Академия управления МВД России

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ И ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Курс лекций

Москва • 2021

УДК 004.056.5
ББК 32.973
И74

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *И. А. Кубасов,* главный научный сотрудник НИИСТ ФКУ НПО «СТиС» МВД России, доктор технических наук, почетный радист Российской Федерации; *А. Я. Балкаров,* заместитель начальника отдела МВД России по Тимирязевскому району г. Москвы, кандидат юридических наук.

И74

Информационные технологии управления и организация защиты информации: курс лекций / В. А. Апульцин, Ш. Х. Гонов, В. Н. Лебедев, В. Ю. Петрова. – Москва : Академия управления МВД России, 2021. – 72 с.

ISBN 978-5-907187-76-4

В курсе лекций рассматриваются особенности применения информационных технологий управления органами внутренних дел, в т. ч. правовые основы защиты информации и основы технической защиты информации. Обосновываются ключевые направления совершенствования организации применения методов анализа данных в информационно-аналитической деятельности органов внутренних дел.

Курс лекций может использоваться в учебном процессе по дисциплинам кафедры информационных технологий, преподаваемым обучающимся по направлениям подготовки: 38.04.02 Менеджмент; 38.04.03 Управление персоналом, 38.04.04 Государственное и муниципальное управление, а также по программам подготовки научно-педагогических кадров и дополнительным профессиональным программам повышения квалификации. Материалы курса лекций могут быть полезны практическим работникам штабных и информационных подразделений, а также специалистам, интересующимся актуальными вопросами использования компьютерных технологий в информационно-аналитической деятельности территориальных органов МВД России.

УДК 004.056.5
ББК 32.973

ISBN 978-5-907187-76-4

Авторский коллектив:

Апульцин *Владимир Анатольевич,* доцент кафедры информационных технологий, кандидат физико-математических наук – введение, заключение, лекция 3;

Гонов *Шамиль Хасанович,* доцент кафедры информационных технологий, кандидат технических наук – заключение, лекции 2, 3;

Лебедев *Вадим Николаевич,* кандидат технических наук, доцент – лекции 4, 5;

Петрова *Виктория Юрьевна,* доцент кафедры информационных технологий, кандидат технических наук, доцент – лекция 1.

Содержание

Введение 5

Лекция I. Правовые и организационные основы информатизации в Российской Федерации 6
Вопрос 1. Понятие информационных технологий в органах внутренних дел 6
Вопрос 2. Законодательство в сфере использования информационных технологий в органах внутренних дел 8
Вопрос 3. Концептуальные основы создания ИСОД 12

Лекция II. Информационные технологии в деятельности органов внутренних дел 15
Вопрос 1. Автоматизированные информационно-поисковые системы 15
Вопрос 2. Инфраструктура единого информационного пространства и Единая система информационно-аналитического обеспечения деятельности МВД России 21
Вопрос 3. Программное обеспечение информационных технологий 28

Лекция III. Аналитическое обеспечение информационных технологий 33
Вопрос 1. Технология анализа статистических данных 33
Вопрос 2. Технологии оценки результатов деятельности ОВД 39
Вопрос 3. Компьютерные технологии анализа социальных сетей 43

Лекция IV. Правовые основы защиты информации в Российской Федерации. Государственная система защиты информации 47
Вопрос 1. Понятие защиты информации. Актуальность изучения вопросов обеспечения защиты информации в ОВД 47
Вопрос 2. Правовые основы защиты информации в Российской Федерации 52

Лекция V. Основы технической защиты информации 57
Вопрос 1. Технические каналы утечки информации 57
Вопрос 2. Средства и методы обеспечения информационной безопасности 61

Заключение 67

Список литературы 68
Нормативные правовые акты 68
Основная литература 69
Электронные ресурсы 69

Введение

В современных условиях одним из направлений совершенствования управления органами внутренних дел является широкое использование компьютерной техники, информационных систем, современных инфо-, телекоммуникационных технологий. Их внедрение в повседневную деятельность служб и подразделений органов внутренних дел должно приводить к качественным изменениям алгоритмов и методов управления. Значительная часть информации, которую обрабатывают органы внутренних дел хранится в виде больших объемов неструктурированных и мало структурированных данных, включая тексты, изображения, видео и др. В этой связи ключевое и действительное различие между аналитической обработкой данных и расширенной аналитикой больших данных заключается в том, что традиционная аналитика, в отличие от расширенной, не в состоянии работать с разноформатными, в т. ч. неструктурированными данными. Принципиальным отличием больших данных от просто данных является их разноформатность, загрязненность и неполнота. Таким образом, перед правоохранительными органами стоит задача создания автоматизированного контура управления, проведения анализа данных с использованием современных математических методов и др. В лекциях рассматриваются проблемы: правового регулирования сбора, передачи, хранения и использования больших объемов информации; организации внедрения и использования современных цифровых технологий в правоохранительной деятельности; обеспечения информационной безопасности при работе с большими данными и др.

Лицо, принимающее решение, оказавшись в эпицентре этих процессов, просто не в состоянии осмыслить те возможности, которые предоставляют ему современные информационные технологии с точки зрения снижения затрат временных ресурсов на реализацию оптимальных алгоритмов достижения той или иной цели (улучшение показателей работы, совершенствование управления силами и средствами и т. п.). В процессе подготовки квалифицированных кадров органов внутренних дел курс лекций будет способствовать реализации стратегических направлений МВД России, направленных на совершенствование управления органами внутренних дел.

Лекция I. Правовые и организационные основы информатизации в Российской Федерации

Вопрос 1. Понятие информационных технологий в органах внутренних дел

Существуют следующие юридически значимые признаки информации, обусловившие ее как правовую категорию[1]:

– информация – это явление идеального мира, представляющее собой знания и отражение в сознании объективного мира;

– информация есть сведения о любых явлениях и процессах окружающего мира, безотносительно их содержания (в любом случае это явление будет информацией);

– информация, как благо нематериальное, способна одновременно находиться у неограниченного круга лиц. Информация при ее использовании не потребляется (не уничтожается);

– информация не обладает неразрывной связью с ее материальным носителем: она может копироваться (множиться); переводиться (словесная форма) с одного языка на другой; преобразовываться из графического вида в словесную форму выражения; из машиночитаемой формы – в форму, непосредственно воспринимаемую человеком (видео, звуковую и др.);

– информация может быть истинной (адекватно отражать явления объективной действительности) или ложной (отражать явления искаженно, неверно);

– для каждого конкретного случая социального использования определенную информацию возможно охарактеризовать как полную либо как неполную;

– информация может быть известной для широкого круга лиц или неизвестной;

– информация может иметь ограниченный доступ либо содержать сведения общего пользования;

– информация может обладать определенной социальной ценностью (личной, государственной, технической, научной, коммерческой и т. п.).

Использование информационных технологий для сбора, хранения, обработки, передачи и представления сведений стало неотъемлемой частью успешной деятельности органов внутренних (далее – ОВД). Оптимизация информационных процессов, авто-

[1] *Сакулина Л. Л.* Механизм административно-правового регулирования реализации права граждан на информацию. Ярославль: Изд-во Ярославского гос. пед. ун-та, 2012. 215 с.

матизированный анализ больших массивов информации, а также оперативный доступ сотрудников к распределенным информационным ресурсам способствует эффективному выполнению служебных обязанностей. За счет автоматизации целого ряда информационных процессов сотрудники освобождаются от рутинных, трудоемких операций и могут основное время посвятить аналитической работе, повышению профессиональных навыков и дальнейшему совершенствованию своей деятельности.

В настоящее время в органах и подразделениях МВД России активно внедряются новые технологии, обеспечивающие связь с Единой системой межведомственного электронного взаимодействия (СМЭВ). Данная система включает в себя информационные базы данных, содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа и взаимодействия с другими информационными системами и электронными ресурсами.

На современном этапе *основными задачами информатизации МВД России являются:*

– создание единого информационного пространства на основе автоматизации информационных ресурсов и перехода к безбумажной технологии, интеграции автоматизированных информационных ресурсов в банки общего пользования и обеспечения к ним удаленного доступа в режиме реального времени;

– разработка программно-технических комплексов на базе современных информационных технологий;

– обеспечение внутриведомственного и межведомственного информационного взаимодействия;

– оптимизация информационных ресурсов и надежное управление ими;

– повышение уровня информационной безопасности.

Решение поставленных задач основывается на реализации следующих принципов:

– перехода на безбумажную технологию;

– повышения полноты и достоверности информации;

– интеграции автоматизированных информационных ресурсов общего пользования на основе консолидации данных, т. е. приведения данных к единой терминологии, обеспечения их одинаковой интерпретации и точного сопоставления, что позволит обеспечить получение сведений из различных информационных ресурсов по одному запросу;

– перехода на использование отечественного свободного (открытого) программного обеспечения;

– использования лицензионного программного обеспечения.

Вопрос 2. Законодательство в сфере использования информационных технологий в органах внутренних дел

Правовое обеспечение процессов информатизации представляет совокупность нормативных правовых актов, принимаемых на различных уровнях власти и управления, регулирующих комплекс общественных отношений, связанных с созданием и использованием информации и перспективных информационных технологий[1].

Правовой основой реализации Министерством своих полномочий в установленной сфере являются Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[2], Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3], Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[4], Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[5], Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»[6], Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[7], Указ Президента Российской Федерации от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации»[8], Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[9], а также нормативные правовые акты МВД России, регулирующие вопросы развития информационных технологий, связи и защиты информации.

Во исполнение перечня поручений Президента Российской Федерации от 9 августа 2011 г. № Пр-2291 разработана Концепция создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах[10], в соответ-

---

[1] Информационные технологии в юридической деятельности: учебник / Т. М. Беляева и др.; под ред. В. Д. Элькина. Москва: Проспект, 2013. 349 с.

[2] СЗ РФ. 1995. № 33. Ст. 3349; 2016. № 28. Ст. 4558.

[3] СЗ РФ. 2006. № 31. Ст. 3448; 2018. № 52. Ст. 8101.

[4] СЗ РФ. 2006. № 31. Ст. 3451; 2018. № 1. Ст. 82.

[5] СЗ РФ. 2010. № 31. Ст. 4179; 2018. № 31. Ст. 4858.

[6] СЗ РФ. 2011. № 7. Ст. 900; 2018. № 32. Ст. 5125.

[7] СЗ РФ. 2011. № 15. Ст. 2036; 2016. № 26. Ст. 3889.

[8] СЗ РФ. 2011. № 10. Ст. 1334; 2018. № 44. Ст. 6707.

[9] СЗ РФ. 2017. № 20. Ст. 2901.

[10] «Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах» (утратил силу) [Электронный ресурс]: приказ МВД России от 30 марта 2012 г. № 205. Доступ из справ.-правовой системы «КонсультантПлюс».

ствии с которой, на базе единой информационно-телекоммуникационной системы ОВД Российской Федерации[1], создавалась единая система информационно-аналитического обеспечения деятельности МВД России.

