы является *генерация правил if... then*. Максимальная длина комбинации в правиле в системе WizWhy равна шести. В соответствии с работой алгоритма производится *эвристический поиск простых логических событий*, на которых потом строится весь анализ.

Система WizWhy является на сегодняшний день одним из лидеров на рынке продуктов Data Mining. Это не лишено оснований: она демонстрирует более высокие показатели при решении ряда практических задач, чем все остальные алгоритмы.

В целом *функции данной системы* совпадают с рассмотренными выше у See5. Однако есть и некоторые отличия. Так WizWhy позволяет оценить вероятность ошибки для каждого правила, прогностическую силу каждого из анализируемых признаков, а также выявить необычные феномены в данных — так называемые неожиданные правила.

Первым шагом на пути интеллектуального анализа с помощью системы WizWhy является *загрузка анализируемых данных*. Здесь имеется несколько возможностей:

- использовать текстовые файлы в формате ASCII;
- напрямую обращаться к базам данных в файлах СУБД Microsft Access, таблицах СУБД Oracle и Microsoft SQL Server;
- воспринимать наборы данных посредством ODBC (Open Database Connectivity).

Для начала работы с процедурой загрузки следует прежде всего обратиться к закладке Basic Data в окне диалога с именем текущего проекта (рис. 3.10). Здесь в поле Open Data of Type нужно указать тип загружаемых данных.

В качестве примера воспользуемся теми же данными, что и для иллюстрации работы системы See5, отражавшими ситуации, связанные с массовыми беспорядками.

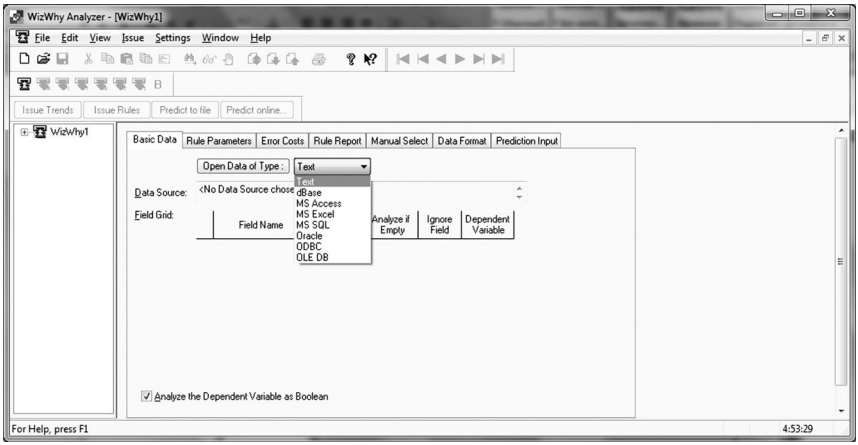


Рис. 3.10. Начало процедуры загрузки данных в систему WizWhy

Эти данные представлены в текстовом файле формата ASCII. В файле такого формата разделителями колонок является знак табуляции, а в первой строке должны быть записаны имена переменных. Вид файла в редакторе «Блокнот» представлен на рис. 3.11.

В процессе настройки загрузки система потребует уточнить тип разделителей колонок и расположение строки с именами переменных. После загрузки (импорта) данные отображаются на вкладке Basic Data (рис. 3.12).

Одной из интересных особенностей системы WizWhy является *учет пустых значений*, то есть пропуски в таблице данных (пустые ячейки) — это самостоятельные информативные события. Для учета подобных пропусков в значениях какой-либо переменной следует установить флажок в колонке Analyze if Empty, а для исключения переменной из анализа — в колонке Ignore Field.

В нашем примере переменные — целевой признак STN, признаки EVT (вид массового мероприятия), DAY (время суток), KND (вид дня проведения мероприятия), MON (фаза луны), WTH (погодные условия) и WPN (вид вооружения) — должны иметь тип данных Category (номинальный). Иногда если в качестве признака используется номер класса, то *обязательно* следует установить Category. Остальные переменные — AGE (средний возраст участников), NUM (количество участников), SQR (площадь проведения мероприятия), NWK (уровень безработицы), INC (показатель дохода), ACT (пассивность — активность участников), DSC (недовольство — лояльность участников) и FRS (количество задействованных сотрудников) — Number (количественные).

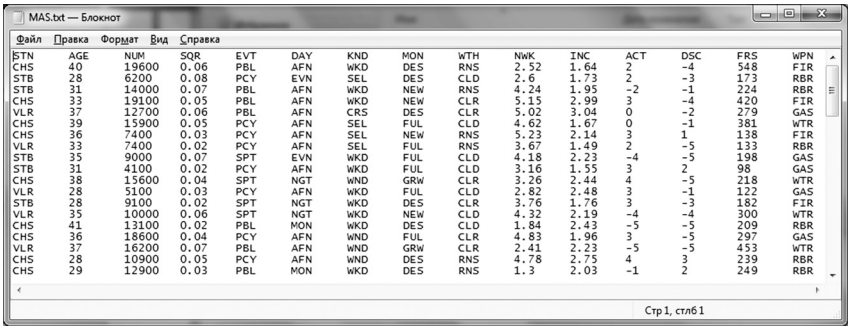


Рис. 3.11. Файл с данными для WizWhy в формате ASCII

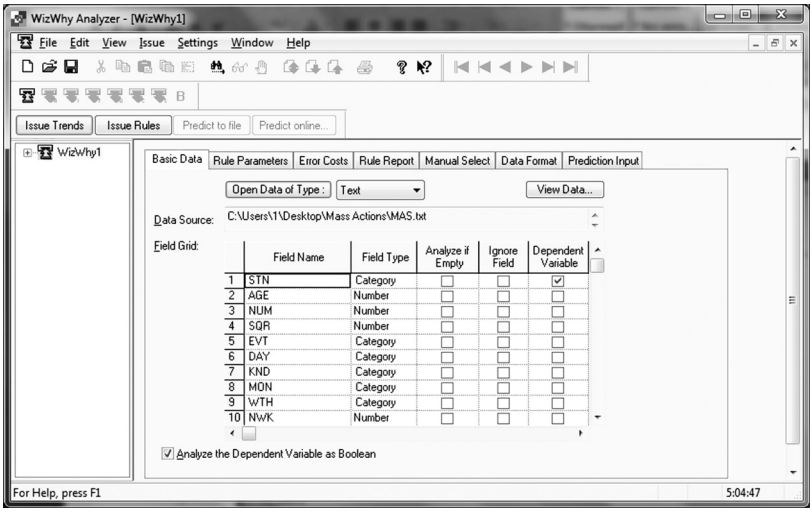


Рис. 3.12. Окно диалога WizWhy для управления данными

После завершения загрузки данных необходимо *настроить процедуру поиска правил*. Настройка заключается в задании ряда параметров.

В системе WizWhy целевой признак разделяет все множество объектов на две части. В рассматриваемом примере целевой признак STN — номинальный. Он принимает три значения: STB — в классе «все законно»; VLR — в классе «отдельные нарушения порядка» и CHS — в классе «массовые беспорядки». Так как в WizWhy необходимо разделить значения целевой переменной на две части, то будем искать в данных if… then правила для объектов, относящихся к «массовым беспорядкам». Для этого, выбрав закладку Rule Parameters (параметры правил), установим значение CHS в поле Predicted Value (рис. 3.13).

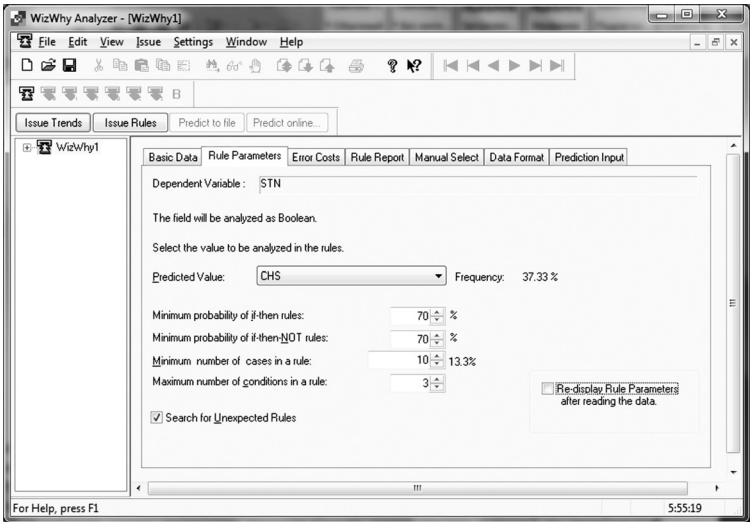


Рис. 3.13. Окно диалога WizWhy для задания параметров поиска правил

Также важным шагом в процессе настройки параметров правил является *настройка точности правила*. Это Minimum probability of if-then rules (минимальная вероятность правил if… then) и Minimum probability of if-then-NOT rules (минимальная вероятность правил if… then not.

Для нашего примера укажем в соответствующих полях одинаковые цифры — 70%. Это означает, что системе WizWhy формулируется требование обнаруживать правила, которые будут ошибаться не более чем в 30% случаев (имеются в виду ошибки по анализируемой выборке). В принципе, можно задавать любые значения минимальных вероятностей от 0 до 100%, но следует понимать, что, задав слишком низкий уровень точности, мы получим большое количество правил, среди которых будет много малоинформативных. В свою очередь, выставив требование 100%, мы, скорее всего, не получим вообще ничего.

Остальные настройки оставим без изменений, согласившись со значениями по умолчанию. Более подробное описание настройки поиска правил в системе WyzWhy можно посмотреть в учебном курсе В. Дюка, А. Самойленко [59].

После завершения настройки можно приступить к поиску правил в загруженных данных. Для этого нужно нажать кнопку Issue Rules (выдача правил) в главном окне. После завершения обработки данных на экране появится окно с информацией о найденных правилах (рис. 3.14).

Здесь имеется возможность вернуться к настройке, нажав Reduce Rules. Например, можно уточнить ряд параметров (количество правил, уровень значимости, вероятность и др.). Нажатие кнопки OK приводит к завершению поиска правил и возврату к главному окну системы.

Для просмотра результатов необходимо выбрать пункт Summary R (Summary Report), при этом откроется окно 2 – Summary Report (рис. 3.15).

В итоговом отчете содержится обобщенная информация как о заданных параметрах поиска, так и о средней (априорной) вероятности прогнозируемого значения переменной.

Наибольший же интерес представляет *отчет о правилах*. Для просмотра этого отчета следует выбрать пункт If-Then Rul (If-Then Rules Report). Результирующий список состоит из правил, упорядочен-

Рис. 3.14. Сообщение WizWhy о найденных правилах

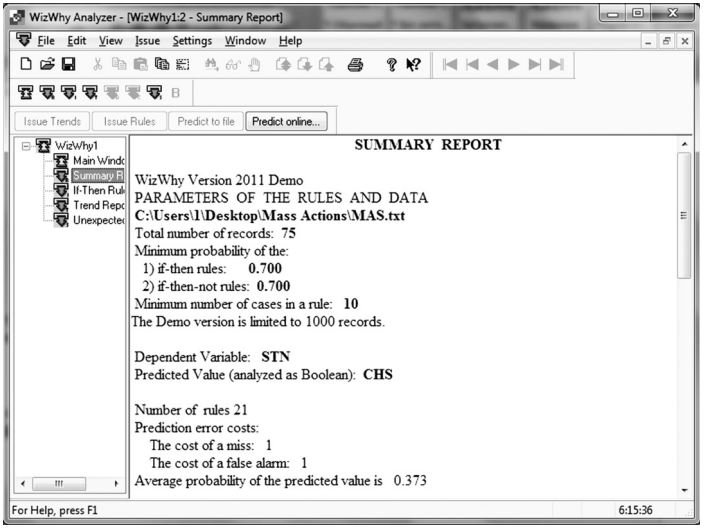


Рис. 3.15. Общий вид отчета о правилах в системе WizWhy

ных по заданному критерию (по умолчанию это число объектов, описываемых правилом). В данных по массовым беспорядкам при установленных параметрах процедуры система WizWhy обнаружила 21 правило. Фрагмент отчета приведен в следующем листинге:

IF-THEN RULES REPORT

IF-THEN RULES:

1) *If* **MON** *is* **GRW**
Then
STN *is not* **CHS**
Rule's probability: **0,867**
The rule exists in **13** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers):
17, 20, 21, 22, 24, 26, 28, 29, 32, 52
Negative Examples (records' serial numbers):
11, 65

2) *If* **WTH** *is* **CLD**
and **DSC** *is* **2,00 … 5,00** (average = **3,09**)
Then
STN *is not* **CHS**
Rule's probability: **0,909**
The rule exists in **10** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers):
10, 20, 28, 29, 32, 34, 38, 44, 48, 70
Negative Examples (records' serial numbers):
51

3) *If* **WPN** *is* **GAS**
Then
STN *is not* **CHS**
Rule's probability: **0,783**
The rule exists in **18** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers):
5, 9, 10, 12, 23, 29, 30, 33, 34, 36
Negative Examples (records' serial numbers):
16, 31, 51, 64, 72

Для пояснения полученных результатов рассмотрим более подробно, например, правило № 2 из фрагмента отчета.

Оно представляет собой конъюнкцию двух элементарных высказываний. Первое — **WTH** *is* **CLD** — говорит о том, что правило относится только к указанному типу погодных условий. Второе — **DSC** *is* **2,00 … 5.00** — определяет диапазон значений для параметра недовольства — лояльности участников мероприятия. Высказывание **STN** *is not* **CHS** означает, что правило характерно для объектов (ситуаций), не относящихся к классу CHS («массовые беспорядки»).

Запись *Rule's probability:* **0.909** означает, что точность правила в данном случае равна 0,909. Следующая запись — *The rule exists in* **10** *records* — характеризует объем множества объектов, для которых справедливо рассматриваемое правило, а другая запись — *Significance Level: Error probability < 0.1* — касается статистической оценки уровня значимости полученного правила (как видим, доверие к нему превышает 90%). Предпоследняя запись — *Positive Examples (records' serial numbers):* — означает «положительные примеры», которые затем представлены как номера записей (объектов) в наборе данных: ***10, 20, 28, 29, 32, 34, 38, 44, 48, 70***. Наконец, последняя запись — *Negative Examples (records' serial numbers):* — означает «отрицательные примеры», которые затем представлены как номера записей (объектов) в наборе данных, не попавших под действие правила: ***51***.

В системе WizWhy предусмотрена также возможность экспорта и сохранения полученных правил в виде операторов на языке *SQL*. Для этого необходимо в системном меню выбрать Edit → Select Rules for SQL и один из вариантов выделения правил (например Select All Rules), затем Issue → SQL Statement… — система выдаст окно диалога, показанное на рис. 3.16. В этом окне можно редактировать совокупность операторов и с помощью переключателей адресовать ее в текстовый файл либо в буфер обмена.

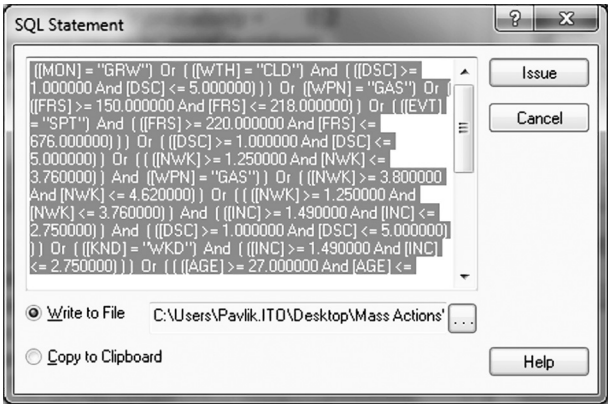


Рис. 3.16. Вывод правила в виде последовательности SQL-операторов

Определенный интерес представляет отчет о трендах, для просмотра и анализа которого требуется выбрать пункт Trend Report (кнопка Trend Repc). Отчет отображает результаты сегментации отдельных признаков (рис. 3.17).

Окно отчета разделено на три области. В области, расположенной в левом верхнем углу, мы задаем анализируемый признак (Field to be analyzed). Здесь можно не только выбирать требующийся признак, но и сортировать признаки по какому-либо критерию (в алфавитном порядке, по номеру поля, по информативности).

Оставшиеся две области предназначены для отражения отношений между значениями признака и зависимой переменной. В верхней правой области окна отчета даются статистические характеристики сегментов выделенного признака. В нижней области приводится графическая иллюстрация информативности каждого сегмента.

На графике по горизонтальной оси располагаются сегменты, на которые выбранные признаки автоматически разбиваются системой WizWhy. По вертикальной оси откладывается отношение количества объектов класса if… then к общему количеству объектов, попадающих в сегмент. Таким образом, высота столбиков на графике отражает информативность сегментов. Если столбик выше горизонтальной черты, значит, в данный сегмент чаще попадают объекты класса if… then, а если ниже горизонтальной черты — класса if… then not. В свою очередь, ширина столбиков пропорциональна количеству объектов, относящихся к данному сегменту.