В целях обеспечения надлежащей реализации полицейских функций, автоматизации служебной деятельности ОВД и предоставления государственных услуг, в составе ИСОД МВД России созданы и внедрены общесистемные (СЭД, СУДИС, СЭП, ВИСП, СВКС-м, Форум, АПК «Официальный интернет-сайт МВД России») и прикладные сервисы (СООП, СОМТО; ФИС ГИБДД-М, СЦУО, ЦИАДИС, СОДИ, СПГУ, СОПС, СОДЧ, СОКД, СОШП, СОДПП, СФП, Ксенон-2). Обеспечена возможность защищенного доступа к сервисам ИСОД МВД России посредством проводных, спутниковых и беспроводных каналов связи. Назначены администраторы доступа к Системе и организован процесс получения единых учетных записей пользователей ИСОД МВД России, количество которых ежегодно увеличивается.

В условиях формирования информационного общества в России конституционное закрепление информационных прав имеет большое политическое и юридическое значение.

Конституция Российской Федерации закрепляет основные, базовые положения для всех отраслей права. Она содержит основополагающие нормы и в отношении информации. В Основном законе информации посвящено несколько статей (ст. 24, 29, 42, 71). Ст. 24: «1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом». Ст. 29 гласит: «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (п. 4); «гарантируется свобода массовой информации. Цензура запрещается» (п. 5).

Конституционные положения, закрепляющие основные информационные права и свободы, развиваются и детализируются в феде-

[1] «Об утверждении новой редакции Программы МВД России “Создание единой информационно-телекоммуникационной системы органов внутренних дел”» (утратил силу) [Электронный ресурс]: приказ МВД России от 20 мая 2008 г. № 435. Доступ из справ.-правовой системы «КонсультантПлюс».

ральном законодательстве. Рассматривая уровень федеральных законов, следует выделить следующие:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий, обеспечение защиты информации);

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (регулирует отношения, связанные с обработкой государственными органами власти, юридическими и физическими лицами персональных данных, которые не составляют государственную тайну);

– Гражданский кодекс Российской Федерации (осуществляет правовое регулирование создания и использования программ для ЭВМ и баз данных: ст. 1261, 1262, 1280, 1333, 1334, 1335, 1336);

– Кодекс Российской Федерации об административных правонарушениях (закрепляет ответственность за нарушение норм в сфере обработки персональных данных: ст. 5.39, 13.11, 13.12, 13.14);

– Уголовный кодекс Российской Федерации (содержит статьи, определяющие ответственность за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети и др. – ст. 137, 140, 272, 273, 274, 284, 292, 324);

– Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне» (регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ, определяет полномочия государственных органов и должностных лиц по обеспечению сохранности и защиты государственной тайны, содержит перечень сведений, составляющих государственную тайну);

– Федеральный закон от 09 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (регулирует отношения, связанные с обеспечением доступа пользователей информацией к сведениям о деятельности государственных органов и органов местного самоуправления, определены принципы и способы обеспечения доступа к информации, формы ее предоставления, права и обязанности пользователей информации, органов власти, их должностных лиц, установлена ответственность за нарушение порядка доступа к информации).

В рамках реформирования системы МВД России, понимая необходимость и важность правового урегулирования информационных отношений, возникающих в сфере внутренних дел, впервые на законодательном уровне был закреплен порядок применения информационных технологий и осуществления процесса защиты информации в ОВД:

– Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции». Пункт 3 ст. 8 данного закона обязывает сотрудников ОМВД регулярно информировать государственные и муниципальные органы, граждан о своей деятельности через средства массовой информации, информационно-телекоммуникационную сеть Интернет. В информировании общественности большая роль принадлежит официальным сайтам территориальных органов МВД России. Разделы и рубрики ведомственных Интернет-ресурсов должны не только своевременно наполняться качественной и актуальной информацией, но и теми материалами, которые будут помогать гражданам в разрешении имеющихся вопросов;

– Указ Президента РФ от 1 марта 2011 г. № 248 «Вопросы МВД РФ» (утвердил Положение о МВД России, в котором указано, что Министерство формирует и ведет, в соответствии с законодательством Российской Федерации, федеральные учеты, базы данных оперативно-справочной, розыскной, криминалистической, статистической и иной информации, а также использует в установленном порядке федеральные учеты, базы данных в этой области других федеральных органов исполнительной власти);

– Указ Президента РФ от 9 мая 2017 г. № 203 «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»;

– Постановление Правительства РФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» (установило требования по обеспечению защиты информации, содержащейся в информационных системах общего пользования);

– Постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (утвердило Правила подготовки планов информатизации государственных органов, а также Правила проведения экспертной оценки документов, используемых в рамках планирования, создания и использования информационно-коммуникационных технологий в деятельности государственных органов);

– Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (определяет для государственных и муниципальных органов, обрабатывающих персональные данные, необходимость обязательного принятия ряда документов, обеспечивающих выполнение законодательства в области персональных данных);

– Постановление Правительства РФ от 25 апреля 2012 г. № 394 «О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов» (скорректированы акты Правительства РФ по вопросам совершенствования использования информационно-коммуникационных технологий в деятельности государственных органов);

– Постановление Правительства РФ от 6 сентября 2012 г. № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти» (принят ряд мер по совершенствованию электронного документооборота в органах государственной власти, а также установлен срок (до 31 декабря 2017 г.) перехода к электронному взаимодействию федеральных органов исполнительной власти между собой и с Правительством РФ).

– Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (пересмотрены требования по защите этих данных при их обработке в соответствующих информационных системах. За безопасность персональных данных отвечает оператор системы, который их обрабатывает, или уполномоченное им лицо. Оператор системы выбирает средства защиты информации в соответствии с нормативными актами ФСБ России и ФСТЭК России).

– Постановление Правительства РФ от 25 декабря 2014 г. № 1494 «Об утверждении правил обмена документами в электронном виде при организации информационного взаимодействия» (определило правила обмена документами в электронном виде).

Вопрос 3. Концептуальные основы создания ИСОД

ИСОД МВД России призвана повысить уровень аналитического обеспечения, которое выражается в возможности использования при принятии управленческих решений обобщенной инфор-

мации, основанной на актуальных данных. Соответственно, как один из основных пунктов, предполагается развитие интегрированной мультисервисной телекоммуникационной системы (далее – ИМТС). Именно такое название после очередного переименования получила компьютерная сеть МВД России.

Основной причиной принятия решения о создании ИСОД в МВД называется отсутствие единых архитектурных решений и системного подхода к внедрению автоматизированных систем в ведомстве, а также повышение качества информационного сопровождения повседневной и оперативно-служебной деятельности должностных лиц ОВД Российской Федерации за счет развития существующих и внедрения новых технических решений с использованием современных информационных технологий[1].

К основным целям создания ИСОД МВД России можно отнести следующие:

• решение задач автоматизации основных видов деятельности подразделений МВД России, организация централизованного хранения и обработки данных;

• эффективное выполнение государственных функций и предоставление государственных услуг за счет снижения времени и трудоемкости операций по обработке информации;

• организация единого источника информации для всех сотрудников подразделений МВД России, обеспечение электронного взаимодействия между ними, разграниченного доступа к информационным ресурсам;

• повышение 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.

В процессе создания ИСОД были в основном решены задачи автоматизации основных видов деятельности подразделений МВД, а также организации централизованного хранения и обработки данных.

Создание ИСОД призвано обеспечить:

• развитие информационно-технологической инфраструктуры подразделений МВД России;

• интеграцию информационных ресурсов МВД России на основе единых информационных банков данных;

---

[1] *Тюркин М. Л.* О концепциях Министерства внутренних дел Российской Федерации в области информатизации, связи и защиты // Оборонный комплекс РФ: состояние и перспективы развития. 2012. С. 409–412.

• создание и развитие единой информационной системы централизованной обработки данных для информационно-аналитической поддержки деятельности подразделений МВД России;

• обеспечение предоставления государственных услуг (функций) в электронном виде.

В результате создания ИСОД МВД России предполагается получение положительного эффекта по следующим целевым показателям:

• достижение требуемого уровня информационно-аналитического обеспечения деятельности МВД России;

• повышение уровня актуальности информации, выраженного в сокращении времени поступления информации из первичных источников, за счет сокращения промежуточных звеньев обработки информации и интеграции существующих разрозненных информационных систем, банков и баз данных;

• снижение финансовых затрат на техническое сопровождение и обслуживание программно-технических комплексов за счет исключения необходимости замены используемых в настоящее время морально устаревших технических средств ввиду использования технологии «облачных вычислений», способной динамически перераспределять нагрузку и обеспечивать требуемый уровень защиты, катастрофоустойчивости и доступности информации;

• повышение качества выполнения государственных функций и предоставления государственных услуг, выраженного в сокращении времени и трудоемкости операций по обработке информации, подготовке отчетов и времени ожидания выполнения запросов;

• повышение эффективности использования информационно-телекоммуникационных технологий в деятельности ОВД и оснащенности программно-техническими средствами;

• снижение трудозатрат на получение, обработку, хранение информации и доведение ее до пользователей;

• повышение уровня квалификации сотрудников ОВД в использовании современных средств информационно-телекоммуникационных технологий.

Вместе с тем до настоящего времени цели развития ИСОД не достигнуты. Имеют место факты, связанные с ненадлежащим функционированием информационных систем и сервисов. Постоянно возрастающие объемы обрабатываемой информации, высокая нагрузка на информационно-телекоммуникационную сеть передачи данных, морально устаревшее оконечное оборудование пользователей приводит к ненадлежащему функционированию информационных систем и сервисов. Отдельной проблемой остается существенная зависимость от проприетарных решений, особенно в серверной части программно-технических комплексов.

Лекция II. Информационные технологии в деятельности органов внутренних дел

Вопрос 1. Автоматизированные информационно-поисковые системы

По некоторым оценкам, общее количество различных автоматизированных информационно-поисковых систем, банков и баз данных всех уровней в системе МВД России превышает несколько тысяч наименований. Значительное число из которых разработано на рубеже 90-х гг. прошлого века, в т. ч. на базе различных инструментальных систем (FLINT) и систем программирования (Clipper, FoxPro и т. п.). Очевидно, что не все из них реально используются, а столь большое количество является следствием отсутствия действенной единой политики в вопросах информатизации. В рамках настоящей лекции будут рассмотрены наиболее типичные, масштабные системы и перспективы их дальнейшего развития.

Основные информационные ресурсы ОВД сосредоточены в информационных центрах территориальных органов МВД России на региональном уровне. К ним относятся криминалистические, розыскные и оперативно-справочные учеты, оперативные учеты, банки биометрической (дактилоскопической) и статистической информации, а также базы и банки данных архивной и научно-технической информации ОВД. В ходе реализации Программы МВД России «Создание Единой информационно-телекоммуникационной системы органов внутренних дел» уже в 2005–2007 гг. во всех информационных центрах были внедрены типовые программно-технические комплексы «Интегрированный банк данных – Регион», который объединил ранее разрозненные учеты в единую систему. Для ведения дактилоскопических учетов была внедрена автоматизированная дактилоскопическая информационная система разработки ЗАО «Папилон», а для ведения фототек – автоматизированная информационная поисковая система «СОВА» («СОВА-Опознание»). На данном этапе развития эти и другие меры позволили значительно усилить техническое оснащение ОВД. Кроме этого наметилась тенденция к развитию межведомственного и межгосударственного целевого взаимодействия в сфере информационного обмена. В то же время отдельные вопросы, связанные с построением эффективной системы информационного обеспечения, остались нерешенными.