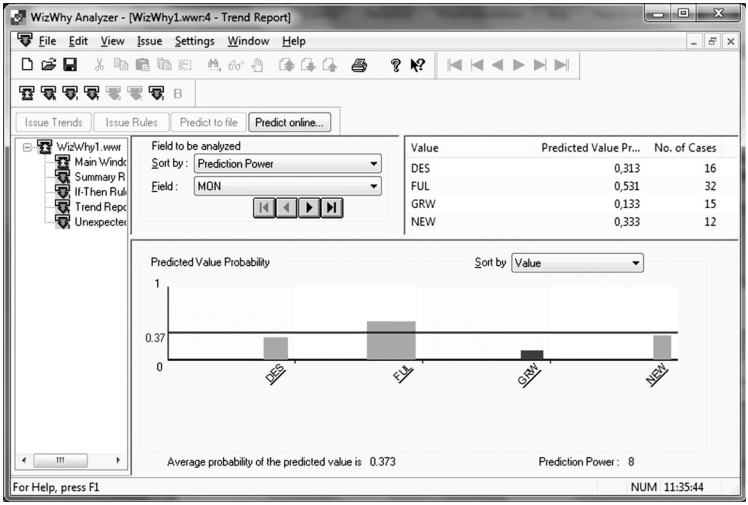


Рис. 3.17. Отчет о трендах в системе WizWhy

Основываясь на данных графика, в нашем случае можно заключить, что на ситуацию, относящуюся к классу CHS (массовые беспорядки), существенное влияние оказывает фаза полнолуния (FUL) и, наоборот, не оказывает влияние фаза растущей луны (GRW).

Как упоминалось в начале обзора данной системы, одним из преимуществ является *формирование представлений о неожиданных правилах*. Под неожиданными понимаются правила в виде конъюнкции двух и более простых высказываний, комбинация которых дает точность и полноту прогноза выше, чем можно было бы ожидать при независимости простых высказываний. Это представление позволяет открывать в данных нетривиальные закономерности.

В нашем случае система обнаружила три неожиданных правила, отчет о которых выдается в окне (рис. 3.18).

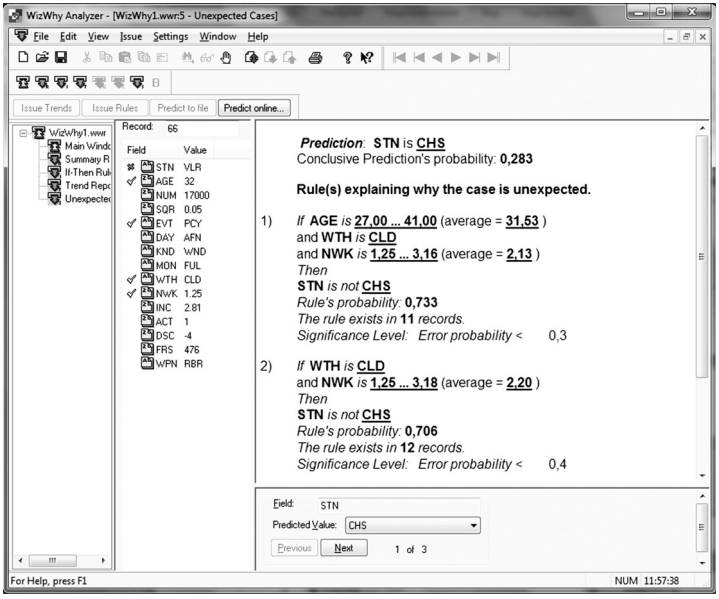


Рис. 3.18. Отображение отчета о неожиданных правилах в системе WizWhy

Окно отчета о неожиданных правилах разделено на три секции. В правой верхней отображаются в стандартной форме найденные неожиданные правила. Левая секция содержит информацию об элементах, из которых составлено неожиданное правило. А в нижней правой секции в поле Predicted Value: No CHS можно выбрать вид значения признака CHS или NoCHS.

Так, в примере на рис. 3.18 первое из найденных неожиданных правил дешифровывается следующим образом: *если AGE (средний возраст участников) в диапазоне от 27 до 41, WTN (погода) CLD (пасмурно) и NWK (уровень безработицы) в регионе в диапазоне от 1,25 до 3.16, то ситуация не может быть CHS (массовые беспорядки)*.

Наибольший интерес, конечно же, представляют *возможности системы по решению задачи прогнозирования*. В системе WizWhy предусмотрены два варианта использования обнаруженных правил для предсказания значений целевого показателя на новом материале.

Первая возможность заключается в ручном вводе значений признаков и обработке нового одиночного объекта (записи). После нажатия на кнопку Predict online... на экране отображается окно WizWhy Predictor (рис. 3.19).

После заполнения (например значениями как на рис. 3.19) строк предложенной таблицы (здесь возможны пропуски) нажимаем кнопку Issue Report (Issue Report) — система находит релевантные правила и создает отчет, в котором подробно описываются как конечный результат предсказания, так и характеристики каждого отдельного правила, сработавшего для данного объекта. Фрагмент этого отчета приводится ниже.

WIZWHY PREDICTION REPORT

File Name: **C:\Users\Pavlik.ITO\Desktop\Mass Actions\MAS.txt**
Condition Fields:
AGE = **35,00**
EVT *is* **PCY**
DAY *is* **EVN**
KND *is* **WKD**
MON *is* **GRW**
WTH *is* **CLD**
NWK = **3,00**
INC = **2,00**
ACT = **3,00**
DSC = **–3,00**
FRS = **250,00**
WPN *is* **GAS**
Dependent Variable: **STN**
Subject for Prediction: **STN** is **CHS**
Prediction's significance level: Error probability = 0,000
Primary Prediction's probability: 0,373
Conclusive Prediction's probability: 0,226
Decision point: 0,238
Prediction: **No CHS**

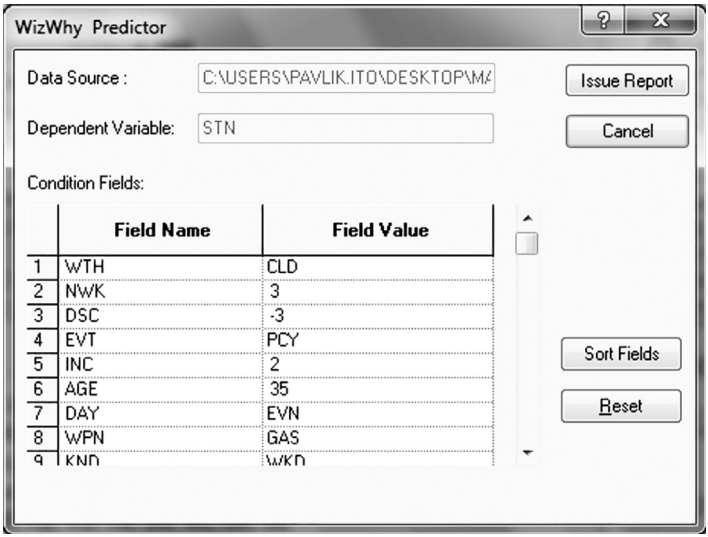


Рис. 3.19. Окно диалога WizWhy для ввода значений признаков вручную

Relevant rules:

1) *If* **MON** *is* **GRW**
   Then
   STN *is not* **CHS**
   Rule's probability: **0,867**
   The rule exists in **13** *records.*
   Significance Level: Error probability < 0,1
2) *If* **WPN** *is* **GAS**
   Then
   STN *is not* **CHS**
   Rule's probability: **0,783**
   The rule exists in **18** *records.*
   Significance Level: Error probability < 0,1

Как видим, в нашем конкретном случае система выдала предсказание, что рассматриваемый объект не относится к классу CHS (Prediction: **No CHS**). Это решение система приняла на основании 12 релевантных правил.

Вторая возможность использования множества правил заключается в обработке сразу большого массива новой информации. Для этого в левой части окна программы нужно выбрать Main Window и на вкладке — Prediction Input. Затем нажать кнопку Open Data of Type :

и в окне диалога для ввода данных указать файл, в котором записана новая информация.

В заключение этой части пособия следует отметить, что применение программных систем, построенных на основе алгоритмов Data Mining, дает возможность на уровне рядового пользователя ИТ решать сложные аналитические задачи — задачи классификации данных и задачи построения решающих правил. Процедура решения сводится к формированию и загрузке в систему набора исходных данных (самое сложное в этой задаче), к настройке и активации режимов обработки данных, получению и интерпретации результатов. Отдельного внимания заслуживает возможность использования полученных классификаторов и правил для оценки прогнозных значений. Таким образом, рассмотренные системы позволяют реализовать полный цикл аналитической обработки от ввода исходных данных до получения результатов в виде обнаружения зависимостей и прогнозных значений.

3.4. Организация системы информационно-аналитического обеспечения на основе интеграции программно-технических средств ситуационного центра и дежурной части органов внутренних дел

Применение программных решений, рассмотренных в подразд. 3.3, в качестве одного из элементов СППР возможно и целесообразно. Так, при решении задач анализа и прогнозирования оперативной обстановки собираются (формируются) различные данные о текущей ситуации, например сведения о состоянии общественного порядка во время массового мероприятия как до, так и в процессе его проведения. В результате обработки данных о массовых мероприятиях за предыдущие периоды генерируются правила if… then. Они используются для предсказания нарушений общественного порядка. При этом имеется возможность оценить значения критических для выхода ситуации из-под контроля параметров, например таких, как численность участников, площадь проведения мероприятия и др.

При выполнении процедуры анализа оценка ситуации проводится как до начала мероприятия, так и во время его течения. Последнее, в частности, позволяет оперативно учесть изменения, происходящие в процессе его проведения.

Также сформированные системой правила могут постоянно уточняться и корректироваться с учетом новых данных, полученных из различных источников.

На основе результатов анализа и прогнозирования оперативной обстановки, оценки имеющихся сил и средств и др. определяется ком-

плекс мероприятий, выполнение которых должно обеспечить решение поставленных задач (в нашем примере — задач поддержания общественного порядка при проведении массовых мероприятий).

Несмотря на развитие и совершенствование инструментария, доступного современному аналитику, в информационно-аналитических службах подразделений ОВД внимание уделяется в основном краткосрочным проблемам, где набор альтернатив мал, необходимость в итеративном анализе невелика, а основные информационные потребности связаны с отслеживанием текущих изменений ситуации. Сегодня ограничен круг специалистов, владеющих необходимой методологией и способных применять ее при анализе меняющейся ситуации. Привлечение научных работников, как наиболее подготовленных к аналитической деятельности и наименее заинтересованных в лоббировании каких-либо решений, сдерживается тем, что академический подход слабо связан с задачами конкретного управленческого консультирования. Поэтому *повышение эффективности информационно-аналитической деятельности может быть осуществлено за счет реализации способов и методик анализа с помощью современных решений на базе информационных и телекоммуникационных технологий*.

Одним из таких решений сегодня выступают СЦ, об интегрировании ИТ в составе которых мы говорили в подразд. 1.5. При этом современные СППР, в том числе программные средства интеллектуального анализа, могут входить в состав ситуационных центров в качестве одного из ключевых элементов — инструмента для моделирования принимаемых решений и прогнозирования их эффективности.

Еще раз повторимся, что современные реалии требуют от руководителя высокой скорости реакции на изменение обстановки, четкого и точного взаимодействия с подчиненными, вышестоящими и внешними структурами для выполнения принятых решений. Безусловно, такие требования обеспечиваются с помощью современных технологических средств обработки информации.

Последние, в свою очередь, объединяются в *информационно-технические комплексы в составе СЦ и, используемые совместно с СППР*, позволяют руководителям успешно решать как повседневные задачи, так и задачи управления в кризисных ситуациях.

К подобным *задачам* относятся:

1) сбор данных о состоянии внешней среды за счет обращения к информационным ресурсам общего пользования (Интернет, СМИ, справочно-поисковые системы и т. п.) и ведомственным банкам данных;

2) мониторинг обстановки на основе различной информации, в том числе данных с устройств видеонаблюдения, сообщений оперативных и дежурных служб по каналам радиосвязи;

3) разработка и обоснование вариантов решений на основе прогностической информации, полученной с помощью СППР;

4) контроль и оценка результатов решений с помощью коммуникационных средств ситуационного центра (видео-конференц-связь, совместная работа над документами, обсуждение ситуации).

Таким образом, реализация в рамках СЦ информационно-аналитической поддержки управленческих процедур и процессов позволяет оперативно анализировать, моделировать, прогнозировать сценарии развития ситуации и динамично вырабатывать эффективные решения.

Так, **созданный и успешно функционирующий в Дальневосточном юридическом институте МВД России многофункциональный информационно-аналитический центр**[1] позволяет значительно повысить качество учебного процесса за счет повышения степени интеграции всех доступных информационных ресурсов и использования инфокоммуникационных технологий.

Структурно МИАЦ (рис. 3.20) представляет собой комплекс программных и аппаратных средств, состоящий из трех сегментов:

1) СЦ;

2) учебный центр «Дежурная часть органа внутренних дел»;

3) серверная МИАЦ.

1. *СЦ — это основной сегмент МИАЦ*, созданный на базе технических решений компании «Стэл КС»; включает 18 АРМ участников СЦ, мультимедийное демонстрационное оборудование, средства видео-конференц-связи.

2. *Учебный центр «Дежурная часть органа внутренних дел»* представляет собой полную модель дежурной части ОВД, включающую АРМ сотрудников дежурной смены, средства отображения информации о местоположении патрулей и видеомониторинга. Программные средства, входящие в состав АРМ, максимально приближают решение учебных задач к реальным задачам дежурной службы ОВД.

3. *Серверная МИАЦ* является центром управления МИАЦ, оборудование которой позволяет аккумулировать все информационные ресурсы обоих сегментов и распределять их в соответствии с поставленной задачей.

Все сегменты находятся в отдельных, но смежных помещениях, оборудованы средствами видео-конференц-связи, что позволяет оптимизировать технологии управления процессом принятия решений или процессом обучения. Такая конфигурация обеспечивает эффективное решение *научно-исследовательских задач, задач управления вузом. Однако основное назначение МИАЦ все-таки заключается в решении ряда учебных задач*. Среди них наряду с получением общих навыков работы с техникой, технологиями, программным и аппаратным обеспечением, применяемым в деятельности ОВД, обучающиеся приобретают знания и навыки по подготовке и принятию, организации испол-

[1] Далее используется сокращение МИАЦ.

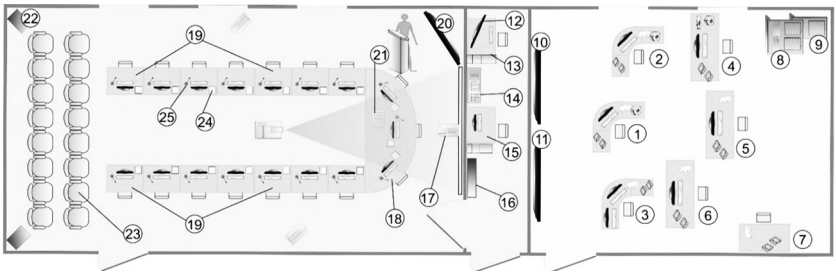


Рис. 3.20. Многофункциональный информационно-аналитический центр ДВЮИ МВД России

1 – АРМ оперативного дежурного ДЧ;
2 – АРМ помощника оперативного дежурного;
3 – АРМ помощника оперативного дежурного;
4 – АРМ оператора администрирования и сопровождения ДЧ;
5 – АРМ оператора связи;
6 – АРМ оператора ИСОД МВД России;
7 – АРМ оператора специальной связи;
8 – АТС;
9 – СУБД Oracle (модель ИБД-Р);
10 – панель вывода информации о местонахождении патрулей и видеоконтроль периметра;
11 – панель отображения интерактивной карты города с транспортными средствами ДЧ;
12 – монитор видеоконтроля;
13 – АРМ администратора, сервер;
14 – сервер аудио-, видео-конференц-связи, система протоколирования;
15 – АРМ подготовки презентаций;
16 – электрощитовая;
17 – видеокамера Eagle Eye;
18 – рабочие места преподавателей (президиум);
19 – рабочие места участников занятий;
20 – монитор отображения оперативной информации;
21 – терминал доступа;
22 – акустическая система;
23 – дополнительные места участников занятий;
24 – терминал доступа;
25 – пульт с микрофоном.

нения и контролю решений по различным направлениям деятельности ОВД. Большой имитационный функционал МИАЦ позволяет на высоком уровне проводить учебные занятия в форме деловых игр, учений.

Возможности ресурсов МИАЦ в *оперативном управлении силами и средствами* иллюстрирует комплексное применение всех средств МИАЦ для контроля за проведением массовых мероприятий, предотвращением и пресечением массовых беспорядков.

Известно, что выработка любого решения основывается на изучении нормативных правовых актов и документов. Программное обеспечение МИАЦ позволяет задействовать справочные правовые системы для выработки решения в соответствии с действующим законодательством. При этом участники СЦ имеют возможность, руководствуясь нормативными документами разного уровня, в том числе ведомственного, при помощи информационно-правовой системы «Гарант», справочно-правовой системы «КонсультантПлюс», а также ведомственной специализированной территориально распределенной автоматизированной системы «Юрист» подготовить проект решения учебной ситуации. В дальнейшем с помощью системы электронного докумен-

тооборота этот проект проходит стадии уточнения, корректировки и окончательного принятия в электронной форме.

Огромное значение для функционирования СЦ имеют аппаратно-программные средства сбора, обработки и отображения (представления) информации о текущем состоянии и вероятных изменениях в поведении системы управления.

Так, аппаратно-программные средства, входящие в состав учебного центра «Дежурная часть органа внутренних дел», в полной мере обеспечивают *решение задач сбора, обработки и представления информации о системе управления участникам СЦ*.

Учебный центр моделирует программно-техническое оснащение современных дежурных частей ОВД. Такое оснащение представлено *АРМ для решения разных задач*.

1. АРМ оперативного дежурного нацелено на координацию и управление силами и средствами дежурных подразделений на основе принятия решений, поддерживаемых учебной версией интеллектуальной комплексной системы «Безопасный город» (подсистема видеонаблюдения, АИС учета сообщений о происшествиях в электронной книге учета сообщений о происшествиях[1]).

2. АРМ помощника оперативного дежурного позволяет вести мониторинг подвижных объектов (маршруты следования автотранспортных средств института отображаются на электронной карте города) и обеспечивать оперативное прибытие подразделений на места происшествий, а также совместно с оперативным дежурным вести наполнение базы данных ЭКУСП.

3. АРМ помощника оперативного дежурного отвечает за принятие решений при реализации задач учебной версии комплексной системы «Безопасный город» (ведется видеомониторинг периметра института).

4. АРМ оператора ИСОД МВД России позволяет получать санкционированный доступ к сервисам ИСОД МВД России, интегрированным банкам данных регионального и федерального уровней (ИБД-Р, ИБД-Ф), к различным АИС (например АИС «Мониторинг»), специализированным территориально распределенным автоматизированным системам (например СТРАС «Юрист») в целях своевременного информирования оперативных подразделений.

5. АРМ оператора связи отвечает за технологию предоставления услуг по линиям городской АТС, междугородней АТС; организацию оперативной телефонной связи, связи по специальным линиям службы 02; поступление информации при экстренной связи гражданин — полиция, факсимильной, радиосвязи; обеспечивает возможность реализации сервисных функций:

[1] Далее используется сокращение ЭКУСП.

- оповещения телефонных абонентов в автоматическом режиме (голосовое или SMS-оповещение);
- организации конференц-связи;
- организации IP-телефонии и др.

6. АРМ оператора администрирования и сопровождения дежурной части позволяет выполнять функции по настройке АРМ дежурной части, сопровождению и отладке программного обеспечения АРМ и серверов, редактированию и обновлению электронной карты города.

7. АРМ оператора специальной связи дает возможность ведения закрытых телефонных переговоров через цифровое коммутационное поле учрежденческой автоматической телефонной станции посредством тонкой настройки параметров каждого канала, осуществлять запись телефонных переговоров, поступающих с аналоговых и цифровых линий, управлять потоками электронной почты.

Каждое рабочее место в системе управления дежурной частью предназначено для выполнения определенных задач. Реализация этих задач требует программно-технической поддержки принимаемых решений с учетом технологий интеллектуального управления. Это обеспечивают *специальные программно-аппаратные средства*.

АПК дежурной части по приему и обработке сообщений оператором службы 02 (рис. 3.21) позволяет зафиксировать поступившую информацию при помощи средств комплекса многоканальной аудио-

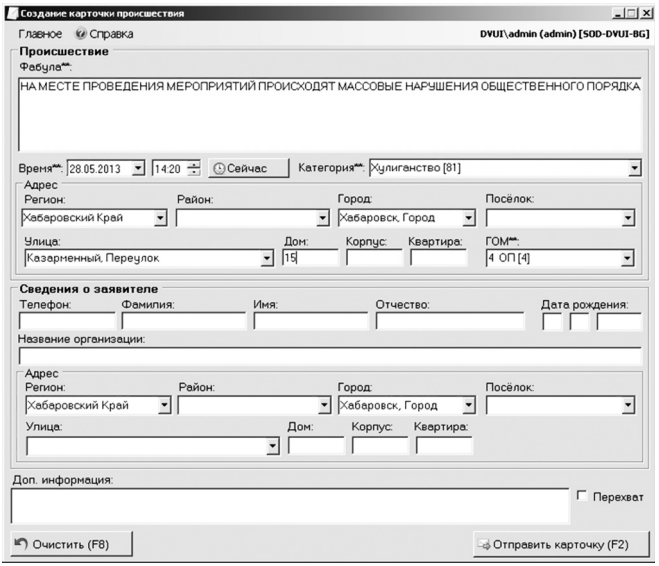


Рис. 3.21. Карточка происшествия (прием и обработка сообщений оператора службы 02)

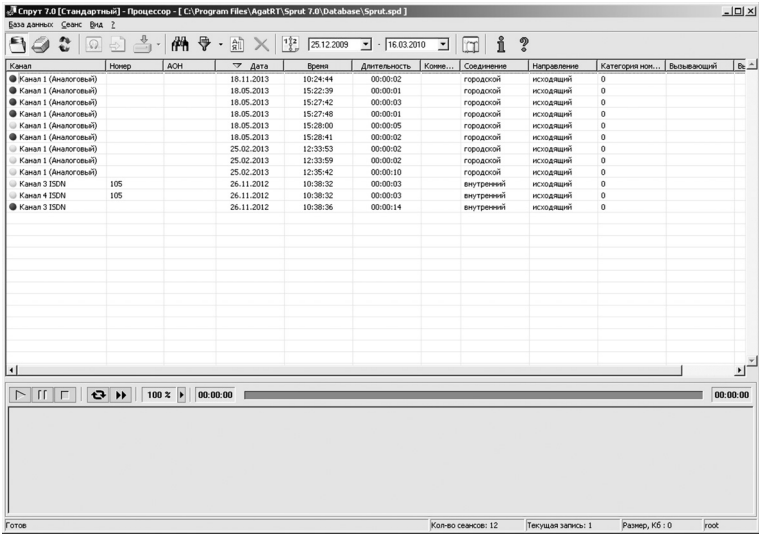


Рис. 3.22. Интерфейс комплекса многоканальной аудиозаписи «Спрут»

записи и оповещения «Спрут» (ООО «КБ АГАТ-РТ») (рис. 3.22). Затем он может проверить полученные сведения по учетам на учебной модели интегрированного банка данных ИБД-Р, разработанной сотрудниками Информационного центра УМВД России по Хабаровскому краю на основе специализированного программного обеспечения, управляемого СУБД Oracle (рис. 3.23).

АПК учебного центра «Дежурная часть органа внутренних дел» в составе МИАЦ обеспечивает в процессе принятия решения участников группы управления СЦ актуальной информацией об изменении оперативной обстановки. Они фиксируются дежурной службой на основе данных, полученных по различным каналам связи (по радиостанции, телефону, через электронное сообщение), а также с помощью системы видеонаблюдения. При этом участники группы управления принимают решения, например по расстановке сил и средств, учитывая информацию из ГИС о дислокации подразделений и перемещении мобильных объектов на территории обслуживания.

Современные ГИС, как мы уже отмечали в подразд. 1.4, 2.4, расширили использование электронных карт за счет хранения графи
ческих данных в виде отдельных тематических слоев. Кроме того, в виде отдельных баз данных представлены качественные и количественные характеристики объектов, имеющихся на картах. Такая организация данных дает пользователю различные аналитические возможности.

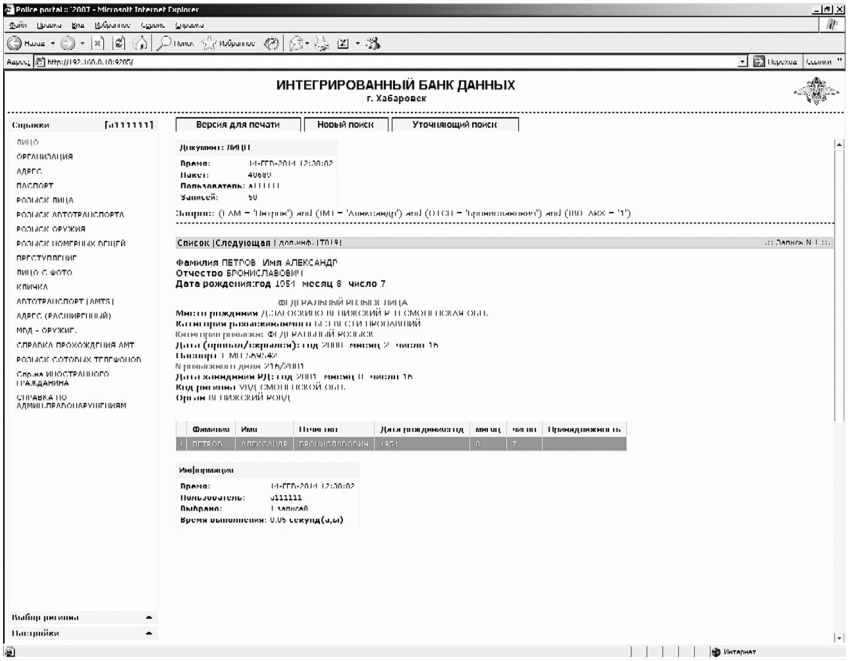


Рис. 3.23. Проверка сведений по учетам учебной модели ИБД-Р

В деятельности полиции ГИС применяются для решения задач:

1) планирования и расстановки сил при подготовке различных мероприятий;

2) моделирования вариантов развития ситуаций;

3) навигации мобильных подразделений;

4) принятия оптимальных управленческих решений на основе анализа пространственных данных.

Учебная модель комплексной информационно-аналитической системы АПК «Безопасный город» содержит модуль ГИС (рис. 3.24), реализованный в среде картографического построения «Панорама» (рис. 3.25).

В качестве альтернативной ГИС в состав АРМ учебного центра «Дежурная часть органа внутренних дел» включена *НМС «Арго-Страж»* производства ЗАО «Навигационные системы». В процессе моделирования деятельности дежурной службы средствами этой системы решаются следующие задачи:

1) нанесение и отображение мест (территорий) оперативного контроля, например проведения массового мероприятия;

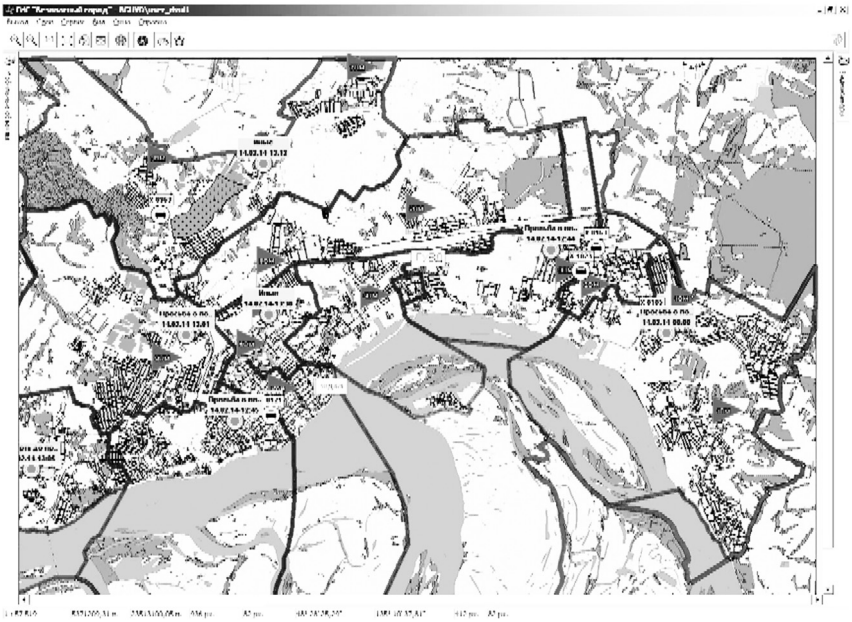


Рис. 3.24. Модуль ГИС учебной модели «Безопасный город»

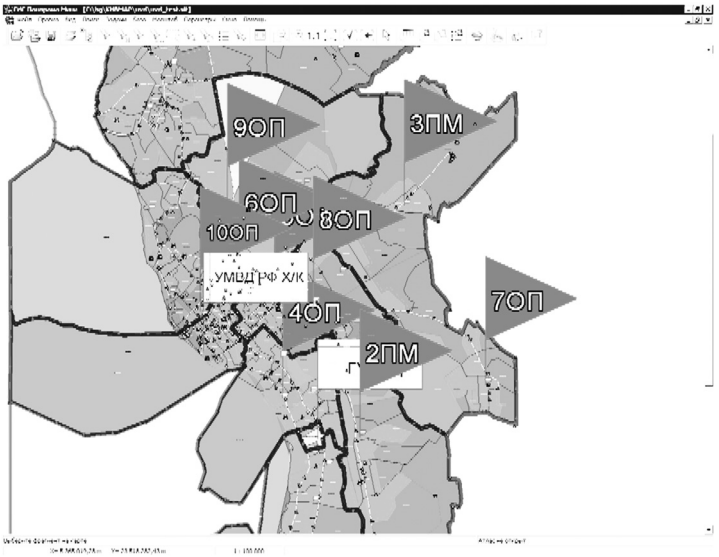


Рис. 3.25. Среда картографического построения «Панорама»

2) нанесение и мониторинг расположения подразделений по охране общественного порядка;

3) отображение вариантов расстановки мобильных объектов с установленными навигационными блоками;

4) участие группы управления СЦ в выборе варианта расположения мобильных объектов и контроля их позиционирования после команды (рис. 3.26).

НМС «Арго-Страж» обеспечивает участников дежурной службы, а через них и СЦ данными о местоположении и процессе движения объектов (рис. 3.27). Прибытие к месту дислокации фиксируется с помощью специального модуля «План-перехват».

Для решения задач управления, например обеспечения охраны общественного порядка при проведении массовых мероприятий и предотвращения возможных беспорядков, аппаратно-программные средства МИАЦ позволяют задействовать *системы видеонаблюдения* для получения актуальной информации о ситуации на территории обслуживания. Такие системы имеются в составе программного обеспечения МИАЦ, это системы Tahion, SecureOS и Macroscop.

Tahion (компания Vocord) входит в состав учебной модели информационно-аналитической системы АПК «Безопасный город» (рис. 3.28).

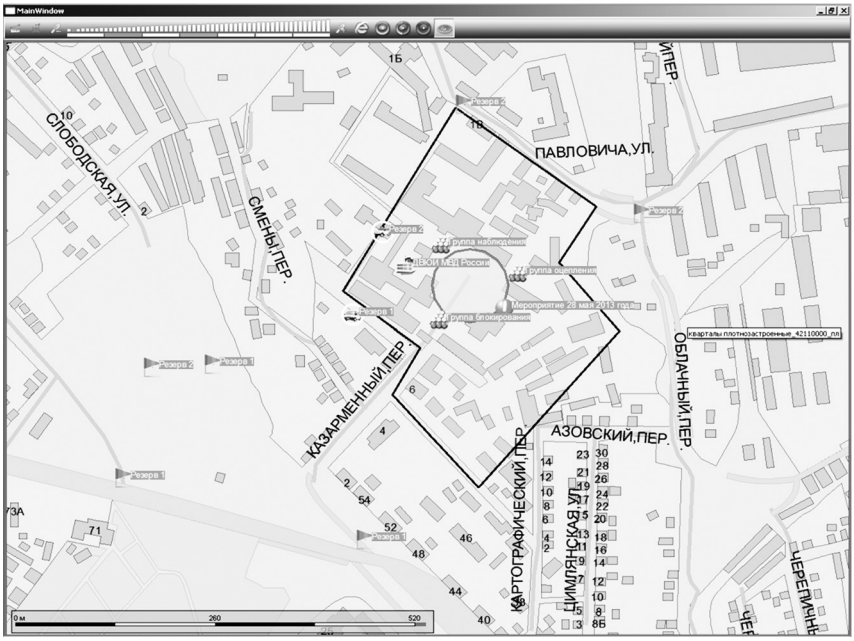


Рис. 3.26. Отображение мобильных объектов и мест оперативного контроля в системе «Арго-Страж»

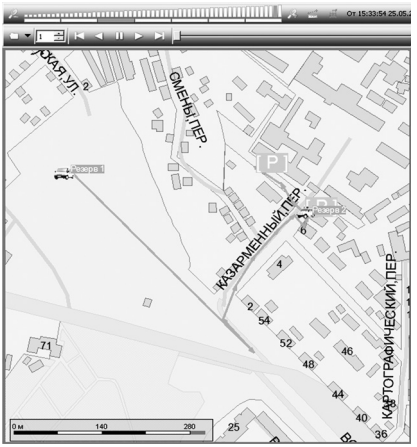


Рис. 3.27. Отображение перемещения объектов в системе «Арго-Страж»

Рис. 3.28. Система видеонаблюдения Tahion

С помощью этой системы демонстрируется реальная видеоинформация, доступная дежурным службам ОВД города, а также функциональные возможности Tahion, в том числе удаленное управление видеокамерами, запись/воспроизведение видеопотоков, поиск видеофрагментов по различным реквизитам.