Не в полном объеме нашли решение вопросы развития банков биометрической и оперативно-розыскной информации. Информационные ресурсы, находящиеся в территориально распределенных банках данных на районном, региональном и федеральном уровнях, до сих не интегрированы между собой. Отсутствует эффективное взаимодействие между существующими специализированными автоматизированными информационными системами, которые разработаны на различной технической, программной и информационной основе, что привело к их информационной несовместимости. Несмотря на наличие модуля поиска «Следопыт-М» для получения сведений об одном и том же объекте из разных банков данных необходимо обратиться к каждому из них. При этом требуется наличие специализированных интерфейсов каждой из автоматизированных информационных систем. Дальнейшая эксплуатация большого количества таких систем обусловливает ежегодное увеличение объемов финансирования на поддержание работоспособности и развитие информационных ресурсов, приводит к усложнению информационных потоков.

Системы дактилоскопической регистрации, основанные на традиционных ручных принципах сбора, обработки и хранения отпечатков пальцев, в настоящее время уже не способны полностью удовлетворять все возрастающие потребности правоохранительных органов. С принятием закона о дактилоскопической регистрации нагрузка на соответствующие подразделения ОВД еще более возросла, сегодня стало очевидно, что необходимо широкое внедрение автоматизированных дактилоскопических информационно-поисковых систем (АДИС). Так, в ГИАЦ МВД России ежедневно поступает несколько тысяч новых дактилокарт. Очевидно, что качественная обработка, последующее хранение и поиск в таком большом массиве без применения средств автоматизации практически невозможны.

Кроме того, накопленный массив бумажных дактилокарт подвержен старению и ветшанию вследствие частых обращений к нему в прошлом и естественных причин. По прогнозам специалистов, через несколько лет значительная часть этих карт должна была прийти в полную негодность. Эту проблему можно было решить лишь переводом информации с бумажных носителей на электронные, что и было сделано.

В связи с тем что развитие в этом направлении шло без должной централизации, в разных регионах уже использовались различные дактосистемы. К середине 2001 г. в целом по ОВД Российской Федерации было развернуто более 300 отечественных комплексов «Папилон», более 50 – «Дакто», несколько комплексов «Сонда», «Поиск», «ДактоПро» и иностранных «Морфо», «Дельта-С».

У иностранных систем были невысокие шансы занять сколь-нибудь значительный сегмент российского рынка автоматизированных дактилоскопических систем в силу их дороговизны как при приобретении (от 500 тыс. до 1 млн долл. за комплект), так и в эксплуатации (до 1 долл. за 1 дактилокарту), а также плохой адаптации к нашим условиям, необходимости обучения и совершенствования квалификации обслуживающего персонала за соответствующую оплату в валюте. Однако решающим стало наличие в России собственных разработок, превосходящих импортные аналоги по эксплуатационным показателям и приемлемых по стоимости закупки и обслуживания.

В настоящее время в мире существует не более 10–15 основных видов автоматизированных систем дактилоскопической регистрации. Одними из первых в 1970-х гг. на рынке появились комплексы Atpex (Великобритания), Printrax и Morpho (США), в начале 1980-х гг. – японская система AFIS NEC и французская AFIS MORPHO. По признанию американских специалистов, в этих системах использовались принципы, разработанные и опубликованные в открытой печати советскими специалистами еще в начале 1950-х гг. В Советском Союзе после выпуска в 1959 г. первого серийного образца «дактилоскопического автомата» на базе электронной вычислительной машины «Минск-100», разработанного институтом милиции СССР, все работы были свернуты более чем на 15 лет. Первая действующая модель и серийный образец отечественного автомата уничтожены. В США аналогичный подход был внедрен лишь во второй половине 1960-х гг., их система выставлена в Историческом музее США и именуется «первой в мире».

История возникновения АДИС связана с появлением в 1990 г. советско-индийской фирмы Совиндейта, которая позже разделилась на две (Папилон и Сонда). Приказом МВД России от 23 августа 2000 г. № 894 «Об утверждении Положения о порядке формирования и ведения Федерального автоматизированного банка данных дактилоскопической информации для раскрытия межрегиональных и серийных преступлений» (утратил силу) прямо было установлено, что указанный банк данных формируется на базе программно-технического комплекса автоматизированной дактилоскопической информационной системы, функционирующей в ГИЦ МВД России (АДИС-ГИЦ) на базе АДИС «Папилон».

С 1997–1998 гг. на базе системы «Папилон» была проведена автоматизация дактилоскопических учетов информационных центров и экспертно-криминалистического управления ГУВД по Пермской области – введен в действие первый в России комп-

лекс автоматизированной дактилоскопической информационно-поисковой системы регионального уровня с емкостью базы данных 1 млн дактилокарт и 100 тыс. следов и сетью удаленных станций автоматизированных систем и станций бескраскового дактилоскопирования. В последующие четыре года был реализован еще ряд крупных проектов автоматизации региональных дактилоскопических учетов (экспертно-криминалистических управлений и информационных центров) регионального уровня, объединяющих учеты информационных центров и экспертно-криминалистических центров с базой данных от 500 тыс. до 2,6 млн дактилокарт.

В 2002 г. по распоряжению МВД России началось создание автоматизированных дактилоскопических банков данных.

Работы по созданию федеральной АДИС-ГИЦ и межрегиональных АДИС-ФО в федеральных округах России были завершены к концу 2006 г.

С 2005 г. эти работы проводились в рамках выполнения подпрограммы по созданию объектов системы автоматизированных банков данных дактилоскопической информации программы МВД России «Создание единой информационно-телекоммуникационной системы (ЕИТКС) органов внутренних дел».

В рамках этой же программы в 2006–2007 гг. были введены в действие автоматизированные дактилоскопические информационно-поисковые системы регионального уровня (АДИС-Р) в 70 регионах России. В настоящее время все территориальные органы МВД России оснащены типовыми комплексами АДИС. Емкости баз данных региональных автоматизированных дактилоскопических систем – от сотен тысяч дактилокарт до нескольких миллионов. Вместе с тем, в настоящее время в большинстве регионов уровень заполнения база данных близок к 100 %, либо значительно превышает паспортные емкости.

К 2007 г. суммарная емкость баз данных всех комплексов автоматизированных дактилоскопических информационно-поисковых систем федерального, межрегионального и регионального уровней составила 138 млн дактилокарт, 3,8 млн следов пальцев и 700 тыс. следов ладоней. К 2012 г. скорость роста количества дактилокарт несколько замедлилась, что связано в первую очередь с завершением в большинстве регионов «залповых» вводов в систему данных с накопленных ранее традиционных бумажных носителей. По состоянию на июнь 2019 г. в базе данных ФКУ «ГИАЦ МВД России» храниться свыше 145 млн дактилокарт.

Автоматизированная дактилоскопическая информационно-поисковая система построена по модульному принципу, масштаби-

руемость ее архитектуры позволяет поэтапно наращивать как объем базы данных (от нескольких тысяч до сотен миллионов дактилокарт), так и пропускную способность. Система позволяет осуществлять обмен информацией с иностранными дактилоскопическими системами в формате ANSI/NIST (RUS-I, Interpol, EFTS, EBTS). Реализация механизма сжатия изображений для хранения и передачи посредством WSQ-алгоритмом сертифицирована в ФБР США[1].

Автоматизированная дактилоскопическая информационная система решает задачи:

– установления личности граждан по отпечаткам и следам пальцев рук и ладоней, в т. ч. путем проведения оперативных проверок личности по оттиску пальца в режиме реального времени;

– идентификации неопознанных трупов;

– установления причастности лиц к ранее совершенным преступлениям;

– объединения преступлений, совершенных одним и тем же лицом.

Использование АДИС предоставляет следующие возможности:

– ввод и хранение в базе данных дактилокарт, фотоизображений лиц и особых примет, словесного описания людей;

– ввод и хранение в базе данных следов пальцев рук и ладоней, изъятых с мест совершения преступлений;

– проведение автоматического поиска типа: «карта-карта», «карта-след», «след-карта», «след-след»;

– проведение поиска и идентификации следов пальцев рук и отпечатков ладоней;

– автоматизированный дактилоскопический учет: проведение поисковых запросов (выборок), сортировка списков базы данных, редактирование и удаление записей, и т. п.;

– поиск по словесному описанию;

– автоматизированный расчет дактилоформулы;

– вывод графических изображений (дактилокарты, фотоизображения, следы) на экран монитора и принтер, печать документов, списков, справок, статистической информации;

– удаленный ввод дактилоскопической информации, удаленный доступ к Центральной базе данных АДИС, построение распределенных систем;

– соответствие основным требованиям по многоуровневому разграничению доступа и закрытию информации, передаваемой по каналам связи и хранящейся в базе данных;

[1] АО Папилон. URL: http://papillon.ru.

– взаимодействие с другими видами автоматизированных учетов;

– экспорт дактилокарт и следов в различных форматах (Интерпол, ФБР, МВД России).

В настоящее время наиболее приоритетной задачей является интеграция разрозненных отраслевых информационных систем, баз данных и программно-технических комплексов в состав ИСОД МВД России, в т. ч. соответствующих ведомственных баз данных в единую биометрическую систему.

Заметим, что в ГИАЦ разрабатываются технические требования на создание информационной системы поиска по изображению лица в составе федеральной информационной системы биометрических учетов, с учетом накопленных массивов фотографий граждан, содержащихся в т. ч. в банках данных подразделений по вопросам миграции и Госавтоинспекции, и опыта использования системы «виодеоаналитики», разработанной на площадке Департамента информационных технологий г. Москвы.

Постоянно совершенствуется программное обеспечение различных подсистем ИБД-Ф, например, подсистемы биометрической идентификации «Опознание». Разработанное специальное программное обеспечение позволяет производить поиск по фотоизображениям лиц, содержащихся в информационных системах МВД России. При разработке программного обеспечения использованы актуальные технологии в области компьютерного зрения и работе с большими данными, эффективно решены задачи построения биометрических шаблонов, кластеризации и поиска информации.

Базовыми технологиями, лежащими в основе разработанного СПО, являются глубокие сверточные нейронные сети, а также методы математического моделирования: нейросетевые и скоринговые модели, многокритериальные методы анализа, методы поиска k-ближайших соседей в пространствах большой (более 100 измерений) размерности, теории вероятностей и математической статистики, теории принятия решений.

Высокую актуальность, эффективность и значимость разработанного СПО подтверждают факты раскрытия подразделениями центрального аппарата и территориальными органами МВД России более 60 преступлений, установления 240 лиц, причастных к противоправной деятельности, 20 преступников, находящихся в федеральном розыске, 4 без вести пропавших лиц, установления личности 5 неопознанных трупов за первые 6 мес. опытной эксплуатации СПО (январь–июнь 2020 г.).