Системы видеонаблюдения SecureOS (рис. 3.29) и Macroscop (рис. 3.30), установленные на АРМ дежурной смены в учебном цен-

тре «Дежурная часть органа внутренних дел» ДВЮИ МВД России, нацелены на фиксацию информации как на территории института (SecureOS), так и внутри помещений (Macroscop).

Видеоинформация, полученная с помощью данных систем, передается на мониторы участников группы управления СЦ и при необходимости проецируется на главный экран.

Наличие *системы видео-конференц-связи* Polycom (компания Polycom Inc.) обеспечивает аудиовизуальное взаимодействие участников группы управления СЦ с дежурной сменой — операторами АРМ в дежурной части: передачу распоряжений оперативному дежурному в учебном центре и прием докладов о состоянии оперативной обстановки.

Осуществляя визуальный контроль с помощью системы видеонаблюдения за ситуацией, группа управления СЦ обсуждает и принимает решения по оптимизации расстановки сил, а в случае необходимости на основе информации, полученной с помощью систем видеонаблюдения, и сообщений от дежурной службы, — по стаби лизации ситуации. При помощи системы видео-конференц-связи доводятся распоряжения до дежурной службы, где отдаются команды силам и средствам, принимающим участие в охране общественного порядка.

Рис. 3.29. Система видеонаблюдения SecureOS

Рис. 3.30. Система видеонаблюдения Macroscop

Наличие в составе АПК «Дежурная часть органа внутренних дел» средств радиосвязи позволяет организовать эффективное взаимодействие с подразделениями ОВД — передачу данных о результатах работы (сведения о задержанных, ориентировки на подозреваемых и др.). Дежурная смена обрабатывает полученные сведения, например проводит (если это необходимо) проверки по массивам модели ИБД-Р.

При помощи программного обеспечения учебной модели системы «Безопасный город» продолжается работа по заполнению и корректировке сведений о происшествиях в части, касающейся фиксации принятия оперативным дежурным необходимых решений — вкладка «Решение дежурного» на карточке событий ЭКУСП (рис. 3.31). При этом данные из книги учета сообщений отображаются на карте в ГИС.

Сотрудники СЦ и дежурная служба ведут непрерывный контроль за изменением ситуации и осуществляют при этом оперативное управление: отдают корректирующие команды и распоряжения.

Таким образом, учебные модели СЦ и дежурной части позволяют на высоком уровне изучать ряд прикладных направлений применения современных аппаратно-программных средств и ИТ к управлению силами и средствами полиции, отрабатывать навыки работы со специальной техникой, совместно и оперативно принимать решения. Информация для принятия решений является, в свою очередь, результатом анализа и обобщения целого комплекса различных сведений и пара

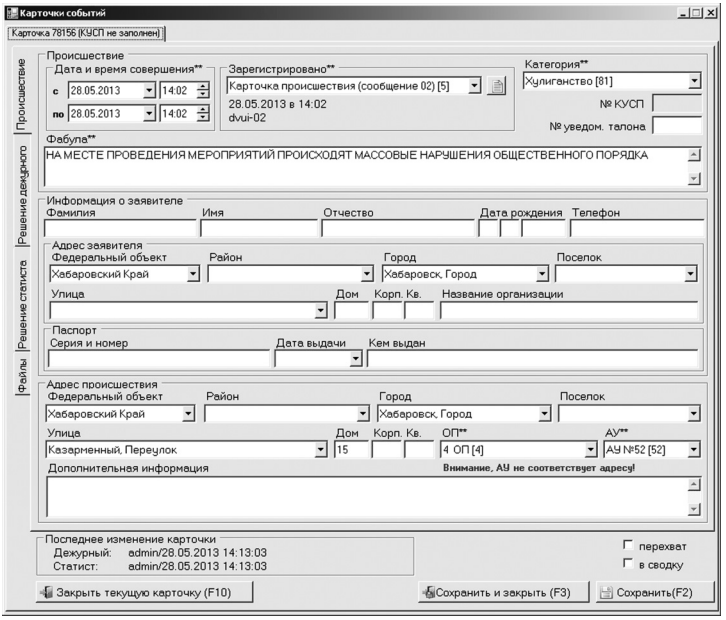


Рис. 3.31. Карточка событий ЭКУСП

метров, получаемых при помощи средств и ресурсов МИАЦ. А интеграция рассмотренных средств и технологий в комплексную информационно-аналитическую систему обеспечивает поддержку принятия решений на уровне, соответствующем современным требованиям и условиям.

Контрольные вопросы

1. В каком виде происходит взаимодействие лица, принимающего решение, с СППР?
2. Что является основной задачей СППР?
3. Какая из подсистем СППР реализуется на основе СУБДД?
4. На какие классы разделяются современные СППР?
5. Какими свойствами обладают знания, полученные с помощью методов Data Mining?
6. Как называется задача Data Mining, которая позволяет определить по известным характеристикам исследуемого объекта значение его ключевого параметра?
7. На какие классы разделяют задачи Data Mining?
8. Каким образом использование методов интеллектуального анализа может повысить качество кадрового обеспечения ОВД?

9. Как называется набор правил, полученный в результате анализа данных с помощью системы See5?

10. Как в системе See5 можно повысить точность результатов?

11. Какой принцип лежит в основе работы системы WyzWhy?

12. Что представляет собой одно из преимуществ системы WyzWhy — поиск неожиданных правил?

13. Назначение какого из компонентов МИАЦ — подготовка информации для участников процесса управления?

14. Что входит в состав учебного центра «Дежурная часть органа внутренних дел»?

15. Какие задачи управления решаются дежурной службой ОВД с помощью ГИС?

16. Для каких задач управления используется система видео-конференц-связи Polycom?

ГЛАВА 4.
ПРИМЕНЕНИЕ МЕТОДОВ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

4.1. Создание системы оценки эффективности функционирования органов внутренних дел в период реформирования

Вопросы эффективности деятельности территориальных органов МВД России всегда находились и находятся в фокусе внимания Правительства Российской Федерации. В условиях экономического кризиса эта проблема становится определяющей для решения задачи сохранения социальной стабильности. При этом следует отметить, что большая часть ответственности за ее решение лежит в плоскости выбора критериев эффективности работы территориальных органов, которые должны не только включать наиболее существенные параметры деятельности ОВД, но и мотивировать сотрудников на честный и результативный труд.

Возрастание значения этих вопросов в современном обществе обусловлено еще и тем, что, как уже отмечалось в предыдущих главах, сложившаяся идеология и технология оценки деятельности ОВД не соответствуют целям их реформирования и изменяющимся требованиям общества.

Очевидно, что реформирование системы ОВД не может быть сведено только к уменьшению численности центрального аппарата и территориальных подразделений ОВД. Без качественного изменения, в первую очередь механизмов управления, ориентированных на новую идеологию взаимоотношений с внешней средой, сами по себе структурные преобразования не способны дать ощутимых результатов.

Важнейшим вопросом идеологии взаимоотношений с внешней средой является разработка оценочных критериев, которые должны мотивировать личный состав подразделений ОВД достигать результата, соответствующего изменившимся требованиям российского общества. Другими словами, *реформирование системы ОВД должно представлять собой последовательно проводимую и постоянно поддерживаемую «настройку» ключевых организационно-управленческих средств*

и методов на объективные потребности общества в правоохранительных «услугах», оказываемых ОВД, удовлетворение которых следует считать главным мерилом эффективности их функционирования.

Создание системы оценки эффективности работы ОВД, которая не только провозглашает социально ориентированную идеологию, но и технологически соответствует ей, позволит развернуть регулятивную функцию оценки в нужном направлении, сделает оценку одним из действенных средств управления ОВД в механизме их реформирования.

Разработка такой системы, особенно в ее технологической составляющей, представляет весьма объемную теоретико-прикладную задачу, решение которой потребует совместных усилий коллективов научно-исследовательских учреждений и различных подразделений ОВД.

В данном пособии представляется возможным обозначить лишь некоторые существенные, на наш взгляд, аспекты рассматриваемой проблемы, не привлекшие к себе должного внимания.

В общем виде под *эффективностью деятельности* понимают ее результативность, определяемую в зависимости от степени достижения соответствующих целей. Однако это всего лишь общая формула — ее механическое применение может привести к серьезным ошибкам при оценке деятельности ОВД, результаты которой сводятся фактически к одним соответствующим показателям в их цифровом выражении. Методология оценки эффективности деятельности ОВД должна исходить из понимания и учета того, какое содержание вкладывается в цели функционирования системы этих органов, какие и в каком количестве используются для их достижения средства и методы.

Большая часть предпринимаемых в последние годы усилий в этой области была подчинена скорее решению текущих оперативных задач и вопросов, обусловленных осложнением криминологической обстановки, ростом угрозы террористической опасности, увеличением масштабов организованной преступности и коррупции. Однако все, безусловно необходимые, подобного рода меры не способны достаточно серьезно повлиять на достижение целей реформирования ОВД.

Сложности на этом пути во многом обусловлены принятыми ранее формальными подходами к оценке деятельности ОВД, которые, доставшись «по наследству», не отвечают сегодняшним целям реформирования.

Формальная природа статистических показателей, преобразуемых в индексные оценки по сложной технологии, не делает их более объективными. Более того, даже их корректное представление неизбежно порождает необъективные и искаженные представления, приводящие к определенным деформациям правоохранительной практики и невозможности принятия по результатам такой оценки обоснованных управ-

ленческих решений. Погоня за процентами для большинства руководителей ОВД все еще остается главным вектором их управленческого воздействия на подчиненные подразделения.

Сказанное не означает отрицания полезности методических средств измерения и использования количественных показателей при оценке деятельности ОВД. Речь идет о том, что необходимо изменить вектор оценки результатов деятельности территориальных органов, уйти от «палочной» системы, при которой не только любое преступление регистрируется как одна неделимая величина («палка»), независимо от вида, тяжести и сложности его расследования, но и оценка эффективности деятельности ОВД по раскрытию и расследованию зарегистрированных преступлений, хотя и через индексную оценку, также предполагает их абсолютную идентичность по трудоемкости и времени расследования.

Рассмотрим, как менялась идеология оценочной политики в последнее время.

4.2. Анализ нормативной базы оценки эффективности деятельности органов внутренних дел

За последние десять лет взгляды на критерии оценки деятельности ОВД менялись несколько раз. Перед реформированием системы МВД России действовал **приказ** от 5 августа 2005 г. **№ 650** «Вопросы оценки деятельности органов внутренних дел Российской Федерации, отдельных подразделений криминальной милиции, милиции общественной безопасности, органов предварительного следствия и органов внутренних дел на транспорте».

В нем были четко выделены *основные показатели, по которым оценивалась деятельность территориальных органов*. Это регистрация, учет и рассмотрение заявлений и сообщений граждан, а также иной информации о происшествиях, правонарушениях и преступлениях; профилактические мероприятия, пресечение, предотвращение преступлений; раскрытие и выявление преступлений; работа предварительного следствия; работа органов дознания; обеспечение охраны общественного порядка и общественной безопасности; личные обращения граждан.

Главной идеей приказа была необходимость вернуть доверие граждан, изменить их отношение в позитивную сторону, заставить действовать сотрудников милиции в конституционно-правовом поле.

Основными инновациями приказа являлись:

- отсутствие показателя «общий процент раскрываемости преступлений»;

- определение «главного» показателя — количества тяжких и особо тяжких преступлений из числа всех расследованных уголовных дел, направленных в суд;
- изменение способа расчета общей оценки, в котором каждый показатель умножается на соответствующий коэффициент, затем подсчитывается итоговое количество индикаторов. Отдел внутренних дел оценивается положительно, если 60% оцениваемых показателей (с учетом коэффициента значимости) имеют положительную оценку.

В структуре данной оценки продолжал применяться такой показатель, как АППГ (аналогичный период прошлого года), из-за которого территориальному органу нужно было показать результаты не хуже, чем в прошлый период, но и не намного лучше, чтобы в следующем периоде этот показатель не был завышенным.

В связи с реформированием ОВД и вступлением в силу Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» [2] был принят **приказ** МВД России от 29 июня 2011 г. **№ 735** «Вопросы оценки деятельности органов внутренних дел».

В нем сохранились основные позиции предыдущего приказа. Скорее всего, причиной его принятия было изменение названия «милиция» на «полиция».

26 декабря 2011 г. был принят **приказ № 1310** «Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации», в котором был сформулирован *новый подход к системе оценки деятельности территориальных органов*.

Прежде всего, *итоговая оценка деятельности территориальных органов становится комплексной*, состоящей из трех частей:

- оценка деятельности по результатам исследования общественного мнения (оценка общественного мнения);
- оценка эффективности деятельности по ведомственным показателям (ведомственная оценка);
- оценка эффективности деятельности территориальных органов МВД России в ходе целевых, инспекторских, контрольных и иных выездов, изучение информационно-аналитических справок и материалов, полученных в рамках осуществления зонального контроля (инспекционная оценка) [42].

Появился *новый критерий* оценки эффективности деятельности территориальных органов — *результат исследования общественного мнения*. Общественное мнение стали изучать, приглашать для этого социологические центры и тратить на замеры значительные средства. Но технология принятия решений на основе полученных данных просто отсутствует. Более того, считается, что полученные данные и есть оценка общественного мнения. То есть данные, полученные при помо-

щи опросов, воспринимаются как статистические. Такое прямое толкование абсолютно недопустимо. *Интерпретация полученных данных социологических опросов — это всегда самостоятельный этап*, на котором необходимо разобраться, что стоит за этими долями и цифрами.

Ведомственная оценка также претерпела значительные изменения. Прежде всего, необходимо отметить, что новый приказ максимально отошел от таких показателей, из-за которых раньше результаты работы сотрудников ОВД часто оценивались по «палочной» системе. Все показатели направлены на улучшение результатов служебной деятельности ОВД. В *перечень статистических показателей* вошли:

- регистрация и рассмотрение сообщений о преступлениях;
- расследование преступлений (расследование тяжких и особо тяжких преступлений; противодействие организованной преступности; обеспечение экономической безопасности и противодействия коррупции; пресечение незаконного оборота наркотиков; противодействие незаконному обороту оружия);
- пресечение и предупреждение преступлений;
- качество расследования уголовных дел;
- возмещение материального ущерба;
- эффективность исполнения законодательства об административных правонарушениях;
- обеспечение безопасности дорожного движения.

Кроме того, если раньше при расчете показателей использовался АППГ, который брался для точки отсчета, чтобы измерить динамику показателя (увеличение или уменьшение), новый приказ вместо него ввел *наибольшее числовое значение показателей по группе* не для оценки динамики показателя, а для оценки эффективности работы конкретного территориального органа. При этом изменения почти не затронули самих принципов оценки.

Основной идеей приказа являлась *попытка избавиться от «палочной» системы и ввести новую систему оценки деятельности по средним значениям показателей*. Теперь для достижения хороших показателей полицейским приходилось решать одновременно две задачи: равняться на территориальные органы, которые демонстрируют самый высокий результат по группе, и следить, чтобы показатели не были ниже, чем в аналогичном отчетном периоде.

31 декабря 2013 г. вышел **приказ № 1040** «Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации» [11].

В новом приказе отдел внутренних дел оценивается по двум направлениям:

- *вневедомственная оценка* — оценка по результатам социологических опросов или иной информации, которая отражает мнение населения;

– *ведомственная оценка*, которая включает в себя экспертную оценку и оценку по результатам деятельности.

В качестве критерия оценки предлагается использовать *наилучшее значение статистического показателя среди оцениваемых территориальных органов МВД России*.

Статистический показатель — относительный показатель (нагрузка, удельный вес, темп роста и иные показатели), рассчитываемый на основе статистических данных и характеризующий количественные и качественные результаты деятельности территориального органа МВД России по соответствующему направлению. Сама оценка производится на основе выраженного в баллах соотношения между статистическим показателем и соответствующим критерием оценки.