В настоящее время планируется развертывание национальной системы биометрической идентификации личности (НС БИЛ),

которая будет состоять из двух сегментов – гражданского и правоохранительного. Гражданский сегмент реализован в виде Единой биометрической системы персональных данных (ЕБС), обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации[1]. Правоохранительный сегмент представлен Федеральной информационной системой биометрических учетов (ФИС БУ), предназначенной в т. ч. и для поиска по изображению лица, с учетом накопленных массивов фотографий граждан, содержащихся в т. ч. в банках и базах данных. Планируется, что ФИС БУ будет состоять из восьми видов учетов:

- Дактилоскопического модуля (ЦИАДИС);
- Голос;
- Изображение лица;
- Татуировки и фрагменты;
- Радужная оболочка глаза;
- Геномная (Ксенон-2);
- Поведенческие признаки;
- Русла вен.

Очевидно, что внедрение данных систем позволит значительно повысить эффективность использования оперативно-справочных (биометрических) и криминалистических учетов в решении задач по выявлению и раскрытию преступлений, расследованию уголовных дел, предупреждению и пресечению преступлений и административных правонарушений, розыска лиц и др.

Вопрос 2. Инфраструктура единого информационного пространства и Единая система информационно-аналитического обеспечения деятельности МВД России

ИСОД МВД России является прямым продолжением развития ЕИТКС ОВД и представляет собой совокупность аппаратно-программных комплексов, программно-технических средств и автоматизированных информационно-поисковых систем, а также средств и систем связи. Необходимость реализации единых технологических решений по внедрению ведомственных информационных систем в деятельность

[1] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: http://digital.gov.ru.

ОВД Российской Федерации привело к созданию ИСОД МВД России, основной целью которой является повышение уровня информационно-аналитического обеспечения деятельности МВД России. Основным индикатором является увеличение количества видов актуальной информации для обеспечения возможности оперативного поиска информации. Следовательно, исходя из теории управления, достижение данной цели выражается в возможности использования обобщенной и актуальной информации при принятии решений.

Для целей интеграции разнородных прикладных систем, обеспечения унифицированного доступа к оперативно-справочным, розыскным и криминалистическим учетам, решения задач организации документооборота с соблюдением требований безопасности информации и прав доступа пользователей к информации, на объектах ОВД устанавливаются унифицированные средства сопряжения функциональных и технологических подсистем в виде типовых программно-технических комплексов, совокупность которых образует интеграционную инфраструктуру единого информационного пространства Единой информационно-телекоммуникационной системы органов внутренних дел. Данные типовые комплексы размещаются на всех уровнях управления системы ОВД Российской Федерации.

В состав программно-технического комплекса входят следующие функциональные и технологические подсистемы:

– организации единого информационного пространства;

– организации единой системы информационной безопасности;

– организации единой системы контроля и управления функционированием;

– электронного документооборота и делопроизводства;

– интегрированная мультисервисная телекоммуникационная сеть ОВД;

– единого времени.

Программно-технические комплексы взаимодействуют между собой, используя технические возможности объектовых телекоммуникационных узлов интегрированной мультисервисной телекоммуникационной сети ОВД. В свою очередь, объекты информатизации в виде локально-вычислительной сети с автоматизированным рабочим местом пользователей и хранилищ информационных ресурсов взаимодействуют между собой только через свои объектовые программно-технические комплексы.

Кроме указанных программно-технических комплексов в составе Единой информационно-телекоммуникационной системы создается система удостоверяющих центров, представляющая собой самостоятельный инфраструктурный компонент. В состав системного удосто-

веряющего центра входят корневой, головной и подчиненные удостоверяющие центры, которые размещаются в здании центрального аппарата МВД России. В каждом регионе развернуты автоматизированные рабочие места администраторов центров регистрации системы удостоверяющих центров, предназначенные для обслуживания пользователей.

В зависимости от назначения, функциональные и технологические подсистемы Единой информационно-телекоммуникационной системы органов внутренних дел разработаны в виде типовых функциональных узлов, из которых комплектуется конкретный программно-технический комплекс для каждого объекта органа внутренних дел.

Единая информационно-телекоммуникационная система органов внутренних дел Российской Федерации. История создания Единой информационно-телекоммуникационной системы органов внутренних дел началась задолго до официального старта программы, объявленной приказом Министра внутренних дел России от 6 декабря 2004 г. № 813 «О мерах по созданию Единой информационно-телекоммуникационной системы органов внутренних дел». Попытки создания подобной системы предпринимались и ранее, однако по различным причинам они не увенчались успехом. Дополнительный импульс процессу придало принятие на федеральном уровне программы «Электронная Россия».

При внешней относительной простоте целей и задач Программы ее реализация столкнулась с рядом трудностей организационного характера. Первоначально сроком окончания создания Единой системы был определен 2008 г. Затем программа подвергалась неоднократным корректировкам согласно приказам МВД России № 813 от 6 декабря 2004 г., № 420 от 8 июня 2006 г. и № 435 от 20 мая 2008 г. В итоге приказом МВД России № 205 от 30 марта 2012 г. (приказ отменен) была утверждена Концепция создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 гг., где указано, что основой данной системы должна послужить ЕИТКС.

Несмотря на то, что программа не была официально завершена, она не только функционирует в масштабах страны, но и на ее инфраструктурной базе развернуты и действуют такие системы поддержки оперативного управления, как единая многоуровневая автоматизированная система сбора и представления информации в дежурную часть МВД России, Единая автоматизированная информационная система дежурных частей ОВД Российской Федерации и некоторые др. Осу-

ществляется обмен данными, удаленный доступ к банкам данных, работают подсистемы связи, в т. ч. и видеоконференции.

Программу начали применять на практике из-за реальной востребованности ресурсов Единой информационно-телекоммуникационной системы органов внутренних дел, хотя до официального ввода в эксплуатацию они не гарантированы и не регламентированы в полной мере. Успешному внедрению телекоммуникационных технологий способствовали ведущие регионы, реализовавшие свои программы развития сегментов Единой системы на местах (это предусматривалось программой, и регионам была предоставлена известная независимость).

Единая информационно-телекоммуникационная система органов внутренних дел представляет собой многофункциональную, иерархическую, территориально распределенную, автоматизированную информационную систему, обеспечивающую реализацию целей и задач по автоматизации процессов информационно-аналитического обеспечения оперативно-служебной деятельности ОВД (оперативно-розыскной, уголовно-процессуальной, экспертно-криминалистической и других) и административно-хозяйственной деятельности ОВД (включая тыловое, кадровое, правовое обеспечение, финансово-экономическую, административную деятельность и др.).

Основными задачами создания Единой информационно-телекоммуникационной системы органов внутренних дел являются следующие:

– реализация единого научно обоснованного подхода МВД России в области информационного обеспечения ОВД с учетом современного уровня развития информационных технологий;

– создание инфраструктуры, интегрирующей коммуникационные, информационные, сетевые и вычислительные ресурсы МВД России с целью обеспечения эффективной информационной поддержки оперативно-служебной деятельности;

– разработка единой информационной среды связи ОВД на базе единых технологий, унифицированных решений и набора типовых программно-технических средств;

– переоснащение основных информационно-вычислительных комплексов общего пользования на федеральном и региональном уровнях;

– создание и развертывание специализированных, территориально распределенных автоматизированных информационных систем по приоритетным направлениям оперативно-служебной деятельности ОВД;

– интеграция информационных ресурсов ОВД общего и специального назначения;

– обеспечение санкционированного оперативного доступа сотрудников ОВД к данным информационных систем общего и специального назначения;

– организация информационного межведомственного взаимодействия с другими правоохранительными органами на разных уровнях;

– обеспечение доступа работников ОВД к услугам публичных и специальных федеральных и ведомственных сетей передачи данных.

Для решения поставленных задач в Единой информационно-телекоммуникационной системе органов внутренних дел реализован ряд функционально-технологических подсистем, обеспечивающих:

– единую модель данных, включающую общие справочники и классификаторы;

– единую мультисервисную телекоммуникационную сеть;

– организацию единого информационного пространства;

– организацию единой системы информационной безопасности;

– автоматизацию документооборота и делопроизводства;

– организацию мониторинга и контроля функционирования всей системы.

После официального ввода в действие рассматриваемая система должна способствовать качественному изменению в лучшую сторону ситуации с информационным обеспечением как управления, так и повседневной оперативно-служебной деятельности сотрудников ОВД.

Одним из важных компонентов Единой системы, способствующих эффективности деятельности ОВД, должна стать подсистема организации электронного документооборота и делопроизводства.

Электронные документооборот и делопроизводство предназначены для автоматизации документооборота и решения задач, связанных с обработкой открытых документов, а также документов, содержащих конфиденциальную информацию всех подразделений МВД России путем обеспечения выполнения следующих функций:

– регистрации документов (входящих, исходящих, внутренних);

– хранения электронных документов;

– обеспечения процессов движения оригиналов и копий документов с формированием реестров внутренней передачи документов;

– подготовкой проектов резолюций, формированием и рассылкой резолюций;

– обеспечением процессов контроля хода исполнения резолюций;

– созданием, согласованием и подписанием с использованием электронной цифровой подписи проектов документов в электронной форме в соответствии с определенными в ОВД требованиями к делопроизводству;

– обеспечением защищенности документооборота за счет использования криптопровайдера;

– маршрутизацией и контролем движения документов, рассылкой по спискам;

– работой с взаимосвязанными документами;

– сканированием и прикреплением электронных образов документов, возможностью поточного сканирования, полнотекстового поиска по прикрепленным файлам;

– применением электронной цифровой подписи для подписания прикрепленных файлов документов;

– обменом документами на всех уровнях;

– справочно-аналитической работой, формированием отчетов;

– поиском документов по любым реквизитам (их совокупности) и тексту документа, включая контекстный поиск, поиск в базе данных архивного хранения, поиск по диапазонам дат и цифр;

– организацией передачи и хранения исполненных документов в архив подразделения с обеспечением оперативного доступа к ним, а также их отправки в ведомственный и государственный архивы.

В ходе создания и ввода в эксплуатацию информационных систем МВД России были использованы различные технические решения и аппаратно-программные платформы, для каждой системы применялось специализированное программное обеспечение. При этом основные проектно-технические решения ИСОД МВД России, в т. ч. о создании инфраструктуры единого информационного пространства и контура защиты конфиденциальной информации, не позволили создать систему, удовлетворяющую современным потребностям подразделений МВД России в информационно-аналитическом обеспечении и соответствующую тенденциям создания информационно-телекоммуникационных систем. В настоящее время ряд внешних и внутренних факторов обусловливают необходимость дальнейшего развития ИСОД МВД России.

Основными внешними факторами выступают:

– рост технического, научного и финансового потенциала преступной среды, усиление угроз терроризма, незаконной миграции;

– вступление мирового сообщества в четвертую научно-техническую революцию, основным содержанием которой является глобальное развитие информационно-телекоммуникационных систем на основе перспективных информационно-коммуникационных технологий и цифровых средств связи;

– недостаточно эффективное планирование и использование результатов фундаментальных и прикладных исследований, научно-технологических разработок в области перспективных информацион-

но-телекоммуникационных технологий, выполняемых за счет государственного бюджета;

– слабое развитие конкурентной среды в сфере проведения научно-исследовательских и опытно-конструкторских работ;

– недостаточное количество квалифицированных кадров по техническим специальностям в системе МВД России.

Основными внутренними факторами выступают:

– построение большинства сервисов ИСОД МВД России с использованием разнородных технологических решений, зачастую излишне усложненных и дорогостоящих, как при разработке, так и в процессе дальнейшей эксплуатации;

– использование практически всеми реализованными в настоящее время сервисами ИСОД МВД России локальных баз данных, содержащих рассогласованную и дублированную информацию (одну и ту же справочную информацию, имеющую разную кодификацию, а также списки физических и юридических лиц, транспортных средств и других объектов учета, совместно используемых во многих подразделениях МВД России);

– отсутствие интеграции унаследованных информационно-телекоммуникационных систем упраздненной ФМС России, а также иных ведомственных информационных систем, разработанных и введенных в эксплуатацию, с инфраструктурой ИСОД МВД России;

– отсутствие единой аппаратно-программной платформы ИСОД МВД России, обеспечивающей возможность оперативного проведения поиска и комплексного анализа накопленной разнородной информации;

– нереализованность в полной мере мероприятий по переходу на российское и (или) свободно распространяемое программное обеспечение с открытым исходным кодом, а также на использование российской микроэлектроники;

– отсутствие ведомственного документа, определяющего направления дальнейшего развития ИСОД МВД России, взамен утратившего силу приказа МВД России от 30 марта 2012 г. № 205 «Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах».

Вышеуказанные обстоятельства негативно влияют на информационно-аналитическое обеспечение деятельности подразделений МВД России, а также обусловливают избыточность ресурсов, затрачиваемых на разработку, эксплуатацию и развитие ведомственных информационно-телекоммуникационных систем, входящих и не входящих в состав ИСОД МВД России.

Вопрос 3. Программное обеспечение информационных технологий

В современных условиях информационные технологии основаны на применении разнообразного программного обеспечения. Условно прикладное программное обеспечение можно разделить на три группы: инструменты разработчика, серверные приложения и пользовательское программное обеспечение.

Инструменты разработки представлены различными средами и средствами разработки программного обеспечения, которую также иногда называют интегрированной средой разработки (ИСР). Данная группа программного обеспечения предназначена для разработки программного обеспечения и включает в себя несколько основных инструментов, таких как редактор кода, транслятор (компилятор), отладчик, а также другие средства и инструменты автоматизации различных задач (Visual Studio, Eclipse). Использование ИСР связано с традиционными языками программирования, такими как C, Pascal, Basic, а также с современными C++, Java, различные вариации PHP и других, и различными процедурными расширениями систем управления базами данных (SQL, PL/SQL). Так, приложения «толстого клиента» ИБД-Регион, эксплуатируемого в системе МВД разрабатывались при помощи процедурного расширения языка SQL (PL/SQL) на основе Oracle Forms&Reports, а модули автоматизированной информационно-справочной системы АИСС «Статистика-Регион» разработаны при помощи языка C.

Серверные приложения основаны на применении клиент-серверных технологий и основой чаще всего является web-сервера. Вкратце сущность данной технологии основана на применении специальных программ (браузеров), которые взаимодействует с сервером приложений. Ключевым отличием данной технологии является кроссплатформенность, а также то, что обработка данных происходит на стороне сервера. Чаще всего основой тонкого клиента является использование систем управления базами данных (далее – СУБД). Классическим примером использования данной технологии является уже упоминавшийся ИБД-Регион, функционирующий в схеме: клиент – браузер – «сервер приложений» – база данных. Заметим, что ИБД функционирует в двух режимах (толстого и тонкого клиентов), в первом случае для обработки данных используется формы клиента, а во втором сервер приложений. Современные сервера приложений представлены достаточно широким многообразием (Apache, Nginx, Cherokee, LightHTTPD и др.)

Наибольшее же распространение получило прикладное (пользовательское) программное обеспечение (далее – ППО), отличительной особенностью которого является ориентация на выполнение определенных пользовательских задач. ППО может быть классифицировано по типу: ППО офисного назначения – текстовые редакторы (MS Office Word, LibreOffice Writer и другие), электронные таблицы (MS Office Excel, LibreOffice Calc и др.), средства подготовки презентаций (MS Office PowerPoint, LibreOffice Impress и др.) и т. п. Кроме этого, к офисному ППО можно отнести некоторые графические редакторы (MS Paint, LibreOffice Draw и др.), а также пользовательские системы управления базами данных (ПСУБД), такие как MS Office Access, LibreOffice Base и др.

Отдельной категорией ППО являются браузеры, предназначенные для просмотра web-страниц, такие как Chrome, MS Explorer (Edge), Opera и др., которые относятся к проприетарному программному обеспечению. В классе браузеров к открытому (свободному) программному обеспечению относится Mozilla FireFox.

В отдельную группу можно вынести статистические пакеты, предназначенные для выявления явных и скрытых закономерностей в социально-экономических явлениях и процессах. Данный класс программ можно разделить на три группы: пользовательские (MS Excel, LibreOffice Calc. PSPP, Minitab), профессиональные (SPSS, Statistika, Gretl, IBM i2 Analyst's) и специализированные (Statistika Adv, SciDAVis, MATLAB, GNU Octave).

Облачные вычисления (от англ. *cloud computing*) – модель обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру. Наиболее крупнейшими игроками в сфере публично-облачных вычислений являются такие гиганты, как Amazon, Google, VMware, Microsoft.

В зависимости от типа используемой лицензии, программное обеспечение можно разделить на две категории: проприетарное (несвободное) и открытое (свободное). В первом случае в целях предотвращения использования, копирования или модификации программное обеспечение выпускается только в виде машинночитаемых двоичных файлов, таким образом ограничивается доступ к исходному коду (закрытый исходный код). Вторая группа предполагает открытый доступ к исходным текстам программ. Данные

типы программ предполагают использование GNU General Public License, т. е. лицензии на свободное программное обеспечение, по которой автор передает разработанное им программное обеспечение в общественную собственность. Заметим, что использование открытого программного обеспечения позволяет повысить уровень информационной безопасности, т. к. в программном коде отсутствуют бэкдор (от англ. *back door* – тайный ход), т. е. не декларированные (не документированные) возможности. Вместе с тем данный тип программного обеспечения также не застрахован от уязвимости «нулевого дня».

Одним из приоритетных направлений повышения эффективности информационно-аналитической работы является использования технологий искусственного интеллекта и больших данных для обеспечения деятельности МВД России. Традиционно, под технологией «Большие данные» – Big Data (далее – БД) понимаются огромные объемы структурированной и неструктурированной информации огромных объемов, которые могут быть эффективно обработаны с применением масштабируемых программных инструментов. А под технологиями искусственного интеллекта понимаются технологии, основанные на использовании искусственного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта.

Большие данные объединяют пять структурных компонентов, взаимосвязанных между собой: объем, многообразие, достоверность, ценность и скорость. Рассмотрим некоторые ключевые отличия от традиционного подхода к обработке больших объемов данных. Во-первых, технология БД предполагает единовременный анализ всего массива доступных данных, классические методы осуществляют постепенный анализ небольших пакетов данных. Во-вторых, информация анализируется в «сыром» виде, обработка же средствами СУБД предполагает, что перед анализом была произведена сортировка и первичная корректировка данных. Если при использовании средств СУБД анализ данных стартует с гипотезы и ее тестирования относительно данных, то БД осуществляют поиск корреляций по всем данным. При традиционном анализе обычно осуществляется сбор, обработка, хранение и анализ, а при использовании технологии БД обработка информации осуществляется в режиме реального времени по мере поступления данных.

Рассмотрим несколько основополагающих характеристик технологии БД в сравнении с технологией СУБД *(табл. 1)*.

Таблица 1

Сравнительные характеристики технологий

Характеристики	Базы данных	Big data
Структурированность	Структурирована	Неструктурирована или малоструктурирована
Объем	Гигабайты, терабайты	Петабайты, эксабайты
Хранилище	Централизованное	Децентрализованное
Взаимосвязь данных	Сильная	Слабая

Технология БД для обработки огромных массивов структурированной и неструктурированной информации использует следующие технологии (Machine learning, Data mining и собственно массивы необработанных данных). Machine learning – это процесс машинного обучения на основе обнаруженных связей в аналитической работе. Data mining – процесс предварительной обработки и структуризации данных с целью выявления закономерностей.

Технология БД для получения результата решает следующие задачи:

– первичная обработка, хранение и управление огромными объемами постоянно обновляющихся данных;

– структурирование разнородных данных для поиска неочевидных или скрытых связей;

– анализ и прогнозирование.

Условно говоря источники данных для БД можно разделить на две большие группы: внутренние (базы данных, транзакции, архивы, данные сотовой связи, СКУД и т. п.) и внешние (информация социальных сетей, блогов, СМИ, форумов, сайтов и т. п.).

К основным методам, используемым технологией БД, следует отнести некоторые достаточно хорошо известные (математической статистики, кластерного анализа, Data Mining, нейронные сети и др.) и перспективные (анализа социальных сетей, машинного обучения, искусственного интеллекта) методы, появившиеся относительно недавно.

Искусственный интеллект (далее – ИИ) можно разделить на две большие группы по уровню принятия решений. К слабому ИИ можно отнести различные методы и методику, направленную на решение задач сбора, обработки и хранения информации, постро-

ения аналитических и прогнозных моделей, а также обеспечение коммуникаций. Вместе с тем в настоящее время решение задачи создания сильного (универсального) ИИ еще не решена.

Выделим несколько ключевых проблем при внедрении технологии БД (ИИ) в повседневную деятельность ОВД:

1. Недостатки в обеспечении безопасности и конфиденциальность данных.

2. Низкий объем накопленных данных в ОВД, не достигающий уровня применения технологий Big Data (ИИ).

3. Высокая стоимость технологий.

4. Недостатки программного обеспечения.

5. Отсутствие высококвалифицированных специалистов в области анализа данных.

Лекция III. Аналитическое обеспечение информационных технологий

Вопрос 1. Технология анализа статистических данных

Развитие любой социальной системы-организации, в т. ч. и ОВД, происходит не изолированно, само по себе, а в тесной взаимосвязи со сложившимися условиями окружающей среды. Следует подчеркнуть, что методы анализа данных в настоящее время активно используется в самых разных сферах человеческой деятельности, в различных отраслях с целью изучения закономерностей их развития. Они также широко применяются и в управленческой деятельности, позволяя принимать обоснованные решения и делать достаточно точные прогнозы, например, динамики валового внутреннего продукта, объемов промышленного производства, динамики безработицы и т. п.