Несмотря на то, что АППГ был заменен на наибольшее числовое значение показателей по группе, при подведении итогов он все равно берется для сравнения. При этом в приказе № 1040 сравнение идет не только с прошлым месяцем, но и с пресловутым АППГ.

Таким образом, анализируя последние приказы, следует отметить, что какие бы новые оценочные критерии ни выбирались, *итоговая оценка сводится к сравнению «палочек» сводной статистики*. При этом априори считается, что все «палочки», отражающие непосредственную деятельность подразделений (статистические показатели или количественные показатели экспертной оценки), имеют одинаковую трудоемкость, хотя апостериори это не так. Действительно, трудно сравнить по трудозатратам деятельность следственной группы по расследованию многоэпизодного экономического преступления и расследование кражи сотового телефона. Но с точки зрения оценочной политики это две абсолютно одинаковые «палки», идущие в зачет. Такой подход, безусловно, *не является объективной оценкой затраченного подразделением труда и часто мотивирует его сотрудников к нарушению регистрационной дисциплины*.

Не меньше вопросов вызывает технология прямого сравнения статистических показателей, нормативно закрепленных в качестве оценочных для следственных подразделений, без учета особенностей территории и нагрузки на следователей. Не берется во внимание тот факт, что у каждого района — своя оперативная обстановка, свои особенности территории, свои случайные факторы. Трудно представить, чтобы оценка труда работника промышленного предприятия (а значит, его заработная плата) зависела от того, как успешно работают его коллеги на аналогичных предприятиях в соседнем районе или как результативно работал он в прошлом месяце или в аналогичном периоде прошлого года.

В этой связи *абсолютно обоснованным и единственно объективным подходом при оценке эффективности работы следственных подразделений является введение нормирования их труда*.

4.3. Нормирование труда сотрудников следственных подразделений

Деятельность ОВД, как и других органов, предприятий, учреждений и организаций, состоит из трудовых операций и процессов, в которых заняты как отдельные работники, так и коллективы, группы работников.

На этом основании если не альтернативой, то важным дополнением к используемым критериям оценки может послужить *разработка и применение на региональном уровне* (что не противоречит приказу МВД России № 1040) *специальных нормативов*, которые не только привязывают саму оценку к особенностям сложившейся оперативной обстановки в регионе, но и дают возможность более адекватно оценить нагрузку сотрудников.

Трудовой процесс (согласно основным канонам научной организации труда) — это совокупность целесообразных действий по воздействию на предмет труда с целью выполнения работ, связанных с затратами физической или нервной энергии работника [72]. Трудовой процесс делится на трудовые операции. Типовыми для ОВД являются принятие и обработка сообщений, осмотр места происшествия, фиксация следов, проверка сообщений и данных, работа «по горячим следам», проведение допроса, очной ставки и т.д.

Многообразие функций, выполняемых сотрудниками ОВД, определяет большое количество трудовых операций, которые приходится им осуществлять в процессе повседневной деятельности. Они значительны не только по объему, но и по видам, часто сложны и отличаются существенной спецификой, обусловленной особенностями организации и функционирования как системы ОВД в целом, так и ее структурных элементов: подразделений дознания, предварительного следствия, уголовного розыска, ГИБДД и т.д. В связи с этим трудовые операции, совершаемые следователем, резко отличаются от трудовых операций оперуполномоченного ГИБДД, а работника уголовного розыска — от действий участкового инспектора и т.п.

В то же время *трудовые операции по отдельным линиям работы достаточно типичны и легко могут быть измерены*. Так, например, для следователя процесс расследования преступлений можно представить как последовательность таких трудовых операций: осмотр места происшествия и изъятие вещественных доказательств, оформление протокола допроса свидетелей, подготовка постановления о возбуждении уголовного дела, заполнение статистической карточки, подготовка постановления о назначении экспертизы и т.д. Временны́е затраты на каждую операцию зависят от опыта и профессиональных способностей работника, но всегда можно *методом экспертных оценок опреде-*

лить оптимальное время, которое будет служить нормативом оценки эффективности выполнения операции.

Безусловно, нельзя оценивать время, необходимое для расследования определенного вида преступления, как сумму времени, необходимого для выполнения трудовых операций: целое будет всегда больше суммы его частей. При этом на эффективность работы следователя влияет огромное количество факторов — от его текущей нагрузки до организации и условий работы в отделе. Тем не менее, по мнению специалистов, вполне реально провести экспертизу с целью классификации преступлений по категориям трудоемкости, определив для каждой категории норму времени на расследование, которое зависит от количества трудовых операций и ряда других факторов.

Это позволит в дальнейшем при оценке эффективности деятельности следственного подразделения за прошедший период не руководствоваться количеством уголовных дел, переданных в суд, а *использовать индексную оценку с учетом степени трудоемкости каждого преступления*.

Предложенный подход *позволяет отказаться от необходимости напрямую сравнивать количественные показатели деятельности подразделения с деятельностью в АППГ или с аналогичными показателями другого подразделения и на основе этого выстраивать их рейтинг*. Как правило, оперативная обстановка в различных районах значительно отличается и с течением времени претерпевает изменения. Поэтому такое сравнение является, по меньшей мере, некорректным.

Использование расчетных временных нормативов на каждую категорию преступлений дает возможность определить не только реальную кадровую потребность и ее соотношение с фактической за прошедший период, но и так называемую *потенциальную «пропускную способность» подразделения*, позволяющую оценить количество преступлений всех категорий, которое может «переработать» подразделение (передать в суд) исходя из кадровых ресурсов. Если работа подразделения по итогам года соответствует потенциальной «пропускной способности», то она оценивается положительно. Чем больше она превышает это значение, тем выше рейтинг подразделения. Если показатели подразделения за прошедший период ниже потенциальной «пропускной способности», то это должно свидетельствовать о наличии управленческой или профессиональной проблемы. Чем больше отставание (можно выразить в процентах), тем больше проблема. Таким образом, можно оценить работу следственного подразделения исходя из сложившейся оперативной обстановки на территории, которое оно обслуживает, не включая в эту оценку работу других подразделений с другой оперативной обстановкой.

Рассмотрим технологию оценки деятельности следственных подразделений с применением математического аппарата системной динамики.

4.4. Технология оценки эффективности работы следственных подразделений на основе методов системной динамики

Для решения этой задачи воспользуемся *построением имитационной модели, воспроизводящей структуру взаимодействия* процессов, отражающих кадровую обеспеченность ОВД и состояние преступности, состояние преступности и эффективность работы правоохранительных органов и т. д. Выявление целостности этих взаимодействий гораздо важнее, чем внутреннее содержание каждого фактора, взятого в отдельности. Особого внимания здесь заслуживает *метод системной динамики*, на основе которого в последнее время активизировались исследования сложных социальных систем. Применение этого метода при построении имитационных моделей предприятия, города, при разработке глобальных моделей мира и т. д. получило всеобщее признание. Эффективен он будет и в нашем случае.

Действительно, *ресурсное обеспечение ОВД и преступность, как элементы более общей единой системы, находятся в сложном взаимодействии* друг с другом. Количество и качество кадрового состава системы ОВД (наряду с организационной структурой, материально-техническим обеспечением) определяют интенсивность входящего потока — выявленные преступления. Когда реальный поток преступлений превышает возможности ОВД по его «переработке», повышается уровень латентной преступности. Кроме того, обнаруженные «излишки» различными путями попадают в отказные материалы, имеют место и случаи укрывательства, нарушения учетно-регистрационной дисциплины. Существует и законный путь снятия криминологической напряженности: увеличение доли лиц, не привлекаемых к уголовной ответственности в связи с передачей материалов на рассмотрение общественности.

Весьма важно отметить, что с увеличением нагрузки на ОВД падает раскрываемость преступлений, снижается эффективность оперативно-разыскных мероприятий, уголовные дела приостанавливаются, а следственная работа по ним, по сути, прекращается и т. д.

Таким образом, *динамическое равновесие элементов системы «преступность — ресурсы» — весьма важное понятие* с точки зрения разработки математических моделей для оценки эффективности работы ОВД.

Общий показатель раскрываемости и набор частных показателей расследованных преступлений по ряду причин также не являются достаточно объективными. В них никак не учитываются нагрузка на сотрудников следственных подразделений, различия в трудозатратах на раскрытие и расследование различных видов преступлений и т. п.

Именно поэтому ряд ученых характеризуют показатель раскрываемости и показатели расследованных преступлений как неэффективные. Другие предлагают использовать его в комплексе с иными показателями [68].

Таким образом, можно с уверенностью сказать, что оценивать только по показателям расследованных преступлений деятельность сотрудников следственных подразделений, работающих в различных условиях, недостаточно. Суть в том, что в настоящее время *неопровержимо доказана нелинейная зависимость показателя раскрытых и расследованных преступлений от таких параметров, как интенсивность зарегистрированной преступности* (число преступлений, отнесенных к численности населения) *и кадровая обеспеченность* (количество сотрудников территориальных органов МВД, отнесенное к численности населения) [64]. Эта зависимость записывается в виде:

$$\alpha = \frac{\gamma \cdot \rho}{I} \cdot (1 - e^{-\frac{I}{\gamma \cdot \rho}}), \qquad (1)$$

где α — показатель расследованных преступлений, равный отношению числа расследованных преступлений к общему числу преступлений (V), находящихся в процессе расследования;

γ — показатель «пропускной способности» следственных подразделений (количество расследованных одним следователем преступлений), зависящий от структуры регистрируемой преступности, уровня организации следственной деятельности, от профессионализма сотрудника и ряда других факторов;

ρ — кадровая обеспеченность, которая выражается через соотношение:

$$\rho = \frac{R}{N}, \qquad (2)$$

где R — реальная численность сотрудников следственных подразделений;

N — численность населения в регионе;

I — интенсивность зарегистрированной преступности, которая определяется по формуле:

$$I = \frac{V}{N}; \qquad (3)$$

e — это математическая (показательная) функция: $y = e^x$.

Вид зависимости показателя раскрываемости от зарегистрированной преступности при $p = const$ представлен на рис. 4.1, а вид зависимости показателя раскрываемости от кадровой обеспеченности при при $I = const$ — на рис. 4.2.

Изучение отмеченных закономерностей, описанных с помощью математической модели (1), позволяет решать *задачу определения ко-*

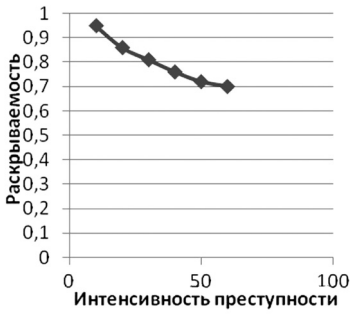


Рис. 4.1. График зависимости раскрываемости преступлений от интенсивности преступности ($\rho = 1{,}6 * 10^{-4}$, $\gamma = 50$)

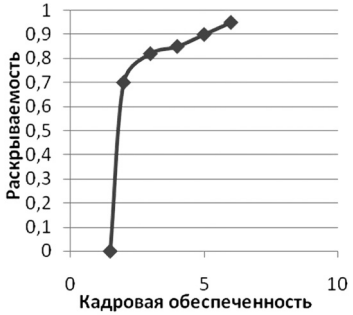


Рис. 4.2. График зависимости раскрываемости преступлений от кадровой обеспеченности следственного подразделения ($I = 34{,}4$, $\gamma = 50$)

эффициента расследованных преступлений на основе реальной «пропускной способности», которую показало подразделение за период.

Для этого формулу (1) с учетом выражений (2) и (3) преобразуем в следующий вид:

$$\alpha = \frac{\gamma \cdot R}{V} \cdot (1 - e^{-\frac{V}{\gamma \cdot R}}) \qquad (4)$$

Показатель «пропускной способности» γ отражает интегрированную оценку оптимальной нагрузки (например количество уголовных дел) на одного следователя. «Пропускная способность» зависит прежде всего от трудозатрат на раскрытие или расследование разных видов преступлений. Мы уже приводили пример, что трудозатраты на раскрытие и расследование многоэпизодного преступления в сфере экономики гораздо выше, чем при расследовании кражи сотового телефона. В этой связи оптимальная нагрузка сотрудника, работающего в сфере борьбы с экономическими преступлениями, должна быть ниже оптимальной нагрузки сотрудника, специализирующегося на краже сотовых телефонов. *Итоговый показатель «пропускной способности»* рассчитывается как интегрированная величина с учетом доли каждой группы преступлений [68].

Допустим, что методом экспертных оценок все преступления классифицированы по четырем категориям в зависимости от трудоемкости процесса раскрытия и расследования. В соответствии с этим по каждой категории преступлений на основании проведенной экспертизы определяется оптимальная нагрузка на одного сотрудника, которая не должна превышать его возможности.

Например, по преступлениям 1 категории, как наиболее трудоемким, определяется оптимальная нагрузка на одного следователя в 5 уголовных дел в год, преступлениям 2 категории — 10 уголовных дел, 3 категории — 20 уголовных дел, 4 категории — 30 уголовных дел.

Пусть доля преступлений 1 категории в общем количестве зарегистрированных преступлений будет составлять 10%, преступлений 2 категории — 15%, 3 категории — 25%, 4 категории — 50%. Итоговая «пропускная способность» (γ) рассчитывается как средневзвешенная:

$$\gamma = 5 \cdot 0{,}1 + 10 \cdot 0{,}15 + 20 \cdot 0{,}25 + 30 \cdot 0{,}5 = 22.$$

Таким образом, оптимальная нагрузка на одного оперуполномоченного — 22 уголовных дела в год.

Подставляя полученное значение γ, а также известные значения R, V в формулу (4), получаем искомую *нормативную раскрываемость*, которую следственное подразделение должно показать за отчетный период с учетом сложившейся нагрузки на одного следователя и трудоемкости зарегистрированных преступлений на территории, которую оно обслуживает. Если реальная раскрываемость выше нормативной, то работа оценивается позитивно, ниже нормативной — негативно.

Для того чтобы определить рейтинг подразделения среди других, можно в качестве критерия взять *процентное отклонение реальной раскрываемости от рассчитанной нормативной*. Лучшим подразделением будет считаться то, которое имеет максимальное превышение в процентах над своей нормативной раскрываемостью.

Таким образом, оценка деятельности следственного подразделения будет зависеть только от качества работы самого подразделения и не зависеть от того, какое «качество» показали «соседи». Именно такой подход действительно поможет избавиться от «палочек» сводной статистики и позволит привязать оценку работы подразделений к трудоемкости преступлений и к нагрузке следователей.

4.5. Пример анализа и оценки деятельности следственного подразделения

4.5.1. Проведение экспертизы по классификации преступлений

Классификация преступлений является основополагающей процедурой, которая определяет в конечном итоге нормативы оценки деятельности подразделений. С учетом специфики деятельности следственных подразделений *в качестве нормативного показателя можно взять ориентировочное время расследования преступлений определенной категории сложности*. Классификация преступлений по категориям сложности и, соответственно, время расследования преступлений каждой категории определяются методом экспертных оценок.

Методы экспертных оценок относят к эвристическим методам, так как при проведении экспертиз экспертам необходимо создать условия, способствующие генерации идей по решению сложных проблем. Экспертные оценки используются в тех случаях, когда необходимо оценить явления и процессы, плохо поддающиеся непосредственному измерению. Группа специалистов-экспертов (экспертная комиссия) измеряет некоторые характеристики, и ее коллективная оценка служит основанием для последующего принятия решений.

Таким образом, под *экспертными методами* понимается комплекс логических приемов и математико-статистических процедур, направленных на получение от специалистов информации, ее обобщение и анализ в целях подготовки и выбора рациональных решений.

В настоящее время методы экспертных оценок нашли широкое применение в деятельности ОВД. В частности, их можно использовать для классификации преступлений по категориям сложности и оценки среднего времени расследования преступлений каждой категории.

Эффективность методов экспертных оценок во многом зависит от обоснованности их применения для решения конкретной проблемы, от того, насколько правильно подобран состав группы экспертов и организована процедура экспертного опроса, а также сбор, обработка и анализ экспертной информации. Точность экспертной оценки зависит от сложности проблемы, степени ее изученности, а также от уровня компетентности экспертов.

Проблема использования суждений экспертов распадается на две части — сначала надо получить от экспертов данные, необходимые для оценки вероятностных событий, а затем преобразовать эту информацию в форму, удобную для принятия решений. Для решения этой проблемы разработан и используется определенный *порядок проведения экспертизы* [42].

1. *Разработка цели экспертизы*. Цели экспертизы преследуют в основном решение задач двух классов:

1) оценка (измерение) имеющихся объектов, например оценка деятельности территориального подразделения ОВД;
2) построение объектов и их оценка. Это может быть построение системы признаков для оценки эффективности деятельности территориальных подразделений ОВД и оценка весомости каждого признака.