Рассмотрим типовую методику информационно-аналитической работы в ОВД. Так, различные подразделения ОВД выполняют специфические функции и задачи. Например, информационные центры территориальных органов МВД России:

– организуют обработку в территориальном органе МВД России документов первичного учета и статистической отчетности, формируют и хранят массивы статистической информации[1];

– обеспечивают выдачу (предоставляет доступ) штабу и структурным подразделениям территориального органа МВД России необходимую информацию о состоянии преступности и результатах деятельности ОВД[2];

– по запросам штаба и иных структурных подразделений территориального органа МВД России осуществляют необходимое информационное обеспечение проводимых аналитических исследований по актуальным вопросам противодействия преступности,

---

[1] О едином учете преступлений [Электронный ресурс]: приказ Генеральной прокуратуры РФ, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Типовое положение об информационном центре территориального органа внутренних дел [Электронный ресурс]: приказ МВД России от 7 декабря 2012 г. № 1088 (п. 7.4, 7.5). Доступ из справ.-правовой системы «КонсультантПлюс»; О статистической отчетности органов внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 30 декабря 2005 г. № 1170 (п. 16). Доступ из справ.-правовой системы «КонсультантПлюс».

предупреждению административных правонарушений в пределах сведений, имеющихся в информационных массивах.

Таким образом, указанные функции тесным образом пересекаются с типовыми функциями информационных центров. Заметим, что информационно-аналитическая работа более не является специфическим видом управленческой деятельности, характерным только для штабных подразделений.

Следовательно, информационно-аналитическую работу можно представить как деятельность по поиску, получению, систематизации, анализу и оценке информации о состоянии оперативной обстановки (результатах работы ОВД) с целью эффективного решения поставленных задач.

В общем случае технология (алгоритм) анализа статистических данных заключается в построении на их основе математических моделей, описывающих поведение исследуемого объекта (процесса, явления), изучении этих моделей. Разработанные математические модели используются в дальнейшем как средство поддержки принятия управленческих решений.

Более подробно *весь процесс анализа данных можно разделить на следующие этапы:*

– постановочный (на этом этапе формируется цель исследования и его основные задачи);

– априорный (проводится анализ особенностей функционирования изучаемого объекта, его характеристики, определяется набор данных, необходимых для исследования);

– информационный (собирается необходимая статистическая информация, характеризующая отобранные переменные);

– идентификации модели (на этом этапе проводится анализ качества модели статистическими методами и оценка ее параметров). Заметим, что идентификацию модели следует отличать от ее идентифицируемости, т. е. от оценки возможностей получения однозначно определенных параметров;

– верификации модели (проверяется адекватность модели и осуществляется ее корректировка).

Первые три этапа весьма важны для качественного решения задачи спецификации модели, заключающейся в представлении в математической форме выявленных характеристик объекта, связей и соотношений, обосновании количества и состава объясняющих переменных, формулировки предпосылок и ограничений модели. Спецификация опирается на имеющиеся социальные теории, специальные знания, а также на интуитивные представления исследователя об анализируемой социальной системе, процессе или явлении.

Реализация на практике представленных выше этапов сегодня не представляет значительных сложностей ввиду развития современных информационных технологий, которые максимально упростили их осуществление. Наиболее трудоемкая работа по математическому моделированию, вычислению статистических параметров, построению таблиц и графиков в основном выполняется средствами вычислительной техники, а за исследователем остается работа по постановке задачи, а также определение характеристик объекта, обоснование выбора соответствующей модели анализа данных, сбор эмпирической информации и интерпретация полученных результатов.

В общем случае, при проведении анализа данных исследователь, как правило, пользуется пространственной (панельные данные, Panel data) либо временной (временные ряды, Time series) формой их представления, или более сложными пространственно-временными формами (перекрестные данные, Cross section). Пространственные данные характеризуют значения различных показателей (факторов) в один и тот же момент или интервал времени, временные являются результатом серии наблюдений за значением одного и того же показателя в последовательные моменты времени. Пространственно-временная форма является сочетанием двух вышеперечисленных и характеризует наблюдения за набором пространственных данных в общий момент времени.

Типовая процедура анализа данных состоит из четырех этапов:

1. Первый этап постоит из четырех компонентов.

1.1. Поиск и получение информации из внутренних (сайты территориальных органов МВД России, ресурсы ЕМТС и др.) и внешних (сайты органов государственной власти в субъекте РФ, сайты Росстата и др.) источников.

1.2. Предварительный анализ факторов внешней среды, заключается в отборе факторов за счет их обобщения по группам (экономические; социальные; демографические; географические; административно-территориальные; экономического развития; культурные; правовые факторы).

1.3. Формирование предположений о статистической зависимости заключается в подборе функции, наилучшим образом описывающей развитие процесса или явления. Функции могут быть отобраны по направлению действия связи (прямые и обратные), а также по аналитическому выражению (линейная зависимость, степенная, логарифмическая, экспоненциальная и др.).

1.4. Расчет структурно-динамических параметров исследуемого вида преступности основывается на некоторых показате-

лях. Относительный показатель получается в результате деления сравниваемого показателя с базой сравнения. Различают следующие показатели: структуры и динамики. *Относительный показатель структуры* характеризует долю отдельных частей в общем объеме совокупности и рассчитывается по формуле:

$$С = \frac{\text{Показатель, характеризующий часть сопокупности}}{\text{Показатель по всей совокупности в целом}}$$

Например: известно, что количество зарегистрированных преступлений в 2018 г. составило 7 842,7 тыс., а число зарегистрированных преступлений, совершенных в общественных местах в том же году – 2 834,6 тыс., то относительная величина динамики составляет 2 834,6 / 7 842,7 = 0,36. Следовательно, структура преступлений, совершенных в общественных местах в общем количестве зарегистрированных преступлений составила 36 %.

Относительный показатель динамики характеризует изменение какого-либо явления (процесса) во времени и рассчитывается по формуле:

$$Д = \frac{\text{Текущий показатель}}{\text{Предшествующий показатель}}$$

Например: известно, что количество зарегистрированных преступлений в 2018 г. составило 7 842,7 тыс., а в 2017 – 7 203,3 тыс., то относительная величина динамики составляет 7 842,7 / 7 203,3 = 1,09. Следовательно, число преступлений выросло на 9 %.

Для характеристики развития явления (процесса) во времени рассчитываются показатели интенсивности изменений.

Абсолютный прирост (Δy) рассчитывается как разность двух уровней ряда. В случае сравнения каждого последующего уровня ряда со своим предыдущим он называется цепным:

$$\Delta y_{\text{цеп}} = y_i - y_{i-1}$$

Если в качестве базы сравнения берется один и тот же период, то прирост называется базисным:

$$\Delta y_{баз} = y_i - y_0 \ ,$$

где y_0 – период, принятый за базу сравнения.

Темп прироста (*Тпр*) показывает, насколько изменился уровень изучаемого показателя и рассчитывается как отношение абсолютного прироста к уровню динамического ряда:

$$Т_{пр\ цеп} \frac{\Delta_{цеп}}{y_i} \cdot 100$$

$$Т_{пр\ баз} \frac{\Delta_{баз}}{y_0} \cdot 100$$

Например: известно, что количество зарегистрированных преступлений в 2018 г. составило 7 842,7 тыс., а в 2017 – 7 203,3 тыс., то темп прироста составляет (7 842,7 – 7 203,3) / 7 203,3 ∗ 100= 8,87 %. Следовательно, число преступлений выросло на 9 %.

2. Второй этап включает два элемента.

2.1. Изучение отобранной и систематизированной информации.

2.2. Определение связи и влияния тех или иных факторов и условий (детерминантов) на состояние правопорядка и эффективность оперативно-служебной деятельности. На данном этапе проводится корреляционный анализ, который позволяет выявить наличие связи между объектами (процессами, явлениями), а также силу связи между объектами (процессами, явлениями). В рамках данного элемента осуществляется построение поля корреляции, его интерпретация и оценка статистической значимости коэффициента. Оценка коэффициента корреляции обычно производиться на основе шкалы Чеддока, где 0,1–0,3 – слабая связь, 0,3–0,5 – умеренная связь, 0,5–0,7 – связь заметная, 0,7–0,9 – связь высокая, 0,9–0,999 – связь очень высокая (близка к функциональной). На практике гипотеза о наличии статистической связи принимается, если коэффициент корреляции R >= 0,7 и R<= –0,7.

3. Третий этап заключается в выборе метода анализа (прогнозирования). Одним из основных направлений информационно-аналитической работы является выявление и прогнозирование тенденций и отклонений. В практической деятельности ОВД используются три основных метода анализа (прогнозирования).

3.1. Многофакторное моделирование. Данный метод более распространен в форме регрессионного анализа, который позволяет выявить характер связи между явлениями, а также построить и исследовать модель. Для нахождения неизвестных параметров модели используется метод наименьших квадратов, разработанный немецким ученым Гауссом в XVIII в. Сущность данного метода состоит в том, что подбирается теоретическая линия регрессии, которая должна пройти так, чтобы сумма квадратов отклонений от нее до каждого эмпирического значения была минимальной. Нестрого говоря, речь в данном случае идет о построении аппроксимирующей кривой, которая может иметь вид одной из функций (линейной, степенной, логарифмической и др.). Также, в рамках регрессионного метода, осуществляется отбор социально-экономических и иных факторов, корреляционный анализ и построение модели (парной, множественной) регрессии. В общем виде модель регрессии обычно представляется как:

$$y = \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n + \varepsilon \quad ,$$

где y – зависимая переменная, x – независимые переменные, β – оцениваемые параметры модели, n – количество факторов, ε – случайная компонента.

3.2. Статистическая экстраполяция динамических рядов. Данный метод относиться к технологии анализа временных рядов и в качестве основного фактора, оказывающего влияние на ряд, является время. Экстраполяция – это отличный от интерполяции метод, который заключается в распространении выводов, полученных из наблюдения над одной частью явления, на другую его часть. Типовая структура временного ряда состоит из тренда, а также сезонной, циклической и случайной компонент. В качестве теоретической модели могут применяться как линейные, так и нелинейные (полиномы, логарифмические, степенные и др.) функции.

В общем виде модель временного ряда обычно представляется как:

$$y = \beta_0 + \beta_1 t + \varepsilon \quad ,$$

где y – зависимая переменная, t – независимая переменная (номер временного ряда), β – оцениваемые параметры модели, ε – случайная компонента. Типичный вид временного ряда с основными элементами представлен на *рис. 1:*

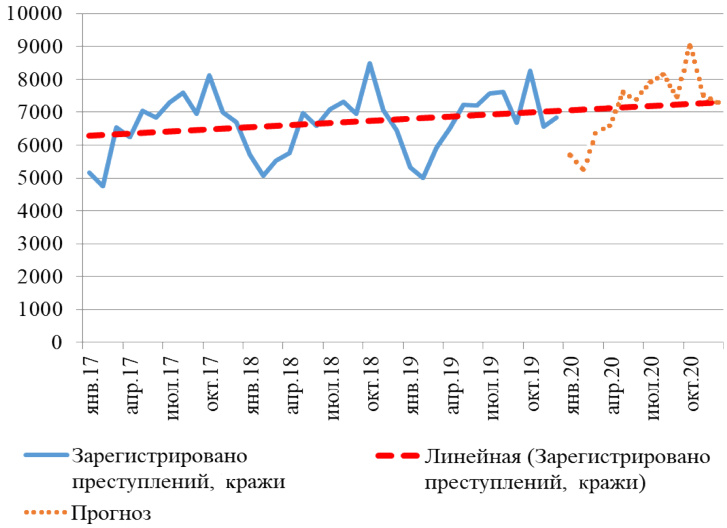

Рис. 1. **Временной ряд (кражи).**

3.3. Методы экспертного прогнозирования (в данном курсе лекций данные методы не рассматриваются).

4. На последнем этапе осуществляется формулирование выводов и оценка сложившегося положения, а также подготовка конкретных предложений, содержащих в себе варианты (альтернативы) управленческих воздействий на складывающуюся на обслуживаемой территории и объектах оперативную обстановку.

Вопрос 2. Технологии оценки результатов деятельности ОВД

Рассмотрим методику расчета оценки результатов деятельности ОВД, закрепленную в приказе МВД России от 31 декабря 2013 г. № 1040 «Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации» (далее – Приказ). Комплексная оценка складывается из вневедомственной и ведомственной, в свою очередь последняя подразделяется на статистическую оценку результатов деятельности территориального органа и экспертную оценку. Вневедомственная оценка основывается на социологических опросах, отражающих общественное мнение населения. Общая экспертная оценка формируется на основе экспертных оценок, выставленных главными инспекторами и сотрудниками центрального аппарата МВД России по материалам зонального контроля по соответствующим направлениям деятельности.

Статистическая оценка осуществляется по показателям (25 – территориальные органы по субъектам и 21 – органы на транспорте), отражающим результаты оперативно-служебной деятельности территориального органа МВД России (9 – территориальные органы по субъектам и 7 – органы на транспорте) по направлениям деятельности. Основным источником статистических данных являются агрегированные данные из документов первичного учета уголовной статистики, обобщаемые ИЦ-ГИАЦ.

Примечательно то, что нормотворец допускает разработку собственной системы оценки, либо изменение показателей, характеризующих оперативную обстановку, с сохранением подхода, изложенного в приказе. Вместе с тем изменение показателей, характеризующих общественное мнение, приказом запрещается.

Объектом оценки являются: управления на транспорте Министерства внутренних дел Российской Федерации (далее – МВД России) по федеральным округам, Восточно-Сибирское и Забайкальское линейные управления МВД России на транспорте, министерства внутренних дел по республикам, главные управления, управления МВД России по иным субъектам Российской Федерации (далее – территориальные органы МВД России).

Предметом оценки выступает эффективность выполнения основных полномочий, возложенных на ОВД и реализуемых полицией и следственными подразделениями.

Основным элементом статистической оценки является статистический показатель (далее – СП) который представляет собой относительный показатель, характеризующий качественное и количественное состояние объекта (процесса, явления). Под критерием оценки понимается наилучшее значение СП среди оцениваемых объектов оценки.

Оценочный показатель (далее – ОП) – это выраженное в баллах от 0 до 100 соотношение между СП и критерием оценки. При этом 100 баллов получает объект оценки, имеющий наилучшее (максимальное или минимальное) значение СП, а 0 баллов – объект, имеющий наихудшее (максимальное или минимальное) значение. Набранные баллы в остальных объектов оценки распределяются соответственно значениям их СП.

Для положительных СП наилучшим является максимальное его значение среди оцениваемых объектов и рассчитывается по формуле:

$$ОП_{полож} = \frac{СП - СП_{min}}{СП_{max} - СП_{min}} \cdot 100$$

Для отрицательных СП наилучшим является минимальное его значение среди оцениваемых объектов и рассчитывается по формуле:

$$ОП_{отриц} = \frac{СП_{max} - СП}{СП_{max} - СП_{min}} \cdot 100 \ ,$$

где $СП_{max}$, $СП_{min}$ – соответственно максимальное (минимальное) значение СП.

Итоговая оценка рассчитывается как средневзвешенное значение ОП и рассчитывается по формуле аддитивной свертки, и строится единый ранжир:

$$ИО = \frac{\sum_i^n K_i ОП_i}{\sum_i^n K_i} \ ,$$

где *Ki*– коэффициенты значимости (являются отражением функции предпочтения ЛПР и принимают значение от 1 до 10), ОП*i* – оценочные показатели, n – количество оценочных показателей. Для расчета итоговой оценки с равнозначными показателями, либо при отсутствии коэффициента значимости применяется формула .

$$ИО = \frac{\sum_i^n ОП_i}{n}$$

Экспертная оценка выставляется по двухбалльной шкале («удовлетворительно» или «неудовлетворительно») сотрудниками центрального аппарата МВД России.

Таким образом, все оцениваемые статистические показатели делятся на две категории: положительные (характеризующие позитивный достигнутый результат) и отрицательные (характеризующие количественную сторону негативных явлений).

Для свертывания оценочных показателей используется вычисление их средневзвешенного значения, т. е. система оценки предусматривает коэффициенты значимости (веса), присвоенные всем показателям, и отражающие то, в какой мере каждый отдельный показатель влияет на итоговую оценку.

Существуют два вида оценочных показателей, характеризующие состояние ($ОП_с$) и динамику ($ОП_д$) относительного показателя, рас-

чет которого осуществляется по формулам, указанным выше. Средневзвешенное значение состояние ($ОП_с$) и динамику ($ОП_д$) определяется по формуле:

$$ОП = 0{,}8 \cdot ОП_с + 0{,}2 \cdot ОП_д$$

Итоговая ведомственная оценка рассчитывается как среднеарифметическое значение итоговой статистической оценки и итоговой экспертной оценки.

Комплексная оценка деятельности (КОД) определяется как средневзвешенная сумма итоговой ведомственной оценки (ИВО) и итоговой вневедомственной оценки (ИВВО) по формуле:

$$КОД = 0{,}8 \cdot ИВО + 0{,}2 \cdot ИВВО$$

Изложенная система оценки называется технологией минимаксного оценивания и применяется в настоящее время для оценки эффективности деятельности территориальных органов МВД России.

Основой рассмотренного подхода является технология нормирования показателей. Под нормированием понимается преобразование формальных показателей, выражаемых в различных единицах, к безразмерному виду для их сопоставления и сравнения. Обычно задача нормирования сводиться к задаче многокритериального оценивания. Как правило, задача данного типа разбивается на несколько последовательных подзадач:

1. Нормализация статистических показателей.

2. Определение критерия оценки, т. е. за счет какого критерия один объект лучше или хуже других.

3. Учет приоритетов критериев в тех случаях, когда из физического смысла ясно, что некоторые критерии имеют приоритет над другими.

В статистике часто складывается ситуация, когда максимальное или минимальное значение носит характер статистического выброса – особой точки со значением сильно отличающимся от остальных. Применительно к деятельности ОВД, появление таких точек часто может рассматриваться как эксцесс и служить причиной проведения проверки с последующей трактовкой аномального значения.

Нормальное распределение, также называемое распределением Гаусса, – это распределение вероятностей, которое играет важнейшую

роль во многих областях знаний, особенно в физике. Физическая величина подчиняется нормальному распределению, когда она подвержена влиянию огромного числа случайных помех. Ясно, что такая ситуация крайне распространена, поэтому можно сказать, что из всех распределений в природе чаще всего встречается именно нормальное распределение. Не является исключением и социальная сфера, где большинство величин стремится к нормальному распределению.

Вопрос 3. Компьютерные технологии анализа социальных сетей

Несмотря на значительные усилия правоохранительных органов по противодействию преступности, совершаемой в информационно-телекоммуникационных системах, распространение преступлений данной категории становится все шире. Столкнувшись с этой проблемой, правоохранительные органы нуждаются в надежных и эффективных методах анализа и оценки структуры и деятельности социальных сетей. Одна из ключевых задач состоит в том, чтобы идентифицировать (деанонимизировать) участника социальной сети с использованием информации о ее топологии. Данная возможность позволит правоохранительным органам сосредоточить усилия по идентификации именно на этих членах, что в условиях ограниченных материальных ресурсов является более предпочтительным.

С данной целью можно использовать некоторые классические метрики центральности из сферы анализа социальных сетей. Метрики центральности призваны дать численную характеристику значимости узла в сети. Например, IBM Analyst Notebook – это программный пакет, используемый во всем мире правоохранительными структурами, – поддерживает степень, близость и промежуточность центральности, которые, вероятно, являются наиболее широко используемыми показателями центральности. Вместе с тем эти метрики имеют некоторые ограничения, и разработка более сложных мер в настоящее время является серьезной областью исследований. Одним из важных направлений современных разработок является применение методов из области теории кооперативных игр к данной проблеме.

С позиции теории графов, социальные сети представляют собой неориентированные взвешенные графы: они состоят из набора узлов (вершин) и неориентированных ребер, соединяющих некоторые узлы, причем каждое ребро является взвешенным. При анализе сетей узлы интерпретируются как участники сообщества, ребра указывают на связи между ними, а веса указывают на силу связи

(например, количество контактов между двумя людьми). Анализ центральности направлен на создание принципиального ранжирования важности узлов в такой сети. Поскольку «важность» зависит от рассматриваемой проблемы, существуют множество различных метрик центральности, среди которых наиболее распространенными являются центральность по степени, центральность по близости и центральность по промежуточности. Согласно взвешенной степени центральности, важность узла равна весу смежных ребер этого узла (т. е. взвешенной степени узла).

Анализ социальных сетей – это относительно новое научное направление, оформившееся самостоятельно как практическое преломление отдельных элементов теории графов, комбинаторики и теории игр. Как следует из наименования, анализ социальных сетей решает задачи, связанные построением выводов и умозаключений относительно социальных сетей, основываясь на структуре этих сетей.

Социальная сеть рассматривается как граф, вершины графа – это социальные объекты, ребра между вершинами – связи между ними[1]. В зависимости от рассматриваемой социально-сетевой модели и задач анализа, в качестве вершин графа могут выступать отдельные люди, коллективы людей, формальные и неформальные организации. От характера социальных объектов зависит и природа связей. Связи между людьми и коллективами могут выражаться любыми социальными и экономическими взаимодействиями: вместе учились, состоят в браке, один занял деньги у другого, приходил в гости, созванивались по телефону и т. д. В современном обществе все большую популярность приобретают сервисы Интернета, позволяющие осуществлять отдельные социальные взаимодействия в виртуальном пространстве, – именно такие сервисы в бытовом понимании сегодня и принято называть социальными сетями. Здесь во избежание путаницы в терминах будем называть их онлайновыми социальными сетями, как подвид социальных сетей в широком смысле.

Центральность вершины в графе – ключевое понятие в анализе социальных сетей. Центральность вершины позволяет на основе топологии графа определить, насколько данная вершина важнее других вершин в некотором смысле. К настоящему времени предложена масса метрик центральности, таких как: центральность по степени, центральность по близости, центральность по промежуточности, собственный вектор и многие другие, каждая из которых

[1] *Торопов Б. А.* Центральность распада в социальных графах и адаптированный алгоритм Флажоле-Мартена для ее расчета // International Journal of Open Information Technologies. 2017. Т. 5. № 9. С. 27–33.