Любой объект характеризуется одним признаком или целым их набором. Измерение объекта осуществляется за счет оценки его признаков. Поэтому для каждого признака необходимо установить *шкалу оценки признака*. Таким образом, целью экспертизы в нашем случае является классификация преступлений по категориям сложности и оценка каждой категории по временно́му параметру.

2. *Разработка процедуры опроса экспертов*. После установления цели экспертизы формируется группа высококвалифицированных специалистов-аналитиков. Часто ее называют *рабочей группой*. Ее основными задачами являются подготовка, проведение опроса и анализ информации, полученной от экспертов.

В процессе разработки процедуры опроса рабочая группа устанавливает методику опроса и перечень вопросов, на которые должны ответить эксперты. Кроме того, готовит для них всю доступную объективную информацию, имеющую отношение к анализируемой проблеме.

В основе большинства экспертных методов лежит *анкетирование или опрос* (заполняется анкета, опросный лист или таблица), с помощью которых осуществляется сбор необходимой информации. Структурно организованный набор вопросов в анкете логически связан с целью экспертизы.

Формулировка вопросов должна обеспечивать однозначное толкование и ответ на каждый из них в виде количественной оценки. От правильности разработки анкеты во многом зависит успех экспертизы.

3. *Формирование группы экспертов*. При формировании группы экспертов обычно определяются ее *численность и степень компетентности экспертов* в выбранной области.

Работу по отбору экспертов, как правило, начинают с определения научных, технических, экономических и других областей знания, которые связаны с объектом, требующим экспертной оценки. Затем составляется список лиц, являющихся специалистами в каждой из этих областей. Вместе с тем желательно, чтобы кандидат в эксперты был широко эрудирован и в смежных областях знания.

Численность группы (обычно колеблется в диапазоне от 7 до 30 человек) определяется исходя из расчетных соотношений с привлечением ряда логических соображений. Опрос не должен быть массовым, так как оценка каждого эксперта в этом случае уже не влияет на групповую. В результате мнения, отличные от мнения большинства, почти не учитываются, хотя они далеко не всегда оказываются ошибочными.

При комплектовании группы *следует выявить потенциально возможные интересы кандидатов, которые могут противоречить целям экспертизы*. Заинтересованность экспертов в результатах экспертизы может вызвать смещение группового мнения в сторону от объективной оценки. В этом случае заинтересованных лиц не следует включать в экспертную группу или же нужно составлять вопросы анкеты таким образом, чтобы замаскировать цель экспертизы.

После того как определены численность экспертной группы и ее состав, рассчитывается степень компетентности каждого эксперта. Определение степени компетентности в большинстве случаев увеличивает

точность групповой оценки. Существует много *способов определения компетентности экспертов*: самооценка, взаимооценка, оценка профессиональных характеристик экспертов и др.

В качестве примера приведем *способ взаимооценки*, который применяется в том случае, когда эксперты хорошо знают друг друга. Экспертам, входящим в группу, сообщается ее состав. Далее каждого эксперта просят оценить компетентность других экспертов в баллах, например от одного до пяти. Эксперт сам себя не оценивает.

Оценки экспертов не известны друг другу (анонимны). Рабочая группа сводит оценки в одну таблицу (см., например, табл. 4.1).

Таблица 4.1

Компетентность экспертов

№ п/п	Эксперты	Баллы					C_i
		1	2	3	4	5	
1	Югов В. А.	–	5	3	4	3	15
2	Гладких С.С.	5	–	3	4	4	16
3	Корж А.С.	2	2	–	3	3	10
4	Кравченко Ю.А.	4	4	5	–	3	16
5	Дятлов В.С.	5	5	4	5	–	19
Общая сумма, С 76							

Подсчитывается сумма баллов каждого эксперта C_i, где $i = 1, 2, 3\ldots$ n (n – количество экспертов), общая сумма баллов всех экспертов $C = \sum_{i=1}^{n} C_i$, и на основании C_i и С определяются коэффициенты компетентности:

$$a_i = C_i / \sum_{i=1}^{n} C_i. \qquad (5)$$

В соответствии с формулой (5) эксперты получают следующие коэффициенты компетентности:

— Югов В. А., $a_1 = 15/76 \cong 0{,}20$;
— Гладких С. С., $a_2 = 16/76 \cong 0{,}21$;
— Корж А. С., $a_3 = 10/76 \cong 0{,}13$;
— Кравченко Ю. А., $a_4 = 16/76 \cong 0{,}21$;
— Дятлов В. С., $a_5 = 19/76 \cong 0{,}25$.

При обработке результатов экспертизы необходимо умножить оценки экспертов на коэффициенты их компетентности [42].

4. *Проведение опроса*. В зависимости от цели экспертизы используются те или иные методы экспертных оценок. Их можно разбить на два класса: методы коллективной работы экспертной группы и методы получения индивидуального мнения членов экспертной группы.

Методы коллективной работы экспертной группы в основном используются для решения задач второго класса, связанных с получением экспертной информации *качественного характера* с последующим ее упорядочением по степени значимости. К этим методам относятся «комиссия», «мозговая атака», «суд», «индуцирование психоинтеллектуальной деятельности» (ИПИД), «игровая имитация».

В указанные методы органично вплетаются эвристические методы повышения эффективности творческой деятельности. Колоссальные по своей эмоционально-психологической нагрузке психоэвристические обсуждения на короткое время мобилизуют все мыслительные резервы участников экспертизы, заставляют их интенсивно думать, познавать всю глубину проблемы.

Представленная технология коллективной экспертизы может быть использована для решения задачи классификации преступлений по категориям в зависимости от степени трудоемкости.

Для получения *количественных оценок* выбранных параметров исследуемого объекта наиболее эффективными являются *методы индивидуальной работы экспертной группы*. Задача определения среднего времени расследования преступлений по каждой категории хорошо решается в рамках этой технологии.

Наиболее известным методом получения индивидуального мнения членов экспертной группы является *метод Дельфи*. Работа экспертов по этому методу организована следующим образом.

Вначале проводится индивидуальный опрос экспертов, при этом они не контактируют друг с другом. Затем происходит статистическая обработка индивидуальных экспертных оценок в целях определения усредненного мнения группы, а также крайних оценок.

Эта обобщенная информация вместе с аргументами экспертов (без персонификации) в пользу своих суждений сообщается всем экспертам. После ознакомления с ней эксперты могут изменить свои первоначальные оценки, если сочтут аргументы коллег убедительными, либо оставить их без изменения. Процедура повторяется несколько раз и завершается при стабилизации экспертных оценок [54].

5. *Анализ и обработка информации, полученной от экспертов*. Заполненные экспертами анкеты являются необходимым материалом для определения коллективной оценки. В зависимости от характера признаков, измеряемых экспертами, формируются правила обработки индивидуальных экспертных оценок, и для получения групповых оценок используется тот или иной метод оценки.

В нашем случае, когда требуется оценить объект (определить время расследования преступлений по каждой категории) в виде определенного числа, анализ результатов опроса производится *методом средней*. Рассмотрим его.

Метод средней используется при оценке явления в виде определенного числа. Экспертов просят определить, например, среднее время расследования преступлений по пяти категориям. Оценки заносятся в таблицу (см., например, табл. 4.2).

Таблица 4.2

Сводная таблица экспертных оценок по времени расследования преступлений 1 категории

Эксперты	1	2	3	4	5
Коэффициенты компетентности	0,2	0,21	0,13	0,21	0,25
Время расследования преступлений первой категории (1 сутки)	40	35	30	45	40

Групповой оценкой является нахождение среднего значения всех оценок, если не учитывается компетентность экспертов, или нахождение средневзвешенного, если их компетентность учитывается.

В данном случае:

- без учета компетентности экспертов X = (40 + 35 + 30 + 45 + + 40): 5 = 38;
- с учетом компетентности экспертов X = 40 · 0,2 + 35 · 0,21 + + 30 · 0,13 + 45 · 0,21 + 40 · 0,25 = 38,7.

Нетрудно заметить, что учет компетентности изменяет групповую экспертную оценку.

Аналогичным образом определяется время расследования преступлений по остальным четырем категориям преступлений.

6. *Определение степени согласованности экспертов*. После получения групповой оценки рабочая группа выясняет, можно ли пользоваться результатом и рекомендовать его в качестве основы для последующего решения. Для этого необходимо уточнить степень согласованности мнений экспертов. В случае их высокой согласованности результат экспертной оценки признается окончательным. Определение степени согласованности экспертов зависит от используемого метода.

Если для расчета групповой оценки используется метод средней, то показателем согласованности мнений экспертов является *коэффициент вариации V*. Когда $V = 0$, то имеется полная согласованность экспертов. Поэтому степень согласованности тем выше, чем меньше значение *V*.

Коэффициент вариации — показатель относительный. Он выражается в процентах и рассчитывается по формуле:

$$K_{вар} = \frac{\sigma}{x_{ср}} \cdot 100\,\%, \qquad (6)$$

где σ — среднее квадратичное отклонение;
$x_{ср}$ — средняя арифметическая величина.

Для расчета среднего квадратичного отклонения σ необходимо предварительно вычислить дисперсию *D*, так как σ рассчитывается по формуле:

$$\sigma = \sqrt{D}. \qquad (7)$$

При расчете дисперсии можно воспользоваться программой Microsoft Excel.

Шаг 1. Копируем табл. 4.2 в окно программы Excel (рис. 4.3), затем устанавливаем курсор в ячейку, где отразятся результаты расчета дисперсии (в нашем случае это ячейка с координатами Н6). Используя мастер функций f_x, выбираем в окне Категория — Статистические, в окне Выберите функцию — ДИСПРА, кликаем по кнопке ОК.

Шаг 2. В появившемся окне Аргументы функции в поле Значение 1 помещаем координаты диапазона ячеек С6: G6 сводной таблицы экспертных оценок (рис 4.4.). После клика по кнопке ОК получаем дисперсию: *D* = 26.

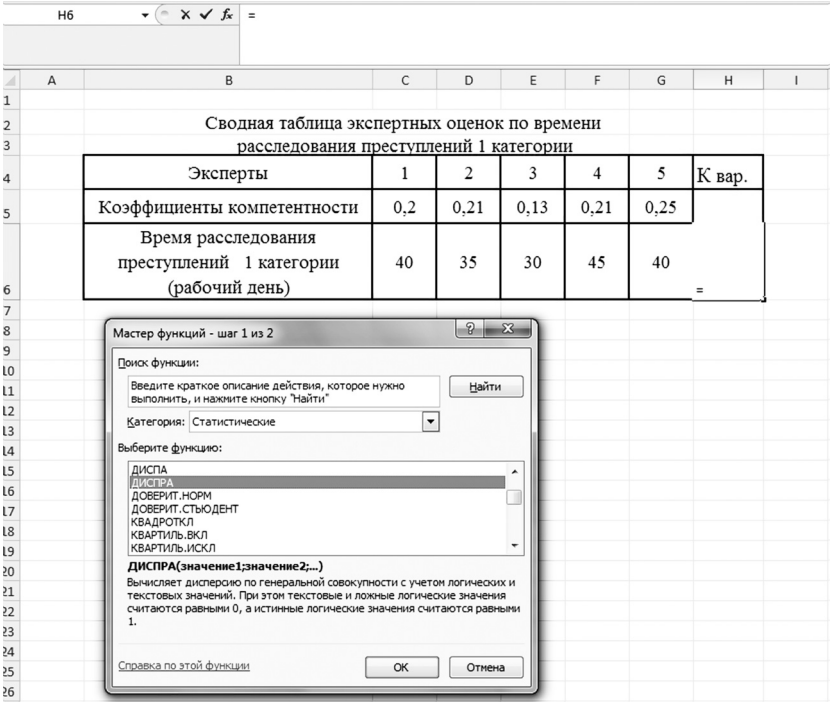


Рис. 4.3. Расчет дисперсии ответов экспертов, шаг 1

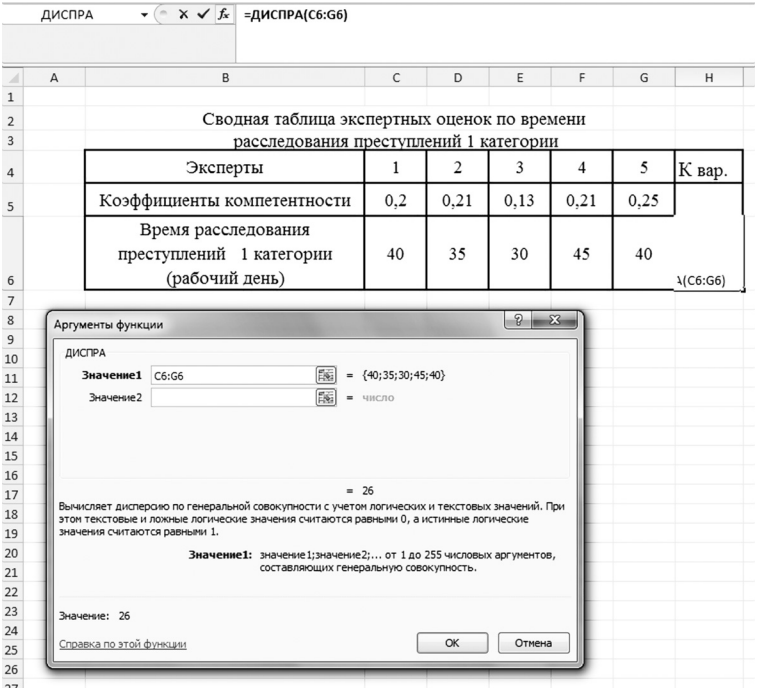


Рис. 4.4. Расчет дисперсии ответов экспертов, шаг 2

Подставляя полученное значение в формулу (6), получаем:

$$\sigma = \sqrt{D} = 5{,}09.$$

Для расчета коэффициента вариации необходимо в соответствии с формулой (5) найти среднее арифметическое оценок экспертов:

$$X = \frac{40 + 35 + 30 + 35 + 30 + 45 + 40}{5} = 38.$$

Подставляя $x_{ср}$ и σ в формулу (5), получаем:

$$K_{вар} = \frac{5{,}09}{38} \cdot 100\ \% = 14{,}03.$$

Коэффициент вариации является критерием объективности средней арифметической величины. Считают, что если он больше 30%, то объективность такой средней величины очень невысока. И наоборот, если значение разброса мнений экспертов мало (< 30%), то средняя величина является объективной и степень согласованности экспертов достаточна для принятия решения [54]. В нашем случае $К_{вар}$ — 14,03%, что является основанием для утверждения в качестве временно́го норматива расследования преступлений 1 катего-

рии $X_{ср}$ — 38 дней (без учета компетенции экспертов) или 38,7 — с учетом компетенции экспертов.

7. *Приведение коллективной оценки в форму, удобную для решения*. В результате проведенной экспертизы должны быть решены следующие задачи:

1) разработан набор качественных и количественных показателей для классификации преступлений по величине трудоемкости;
2) определены диапазоны значений количественных показателей для отнесения преступлений к соответствующей категории;
3) определено среднее время расследования преступлений каждой категории с доверительным интервалом разброса.

Рабочая группа, получив окончательную коллективную оценку, составляет записку, в которой излагаются результаты экспертизы. В этом документе содержится следующая информация: постановка задачи; процедура опроса; состав и компетентность экспертов; метод получения экспертных оценок; коллективная оценка и ее обоснование; степень согласованности экспертов; количество туров опроса; особые мнения экспертов, не согласных с коллективной оценкой, и обоснование их мнений; дата проведения экспертизы; подписи членов рабочей группы. Эта записка передается руководству для последующего принятия решений по проблеме, для которой проводилась экспертиза.

4.5.2. Информационно-технологическая процедура классификации преступлений по категориям трудоемкости и определение расчетных показателей пропускной способности

Рассмотрим (условно) деятельность УМВД России по Сергеевской области. В результате классификации все преступления были разбиты, допустим, на 5 категорий трудоемкости. Для каждой категории определен ориентировочный срок расследования преступлений.

Например:

— для преступлений 1 категории определен срок расследования в 38,7 рабочих дня;

– 2 категории — 20;

– 3 категории — 15;

– 4 категории — 10;

– 5 категории — 5 (см. табл. 4.4).

Таким образом, самые сложные и трудоемкие преступления определены в первую группу, наименее трудоемкие — в пятую.

Результаты классификации преступлений по категориям трудоемкости по Сергеевской области представлены в табл. 4.3.

Таблица 4.3

Классификация преступлений по категориям трудоемкости

Наименование отдела полиции	Количество преступлений по категориям				
	1	2	3	4	5
Ленинский	0	207	153	180	360
Октябрьский	0	70	70	210	350
Фрунзенский	22	264	275	341	198
г. Сергеев	24	184	456	80	56
Александровский	39	221	327	39	337
Вязниковский	18	202	492	53	114
Гороховецкий	13	54	31	59	100
Гусь-Хрустальный	23	200	123	70	170
Камешковский	0	312	159	159	62
Киржачский	10	266	335	237	138

Представим абсолютные значения преступлений в виде процентных соотношений от общего количества преступлений по категориям для каждого подразделения. Добавим дополнительный столбец для результатов расчета итоговой «пропускной способности» на одного следователя (табл. 4.4).

Таблица 4.4

Расчет «пропускной способности» одного следователя

Наименование отдела полиции	Количество преступлений по категориям,%					Пропускная способность одного следователя
	1	2	3	4	5	
Ленинский	0	23	17	20	40	11,500
Октябрьский	0	10	10	30	50	9,000
Фрунзенский	2	24	25	31	18	13,324
г. Сергеев	3	23	57	10	7	15,661
Александровский	4	23	34	4	35	13,398
Вязниковский	2	23	56	6	13	15,024
Гороховецкий	5	21	12	23	39	12,185
Гусь-Хрустальный	4	34	21	12	29	14,148
Камешковский	0	45	23	23	9	15,200

Окончание табл. 4.4

Наименование отдела полиции	Количество преступлений по категориям,%					Пропускная способность одного следователя
	1	2	3	4	5	
Киржачский	1	27	34	24	14	13,987
Время расследования по категориям	38,7	20,0	15,0	10,0	5,0	

Итоговая «пропускная способность» на одного следователя рассчитывается как средневзвешенная. Например, для Ленинского района:

$$\gamma = 0 \cdot 38{,}7 + 0{,}23 \cdot 20 + 0{,}17 \cdot 15 + 0{,}2 \cdot 10 + 0{,}4 \cdot 5 + 11{,}5.$$

Аналогичным образом рассчитываются значения пропускной способности одного следователя по другим районам (см. табл. 4.4).

На основании полученных значений пропускной способности γ и имеющихся данных по каждому подразделению о количестве уголовных дел в производстве V и численности следователей R в подразделении в отчетном периоде можно рассчитать теоретический (нормативный) коэффициент расследованных преступлений $\alpha_т$, который при сложившейся оперативной обстановке и с учетом нагрузки должно показать подразделение. При этом еще на этапе экспертизы следует определиться с допустимым интервалом рассеяния вокруг показателя теоретического коэффициента расследованных преступлений $\alpha_{т.}$

Для этого воспользуемся формулой системной динамики (4) и выполним расчет по следующей технологии.

1. Представим данные для расчета теоретического коэффициента расследованных преступлений $\alpha_т$ (табл. 4.5).

Таблица. 4.5

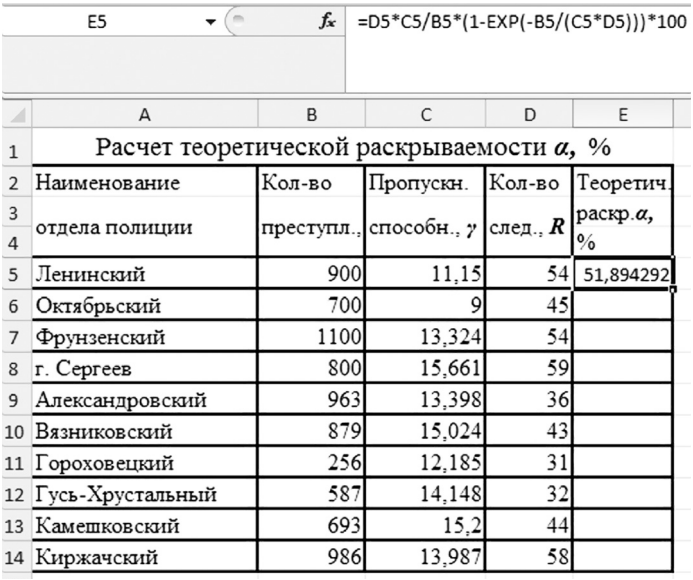
Данные для расчета теоретического коэффициента расследованных преступлений $\alpha_т$,%

Наименование отдела полиции	Количество преступлений, V	Пропускная способность, γ	Количество следователей, R	Теоретическая раскрываемость
Ленинский	900	11,150	54	
Октябрьский	700	9,000	45	
Фрунзенский	1100	13,324	54	
г. Сергеев	800	15,661	59	
Александровский	963	13,398	36	

Окончание табл. 4.5

Наименование отдела полиции	Количество преступлений, V	Пропускная способность, γ	Количество следователей, R	Теоретическая раскрываемость
Вязниковский	879	15,024	43	
Гороховецкий	256	12,185	31	
Гусь-Хрустальный	587	14,148	32	
Камешковский	693	15,200	44	
Киржачский	986	13,987	58	

2. Скопируем табл. 4.5 в окно программы Excel, установим курсор в ячейку E5 и рассчитаем $\alpha_т$ по формуле (4) для Ленинского района (см. рис. 4.5).



	A	B	C	D	E
1	Расчет теоретической раскрываемости *α*, %				
2	Наименование	Кол-во	Пропускн.	Кол-во	Теоретич.
3	отдела полиции	преступл.,	способн., *γ*	след., *R*	раскр.*α*,
4					%
5	Ленинский	900	11,15	54	51,894292
6	Октябрьский	700	9	45	
7	Фрунзенский	1100	13,324	54	
8	г. Сергеев	800	15,661	59	
9	Александровский	963	13,398	36	
10	Вязниковский	879	15,024	43	
11	Гороховецкий	256	12,185	31	
12	Гусь-Хрустальный	587	14,148	32	
13	Камешковский	693	15,2	44	
14	Киржачский	986	13,987	58	

Рис. 4.5. Расчет теоретического (нормативного) коэффициента расследованных преступлений $\alpha_т$ для территориального подразделения органа внутренних дел Ленинского района Сергеевской области

3. Скопируем формулу из ячейки E5 в блок ячеек E6 — E14. Получим набор значений теоретического коэффициента расследованных преступлений для каждого подразделения Сергеевской области.

4.5.3. Построение рейтинга подразделений

Полученные значения теоретического коэффициента расследованных преступлений (рис. 4.6) могут быть рассмотрены как своеобразный норматив для территориальных подразделений ОВД. Если результаты практической деятельности подразделений за отчетный период показывают соответствие нормативу или превышают его, то можно сделать вывод об эффективной работе подразделения. Отклонение от норматива в меньшую сторону свидетельствует о наличии управленческих и профессиональных проблем в подразделении. Величину и направление таких отклонений можно взять в качестве критерия для построения нового рейтинга подразделений, где будет учитываться не только нагрузка следователей, но и трудоемкость преступлений, расследованных в отчетный период.

Допустим, территориальные подразделения ОВД Сергеевской области за отчетный период показали практические результаты, представленные в табл. 4.6.

E5 f_x =C5*D5/B5*(1-EXP(-B5/(C5*D5)))*100

	A	B	C	D	E
1	Расчет теоретической раскрываемости α_m				
2	Наименование	Кол-во	Пропускн.	Кол-во	Теоретич.
3	отдела полиции	прест., V	способн., γ	следоват.	раскрыв. α,
4					
5	Ленинский	900	11,15	54	51,8942921
6	Октябрьский	700	9	45	47,5834981
7	Фрунзенский	1100	13,324	54	51,2290789
8	г. Сергеев	800	15,661	59	66,9074505
9	Александровский	963	13,398	36	43,2842682
10	Вязниковский	879	15,024	43	54,6442155
11	Гороховецкий	256	12,185	31	72,629666
12	Гусь-Хрустальный	587	14,148	32	56,0351002
13	Камешковский	693	15,2	44	62,2663448
14	Киржачский	986	13,987	58	57,87433
15					

Рис 4.6. Расчет теоретического (нормативного) коэффициента расследованных преступлений $\alpha_т$ для территориальных подразделений органов внутренних дел Сергеевской области

Таблица 4.6

Значения практического коэффициента расследованных преступлений по Сергеевской области

№ п/п	Наименование отдела полиции	Коэффициент расследованных преступлений, $\alpha_{пр}$,%
1	Камешковский	72,43
2	Киржачский	71,51
3	Фрунзенский	68,85
4	Гусь-Хрустальный	68,83
5	г. Сергеев	68,45
6	Александровский	67,80
7	Гороховецкий	65,23
8	Вязниковский	56,78
9	Октябрьский	56,47
10	Ленинский	49,11

Как следует из данных табл. 4.6, лучшим отделом полиции по расследованным преступлениям является отдел полиции Камешковского района: $\alpha_{пр}$ = 72,43%. Худшие показатели за отчетный период показал Ленинский район: $\alpha_{пр}$ = 49,11%.

Посмотрим, насколько изменится рейтинг подразделений, если будем учитывать особенности оперативной обстановки: сложность и трудоемкость преступлений, расследованных в отчетный период в каждом районе, нагрузку на следователей.

Для этого построим рейтинг подразделений в зависимости от разности практического и теоретического (нормативного) коэффициентов расследованных преступлений. Результаты расчетов представим в табл. 4.7.

Таблица 4.7

Рейтинг подразделений по Сергеевской области

№ п/п	Наименование отдела полиции	Практическая раскрываемость, $\alpha_{пр}$,%	Теоретическая раскрываемость, $\alpha_{т}$,%	Разность, $\alpha_{пр} - \alpha_{т}$,%
1	Фрунзенский	68,85	51,23	17,62
2	Киржачский	71,51	57,87	13,64
3	Гусь-Хрустальный	68,83	56,04	12,79

Окончание табл. 4.7

№ п/п	Наименование отдела полиции	Практическая раскрываемость, $\alpha_{пр}$,%	Теоретическая раскрываемость, $\alpha_{т}$,%	Разность, $\alpha_{пр} - \alpha_{т}$,%
4	Александровский	67,80	55,81	11,99
5	Камешковский	72,43	62,27	10,16
6	Октябрьский	56,47	47,58	8,89
7	Вязниковский	56,78	54,64	2,14
8	г. Сергеев	68,45	70,08	–1,63
9	Ленинский	49,11	51,89	–2,78
10	Гороховецкий	65,23	72,63	–7,40

Наибольшее превышение показателя расследованных преступлений над своим нормативом (табл. 4.7) показал Фрунзенский отдел полиции — 17,62%. Он возглавляет таблицу рейтинга и является наиболее эффективно действующим подразделением. Камешковский отдел полиции, возглавлявший таблицу рейтинга (табл. 4.6) по количеству расследованных преступлений $\alpha_{пр}$, по эффективности работы оказывается только на пятом месте. В то же время, занимающий 7 место по количеству расследованных преступлений Гороховецкий отдел полиции, по эффективности работы оказывается на последнем, десятом месте, — разность со «своим нормативом» составляет 7,4%.

Таким образом, представленная технология позволяет избавиться от наследия «палочной» системы учета преступлений и включает в себя решение ряда задач.

1. Методом экспертных оценок разрабатывается система количественных и качественных показателей, предназначенных для классификации преступлений по уровню сложности и трудоемкости.

2. На основе выбранных критериев экспертная группа проводит классификацию преступлений по категориям с учетом уровня сложности и трудоемкости.

3. Для каждой категории преступлений определяется нормативное время расследования преступлений.

4. Исходя из годового временного ресурса одного следователя, определяется его «пропускная способность» — количество уголовных дел различных категорий сложности, которое он может расследовать за год.

5. По формуле динамического равновесия показателей раскрытых и расследованных преступлений, интенсивности зарегистрированной преступности и кадровой обеспеченности (4) определяется нормативный коэффициент расследованных преступлений территориального подразделения ОВД, соотнесенный с особенностями оперативной обстановки за отчетный период.

6. Выстраивается рейтинг подразделений в зависимости от разности практического и теоретического (нормативного) коэффициентов расследованных преступлений.

Контрольные вопросы

1. Какой нормативный документ регламентирует оценку деятельности территориальных подразделений ОВД? Каковы особенности предложенного в нем подхода к системе оценки деятельности территориальных подразделений ОВД?

2. В чем недостатки «палочной» системы учета преступлений? Какие направления нового подхода к системе оценки деятельности территориальных подразделений ОВД позволят их избежать?

3. Что понимается под выражением «нормирование труда следственных подразделений»? Какие направления их работы можно «нормировать»?

4. Какой эмпирический метод применяется для классификации преступлений по величине сложности и трудоемкости преступлений?

5. В чем заключается характеристика основных этапов проведения экспертизы по разработке показателей системы оценки деятельности территориальных подразделений?

6. Что такое «динамическое равновесие показателей раскрытых и расследованных преступлений, интенсивности зарегистрированной преступности и кадровой обеспеченности»? Как его использовать для оценки деятельности следственных подразделений ОВД?

7. Существует ли разница между теоретическим и практическим коэффициентами расследованных преступлений?

8. В чем суть построения рейтинга следственных подразделений по нормированию труда следователей и динамическому равновесию показателей раскрытых и расследованных преступлений, интенсивности зарегистрированной преступности и кадровой обеспеченности?

Список использованных источников

Нормативно-правовая база

1. О навигационной деятельности: федер. закон от 14.02.2009 № 22-ФЗ: ред. от 13.07.2015. Доступ из справ.-правовой системы «КонсультантПлюс».

2. О полиции: федер. закон от 07.02.2011 № 3-ФЗ: ред. от 05.12.2017. Доступ из справ.-правовой системы «КонсультантПлюс».

3. О связи: федер. закон от 07.07.2003 № 126-ФЗ: ред. от 05.12.2017. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ: ред. от 25.11.2017. Доступ из справ.-правовой системы «КонсультантПлюс».

5. О Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город»: постановление Правительства Рос. Федерации от 20.01.2014 № 39: ред. от 23.09.2017. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS: постановление Правительства Рос. Федерации от 25.08.2008 № 641: ред. от 12.11.2016. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: распоряжение Правительства Рос. Федерации от 03.12.2014 № 2446-р // Собр. законодательства Рос. Федерации. 2014. № 50, ст. 7220.

8. Об утверждении состава Межведомственной комиссии по внедрению и развитию систем аппаратно-программного комплекса технических средств «Безопасный город», системы обеспечения вызова экстренных оперативных служб по единому номеру «112» и Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС»: распоряжение Правительства Рос. Федерации от 10.11.2017 № 2489-р. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Вопросы организации работы сервиса обеспечения деятельности подразделений материально-технического обеспечения органов внутренних дел Российской Федерации: приказ МВД России от 24.03.2016 № 133. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

10. Вопросы организации работы сервиса обеспечения деятельности правовых подразделений системы МВД России: приказ МВД России от 23.12.2016 № 888: ред. от 06.10.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

11. Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации: приказ МВД России от 31.12.2013 № 1040: ред. от 13.02.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

12. Вопросы эксплуатации программного комплекса формирования и ведения единого банка данных подразделений архивной информации органов

внутренних дел Российской Федерации: приказ МВД России от 15.01.2016 № 14. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

13. Вопросы эксплуатации программного обеспечения для реализации сервиса обеспечения оперативно-служебной деятельности НЦБ Интерпола МВД России: приказ МВД России от 03.11.2016 № 696: ред. от 27.07.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

14. Вопросы эксплуатации программного обеспечения для реализации сервиса оформления проезда сотрудников органов внутренних дел Российской Федерации и военнослужащих внутренних войск МВД России по электронным воинским перевозочным документам: приказ МВД России от 19.11.2015 № 1112: ред. от 07.11.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

15. Вопросы эксплуатации программного обеспечения для реализации Сервиса обеспечения охраны общественного порядка: приказ МВД России от 11.01.2016 № 1. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

16. Вопросы эксплуатации программного обеспечения для реализации Сервиса обеспечения кадровой деятельности: приказ МВД России от 28.06.2016 № 349: ред. от 07.06.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

17. Вопросы эксплуатации сервиса обеспечения деятельности организационно-штатных подразделений органов внутренних дел Российской Федерации: приказ МВД России от 22.04.2015 № 460: ред. от 07.12.2016. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

18. Вопросы эксплуатации сервиса предоставления государственных услуг: приказ МВД России от 03.11.2015 № 1054. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

19. О вводе в эксплуатацию Системы удостоверяющих центров органов внутренних дел Российской Федерации: приказ МВД России от 28.05.2013 № 294: ред. от 25.12.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

20. О мероприятиях по созданию единой системы информационно-аналитического обеспечения деятельности МВД России: приказ МВД России от 30.07.2011 № 891: ред. от 30.11.2012. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

21. О порядке и этапах оснащения транспортных средств органов внутренних дел Российской Федерации и внутренних войск МВД России аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS: приказ МВД России от 26.09.2009 № 737. Доступ из справ.-правовой системы «КонсультантПлюс».

22. О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции: приказ МВД России от 05.02.2016 № 60. Доступ из справ.-правовой системы «КонсультантПлюс».

23. О принятии на снабжение программно-технических комплексов: приказ МВД России от 19.06.2009 № 465. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

24. О системе информационного обеспечения централизованного учета оружия, контроля за соблюдением законодательства Российской Федерации в области оборота оружия, частной детективной (сыскной) и охранной деятельности Министерства внутренних дел Российской Федерации: приказ МВД России от 15.10.2014 № 883. Доступ из справ.-правовой системы «КонсультантПлюс».

25. Об организационных мероприятиях по участию органов внутренних дел Российской Федерации в создании и развитии аппаратно-программного комплекса «Безопасный город»: приказ МВД России от 09.12.2015 № 1149: ред. 31.12.2016. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

26. Об утверждении Концепции информатизации органов внутренних дел Российской Федерации и внутренних войск МВД России до 2012 года: приказ МВД России от 04.04.2009 № 280. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

27. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169: ред. от 26.10.2016. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

28. Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012—2014 годах: приказ МВД России от 30.03.2012 № 205. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

29. Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации: приказ МВД России от 23.09.2015 № 926: ред. от 25.08.2017. Доступ из специализир. территориально распределен. автоматизир. системы «Юрист».

30. Концепция обеспечения безопасности жизнедеятельности населения Хабаровского края «Безопасный край» на 2014—2020 годы: распоряжение Правительства Хабар. края от 24.06.2013 № 429-рп // Электронный фонд правовой и нормативно-технической документации: сайт. URL: http://docs.cntd.ru/document/465309815 (дата обращения:01.03.2018).

Производственно-практическая литература (методические рекомендации, требования и др.), управленческая, техническая документация, информационные материалы

31. АПК «Безопасный город»: построение (развитие), внедрение и эксплуатация: метод. рек. / В. В. Гаршин [и др.]. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2015. 72 с.

32. Аппаратно-программный комплекс «Безопасный город» // МЧС России: сайт. URL: http://mchs.gov.ru/dop/Bezopasnij_gorod (дата обращения: 01.03.2018).

33. В Хабаровске эффективно работает современный аппаратно-программный комплекс «Безопасный город» // Администрация города Хабаров-

ска: сайт. URL: https://www.khabarovskadm.ru/news/index.php? ELEMENT_ ID=718253 (дата обращения: 01.03.2018).

34. Временные единые требования к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город»: одобр. на заседании Межведомств. комиссии по вопросам, связан. с внедрением и развитием систем аппарат.-програм. комплекса техн. средств «Безопасный город» под рук. зам. председателя Правительства Рос. Федерации Д. О. Рогозина 23.12.2014. М.: МЧС России, 2014. 147 с.

35. Всероссийская конференция «Аппаратно-программный комплекс ″Безопасный город″». URL: http://апкбг.рф: сайт (дата обращения: 01.03.2018).

36. Доклад отв. секретаря МВК Ананьева А. Н. об архитектуре АПК БГ и реализации принципов импортозамещения // МЧС России: сайт. URL: http://www.mchs.gov.ru/document/4742843 (дата обращения: 01.03.2018).

37. Методические рекомендации по построению и развитию АПК «Безопасный город» в субъектах Российской Федерации: утв. зам. министра Рос. Федерации по делам гражд. обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, зам. председателя Межведомств. комиссии по вопросам, связан. с внедрением и развитием систем аппарат.-програм. комплекса техн. средств «Безопасный город» А. П. Чуприяном 08.12.2016 // МЧС России: сайт. URL: http://www.mchs.gov.ru/upload/site1/document_file/ne7XCJAFMN.pdf (дата обращения: 01.03.2018).

38. Методические рекомендации по применению спутниковых навигационно-мониторинговых систем на основе радионавигационной системы ГЛОНАСС в интересах органов внутренних дел. М.: ГУ НПО «Специальная техника и связь МВД России», 2009. 112 с.

39. Методическое пособие по разработке организационных документов по созданию и развитию аппаратно-программного комплекса «Безопасный город» / С. А. Качанов [и др.]. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2016. 219 с.

40. Протокол совещания рабочей группы для обеспечения рабочего взаимодействия при реализации плановых мероприятий работы Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город» от 17.01.2017 № 12. URL: http://www.mchs.gov.ru/upload/site1/document_file/hSxrnbaAHX.pdf (дата обращения: 01.03.2018).

41. Протокол совещания рабочей группы для обеспечения рабочего взаимодействия при реализации плановых мероприятий работы Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город» от 24.11.2016 № 11. URL: http://www.mchs.gov.ru/upload/site1/document_file/VJrqD2b1E0.pdf (дата обращения: 01.03.2018).

42. Рыбак А. В. Оценка эффективности деятельности следственных подразделений на основе методов системной динамики: метод. реком. / Дальневосточ. юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2016. 33 с.

43. Сервис управления доступом к информационным системам и ресурсам единой системы информационно-аналитического обеспечения деятельности МВД России: метод. реком. по интеграции сервисов ИСОД с Сервисом управления доступом в контуре ЗИ (версия 3.3). М., 2014. 131 с.

44. Сервис управления доступом к информационным системам и ресурсам единой системы информационно-аналитического обеспечения деятельности МВД России: методические рекомендации по интеграции сервисов ИСОД с СУДИС (версия 4.0). М., 2016. 92 с.

45. Создание типовых центров многоуровневой системы контроля и управления подвижными объектами и системы информационной поддержки территориальных ОВД и подразделений внутренних войск МВД России: опыт.-конструктор. работа (шифр «Центр-НМС»): техн. проект. Пояснительная записка ИВЯФ.464428.110.ПЗ. М.: ОАО «Российские космические системы», 2013. 72 с.

46. Prognoz Platform 8.2. Онлайн-документация // АО «ПРОГНОЗ»: сайт. URL: http://help.prognoz.com/ru/ (дата обращения: 01.03.2018).

Научная и учебная литература

47. Анализ данных и процессов: учеб. пособие / А. А. Барсегян [и др.]. СПб.: БХВ-Петербург, 2009. 512 с.

48. Аппаратные средства вычислительной техники: учеб. для вузов: в 2 кн. / под общ. науч. ред. В. А. Минаева, Н. Г. Топольского, А. П. Фисуна. Орел: ГУ УНПК, ОГУ, 2014.

Кн. 1. 311 с.

Кн. 2. 151 с.

49. Аппаратные средства вычислительной техники: учеб. пособие / К. М. Бондарь [и др.]. Хабаровск: Дальневосточ. юрид. ин-т МВД России, 2012. 160 с.

50. Башмаков М. В. Новые направления создания навигационно-мониторинговых систем МВД России с использованием современных навигационных и информационных технологий // Информационные технологии, связь и защита информации МВД России — 2015: темат. сб. М.: ООО «Компания ″ИНФОРМАЦИОННЫЙ МОСТ″», 2015. С. 46—49.

51. Бокова О. И., Дунин В. С., Хохлов Н. С. К вопросу о внедрении механизмов интеллектуального анализа в информационную среду АПК «Безопасный город» // Моделирование, оптимизация и информационные технологии: электрон. науч. журн. 2015. № 4 (11). URL: https://moit.vivt.ru/wp-content/uploads/2015/12/BokovaSoavtori_4_15_1.pdf (дата обращения: 01.05.2016).

52. Бондарь К. М., Едынак И. В., П. Б. Скрипко. Базы данных в деятельности органов внутренних дел: учеб.-практ. пособие. Хабаровск: Дальневосточ. юрид. ин-т МВД России, 2012. 92 с.

53. Бондарь К. М., Емельянова О. В., Скрипко П. Б. Методика проведения аналитической работы в органах внутренних дел: учеб.-практ. пособие / Дальневосточ. юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2013. 144 с.

54. Бондарь К. М., Рыбак А. В., Скрипко П. Б. Прогнозирование преступности в аналитической деятельности органов внутренних дел: учеб.-практ. пособие / Дальневосточ. юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2014. 72 с.

55. Дворянкин С. В., Жаркой Р. М., Минаев В. А. Безопасный город: интеллектуальные технологии // Спецтехника и связь. 2010. № 2—3. С. 23—30.

56. Дунин В. С. К вопросу о создании доверенной среды КАИАС «Безопасный город» как сервиса ИСОД ОВД // Охрана, безопасность, связь — 2014: мат-лы междунар. науч.-практ. конф. Воронеж: Воронеж. ин-т МВД России. 2015. С. 139—143.

57. Дунин В. С. Некоторые аспекты реализации положений концепции АПК «Безопасный город» // Общественная безопасность, законность и правопорядок в III тысячелетии — 2015: сб. мат. междунар. науч.-практ. конф. Воронеж: Воронежский ин-т МВД России, 2015. Ч. 3. С. 19—23.

58. Дунин В. С. Развитие КАИАС «Безопасный город» на примере совершенствования подсистемы видеонаблюдения // Охрана, безопасность, связь — 2013: мат. междунар. науч.-практ. конф. Воронеж: Воронежский ин-т МВД России. 2014. Ч. 1. С. 191—194.

59. Дюк В., Самойленко А. Data Mining: учеб. курс. СПб.: Питер, 2001. 368 с.

60. Информатика и информационные технологии в профессиональной деятельности: курс лекций / под ред. К. М. Бондаря; Дальневосточ. юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2015. 188 с.

61. Информатика и информационные технологии в юридической деятельности: учеб. пособие. Изд. 2-е, испр. и доп. / под ред. В. А. Минаева, А. П. Фисуна, К. М. Бондаря. Хабаровск: Дальневосточ. юрид. ин-т МВД России, 2011. 380 с.

62. Информатика: в 3 ч.: учеб. для вузов / под общ. науч. ред. В. А. Минаева, М. П. Сычева, А. П. Фисуна. Орел: ОрелГТУ, ОГУ, 2014.

Ч. 1. Методологические и технологические основы. 265 с.

Ч. 2. Организационные и технико-экономические основы. 398 с.

Ч. 3. Методы, модели и средства обработки графической информации. 628 с.

63. Информационные системы и технологии в профессиональной деятельности сотрудников органов внутренних дел: учеб. пособие / К. М. Бондарь [и др.]; Дальневосточ. юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2013. 216 с.

64. Информационные технологии управления: учеб. пособие для вузов / под ред. проф. Г. А. Титоренко. М.: ЮНИТИ-ДАНА, 2003. 439 с.

65. Ляшенко С. Н. Основные этапы развития информационных технологий, связи и защиты информации в МВД России // Информационные технологии, связь и защита информации МВД России — 2016: темат. сб. М.: ООО «Компания ″ИНФОРМАЦИОННЫЙ МОСТ″», 2016. С. 18—21.

66. Ляшенко С. Н. Этапы и ключевые направления развития информационно-телекоммуникационной системы МВД России // Информационные технологии, связь и защита информации МВД России — 2015: темат. сб. М.: ООО «Компания ″ИНФОРМАЦИОННЫЙ МОСТ″», 2015. С. 16—19.

67. Методы и модели анализа данных: OLAP и Data Minig / А. А. Барсегян [и др.]. СПб.: БХВ-Петербург, 2004. 336 с.

68. Минаев В. А. Кадровые ресурсы органов внутренних дел: современные подходы к управлению: моногр. М.: Академия МВД СССР, 1991. 163 с.

69. Минаев В. А., Умеренков В. В. Космические навигационные системы в деятельности оперативных служб: учеб. пособие. Орел: Орлов. гос. техн. ун-т, 1999. 96 с.

70. Паклин Н. Б., Орешков В. И. Бизнес-аналитика: от данных к знаниям. СПб.: БХВ-Петербург, 2009. 624 с.

71. Правовые основы информационной безопасности: учеб. / Ю. А. Белевская [и др.]; под общ. науч. ред. В. А. Минаева [и др.]: в 2-х кн. Кн. 1. Орел: ГУ УНПК, ОГУ, 2014. 200 с.

72. Рыбак А. В., Скрипко П. Б., Бондарь К. М. Основы управления в органах внутренних дел: курс лекций / под ред. А. В. Рыбака; Дальневосточ. юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2015. 176 с.

73. Скрипко П. Б. Основы делопроизводства: учеб.-практ. пособие; Дальневосточный юрид. ин-т МВД России. Хабаровск: РИО ДВЮИ МВД России, 2014. 132 с.

74. Скрипко П. Б. Применение системы управления базами данных Microsoft Office Access в информационно-аналитическом обеспечении органов внутренних дел: учеб.-практ. пособие. Хабаровск: Дальневосточ. юрид. ин-т МВД России, 2011. 88 с.

75. Тарасов А. В. Опыт в создании аналитических решений в органах МВД // Информационные технологии, связь и защита информации правоохранительных органов — 2013: темат. сб. М.: ООО «Компания ″ИНФОРМАЦИОННЫЙ МОСТ″», 2013. Ч. 1. С. 18—19.

76. Теория информации: учеб. для вузов: в 2 кн. / под общ. науч. ред. В. Т. Еременко [и др.]. Орел: ОрелГТУ, ОГУ, 2014.

Кн. 1. 226 с.

Кн. 2. 312 с.

77. Фурсик А. В. Железный инспектор // Информационные технологии, связь и защита информации правоохранительных органов — 2013: темат. сб. М.: ООО «Компания ″ИНФОРМАЦИОННЫЙ МОСТ″», 2013. Ч. 1. С. 12—13.

78. Шерстюков С. А., Кожин А. Ю. Системы и сети передачи информации в единой информационно-телекоммуникационной системе органов внутренних дел Российской Федерации: учеб. пособие. Воронеж: Воронеж. ин-т МВД России, 2012. 264 с.

Электронные ресурсы государственных органов; компаний, организаций

79. Компания «Информационный Мост»: сайт ООО «Компания ″ИНФОРМАЦИОННЫЙ МОСТ″». URL: https://informost.ru (дата обращения: 01.03.2018).

80. КриптоПро. Ключевое слово в защите информации: сайт ООО «КРИПТО-ПРО». URL: http://cryptopro.ru (дата обращения: 01.03.2018).

81. Официальный интернет-портал государственных услуг. URL: https://gosuslugi.ru (дата обращения: 01.03.2018).

82. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф (доступ через Интернет и ИМТС МВД России) (дата обращения: 01.03.2018).

83. Рутокен: сайт компании. URL: https://rutoken.ru (дата обращения: 01.03.2018).

84. Система информационно-аналитического обеспечения деятельности Министерства внутренних дел Российской Федерации (ИСОД МВД России).

URL: https://it.mvd.ru (доступ через ИМТС МВД России) (дата обращения: 01.03.2018).

85. Удостоверяющий центр МВД России: сайт. URL: https://уц.мвд.рф (доступ через Интернет и ИМТС МВД России) (дата обращения: 01.03.2018).

86. ФКУ НПО «СТиС» МВД России: сайт. URL: http://stismvd.ru (дата обращения: 01.03.2018).

87. BaseGroup labs. Технологии анализа данных: сайт компании BaseGroup Labs, ООО «Аналитические технологии». URL: http://basegroup.ru (дата обращения: 01.03.2018).

88. infotecs: сайт ОАО «ИнфоТеКС». URL: http://infotecs.ru (дата обращения: 01.03.2018).

89. ISS. Интеллектуальные системы безопасности: сайт компании ISS. URL: http://iss.ru (дата обращения: 01.03.2018).

90. Macroscop: сайт компании. URL: http://macroscop.com (дата обращения: 01.03.2018).

91. RULEQUEST RESEARCH data mining tools. URL: http://rulequest.com (дата обращения: 01.03.2018).

92. Vocord. Системы видеонаблюдения и аудиорегистрации: сайт компании Vocord. URL: http://vocord.ru (дата обращения: 01.03.2018).

93. WizSoft, Inc.: сайт компании. URL: http://www.wizsoft.com/ (дата обращения: 01.03.2018).

Учебно-практическое пособие

Константин Михайлович Бондарь,
кандидат технических наук, доцент;
Вадим Сергеевич Дунин,
кандидат технических наук, доцент;
Александр Владимирович Рыбак,
кандидат технических наук, доцент;
Павел Борисович Скрипко,
кандидат технических наук, доцент
(Дальневосточный юридический институт МВД России)

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В УПРАВЛЕНИИ ДЕЯТЕЛЬНОСТЬЮ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Редактор ***И. В. Кравцова***
Корректор ***Н.Б. Хохлова***

Оригинал-макет
Дальневосточного юридического института МВД России

Подписано в печать 28.07.2018.
Формат 60×90 $^{1}/_{16}$. Бумага офсетная.
Усл. печ. л. 12,0. Тираж 2811 экз. Заказ № 9225.

Макет подготовлен и отпечатан при участии ООО ИПК «Медиа-Принт»
143200, г. Можайск, ул. Мира, 93.