позволяет оценить важность вершины в графе по сравнению с другими вершинами. Будучи рассчитанной для каждой вершины социального графа, любая метрика центральности позволяет определить К наиболее значимых вершин.

Для небольших сообществ, рассматриваемых герметично, в изоляции от внешнего мира, скорее всего, будет наиболее важна центральность по степени (числу прямых контактов с остальными участниками).

Центральность по близости зачастую рассматривается как метрика, показывающая, насколько быстро информация распространится по сети, если инициатором распространения будет заданная вершина.

Центральность по промежуточности (от англ. *betweenness* – промежуточность) характеризует посредническую силу вершины. Она показывает, насколько часто вершина v оказывается на кратчайшем пути между всеми возможными парами вершин графа.

При решении некоторых практических задач «традиционные» метрики центральности (отнесем к ним степень, близость и промежуточность) показывают несостоятельность отразить реальные социальные сети и происходящие в них процессы, а наиболее подходящими оказываются более изощренные характеристики участников сети, такие как, например, собственный вектор.

В контексте изучения сетей различной природы (от электрических и транспортных до социальных, и даже до сетей, образуемых белковыми соединениями) зачастую встает задача определения наиболее важных элементов из числа тех, что образуют сеть. Например, в транспортной сети нужно найти наиболее важную дорогу, в социальной сети – наиболее важных людей и т. п. Различные метрики центральности служат для количественной оценки важности вершин, и традиционные метрики, в т. ч. рассмотренные выше, сегодня достаточно широко изучены. Результат расчета метрики центральности для графа заключается в присвоении каждой его вершине количественной характеристики, коррелирующей с важностью этой вершины в контексте решаемой научной или прикладной задачи.

Вектор Шепли, вероятно, является наиболее важной формализованной концепцией решения коалиционных игр. В любой ситуации, когда агенты, действуя коллективно, достигают общей цели, вектор Шепли предлагает справедливую схему раздела выигрыша либо справедливые доли, в которых агенты несут издержки, в зависимости от рассматриваемой ситуации.

Одно из относительно новых направлений применения вектора Шепли находится в плоскости анализа социальных сетей. А именно, данная концепция позволяет рассчитывать центральности вершин в графах, являющихся моделями социальных сетей различной природы.

Следует отметить, что разработка эффективных алгоритмов расчета ТИЦ является актуальным научно-практическим направлением. Чрезвычайно высокая гибкость и универсальность данного механизма подразумевает наличие огромного количества форм ТИЦ, различающихся тем, какие именно характеристики вершин изучаемого социального графа важны для формируемой коалиции. То есть ТИЦ может учитывать в любых пропорциях любой набор традиционных метрик центральности вершин (под ними будем иметь в виду степень, близость, промежуточность, рассмотренные выше), которые опираются на положение вершин в графе, совместно с любым набором как качественных, так и количественных характеристик, присущих этим вершинам вне зависимости от положения в графе.

В контексте рассмотрения процессов распространения информации в онлайновых сервисах Интернета наибольший интерес представляет метрика центральности по близости (или просто близость). Рассмотрим данную традиционную метрику центральности, а также ее теоретико-игровое преломление на основе вектора Шепли.

Проблема идентификации участников социальных сетей является важной проблемой в научной литературе, которая вызывает значительный интерес в сообществе аналитиков. Решение этой проблемы требует определения метрики центральности, которая должна учитывать характеристики каждого участника, уметь определять синергию в различных подсетях и объединять всю эту информацию в согласованный рейтинг. В последнее время было предложено достаточно много различных метрик центральности на основе теории кооперативных игр, и тем самым предоставлен богатый набор вариантов решений для оценки социальных сетей. К сожалению, эти новые метрики сложны и вызывают сложные вычислительные проблемы даже для относительно небольших сетей.

Лекция IV. Правовые основы защиты информации в Российской Федерации. Государственная система защиты информации

Вопрос 1. Понятие защиты информации. Актуальность изучения вопросов обеспечения защиты информации в ОВД

Одним из важнейших направлений обеспечения защиты информации является дальнейшее развитие сбалансированной системы правовых норм и механизмов, направленных на противодействие и нейтрализацию угроз как государственным интересам России в этой сфере, так и органам внутренних дел.

В Конституции Российской Федерации[1] провозглашены информационные права и свободы граждан нашей страны. Однако декларация информационных прав и свобод не означает отказ государства от защиты информационных ресурсов. Правовое обеспечение информационной безопасности формируется на основе поддержания баланса интересов граждан, общества, государства, что особенно важно в условиях существования различных форм собственности.

Законодатель закрепил право каждого гражданина на сокрытие определенных сведений – право на тайну. В Конституции Российской Федерации имеются определенные ограничения, направленные на регламентацию распространения и использования информации. Информационные права и свободы не должны быть использованы для разглашения сведений, составляющих государственную тайну (ч. 4 ст. 29).

Конституцией определены основания для ограничения информационных прав и свобод граждан. Это – защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны страны и безопасности государства (ч. 3 ст. 17, ч. 3 ст. 55). Основным Законом также предусмотрена возможность ограничения прав и свобод в условиях чрезвычайного положения с указанием пределов и сроков их действия (ст. 56).

[1] Конституция Российской Федерации: с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ: принята всенародным голосованием 12 декабря 1993 г. // СЗ РФ. 2009. № 4. Ст. 445.

С учетом международных договоренностей России, основными источниками права в сфере информационных отношений и защиты информации являются международные конвенции и законодательные акты.

Так, гарантии невмешательства в личную жизнь граждан, с одной стороны, и соблюдение законности в случае необходимости обоснованного вмешательства – с другой, развиваются в Кодексе поведения должностных лиц по поддержанию правопорядка. В этом международном документе, принятом Резолюцией Генеральной Ассамблеи ООН № 34/169 от 17 декабря 1975 г. в ст. 4 указывается, что «сведения конфиденциального характера, получаемые должностными лицами по поддержанию правопорядка, сохраняются в тайне, если исполнение обязанностей или требования правосудия не требуют иного»[1].

Приведем еще один международный документ, который рекомендован руководству различных государств для реализации в национальных законодательствах. Генеральной Ассамблеей ООН были приняты Руководящие принципы в области предупреждения преступности и уголовного правосудия (приняты VII Конгрессом ООН по предупреждению преступности и обращению с правонарушителями).

В ст. 34 Руководящих принципов отмечается, что «ввиду возможности накопления в электронно-вычислительных системах данных на различных лиц, которые могут быть использованы для нарушения прав человека, включая право на охрану личной жизни, или для других злоупотреблений, необходимо предусмотреть соответствующие гарантии, обеспечить конфиденциальность, создать систему индивидуального доступа к таким данным и коррективных мер, а также процедуры изъятия таких данных в целях разрешения этих и других дискриминационных проблем, возникающих в связи с возможным злоупотреблением ими»[2].

Приведенные выше международные документы свидетельствуют об осознании важности не только стремительно развивающихся информационных технологий, но и проблемах, возникающих при их повсеместном использовании. Такой проблемой, прежде всего, является защита информационных ресурсов.

---

[1] Кодекс поведения должностных лиц по поддержанию правопорядка // Международные соглашения и рекомендации ООН в области защиты прав человека. Москва: Академия МВД СССР, 1969. С. 134.

[2] Руководящие принципы в области предупреждения преступности и уголовного правосудия // Международные соглашения и рекомендации ООН в области защиты прав человека. Москва: Академия МВД СССР. 1969, С. 160–161.

Актуальность проблем управления информационной сферой современного постиндустриального информационного общества обусловливается целым рядом специфических черт и особенностей.

Во-первых, информация, в процессе производства и распространения которой занято большинство экономически активного населения, стала товаром. Причем товаром массового производства и потребления, но товаром весьма специфическим.

Во-вторых, массовый характер производства и потребления информации требует разработки методов безопасного обращения с ней подобно тому, как массовое участие людей в процессе переработки вещества и энергии требовало массового образования в области безопасных методов труда.

В-третьих, повышенные требования к обеспечению информационной безопасности предъявляет нынешний уровень и темпы технического прогресса. За последние десятилетия количество физических процессов и объектов, использующих информационные технологии, многократно увеличилось. И появление в информационной сфере каждого нового технического и технологического процесса вызывает новые специфические требования к защите информации.

Доктрина информационной безопасности Российской Федерации[1] определяет информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[2].

Конфиденциальность – свойство информационных ресурсов, в т. ч. информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

Целостность – неизменность информации в процессе ее передачи или хранения.

Доступность – свойство информационных ресурсов, в т. ч. информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Информационная безопасность (от англ. *information security*) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуе-

[1] Доктрина информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

[2] *Там же.*

мости, подотчетности, аутентичности и достоверности информации или средств ее обработки[1].

Мы видим, что в трех представленных определениях объекты защиты представлены по-разному.

Ведомственный нормативный правовой акт информационную безопасность ОВД рассматривает как состояние защищенности информации, информационных ресурсов и информационных систем ОВД, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования[2].

Оба представленных направления тесно связаны вместе с собой, используемы средства и методы в целях защиты информации и информационных систем во многом схожи или используют одни и те же принципы защиты.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность[3].

С данным понятием тесно связано понятие «защита информации». В национальном стандарте Российской Федерации ГОСТ Р 50922-2006[4] *защита информации* определяется как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

На наш взгляд, более емкое определение дано в Федеральном законе № 149-ФЗ[5]. Под защитой информации следует понимать принятие правовых, организационных и технических мер, направленных на достижение следующих целей:

– обеспечение зашиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

---

[1] ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Москва: Стандартинформ, 2007.

[2] Концепция обеспечения информационной безопасности ОВД РФ до 2020 года: приказ МВД России от 14 марта 2012 г. № 169 // опубликован не был.

[3] ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»: приказ Ростехрегулирования от 27 декабря 2006 г. № 373-ст. Москва: Стандартинформ, 2008.

[4] *Там же*.

[5] Об информации, информационных технологиях и о защите информации: федер. закон РФ от 27 июля 2006 г. № 149-ФЗ. Ст. 2 // СЗ РФ. 2006. № 31. Ч. 1. Ст. 3448.

– соблюдение конфиденциальности информации ограниченного доступа;

– реализация права на доступ к информации.

К рассмотрению вопросов об актуальности изучения вопросов, связанных с обеспечением информационной безопасности и защиты информации в ОВД подойдем с позиции рассмотрения требований нормативных правовых актов к организации данного процесса в органах государственной власти. Проанализируем требования закона РФ «О государственной тайне».

Защита государственной тайны является видом основной деятельности органа государственной власти.

Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Таким образом, рассматривая данную тему, мы изучаем правовые вопросы организации одного из основных направлений деятельности территориального органа и организации МВД России.

Кроме этого, необходимо обратить внимание на тот факт, что *территориальный орган МВД России на региональном уровне* обеспечивает ведение и функционирование информационных систем, в т. ч. банков данных, достоверность, актуальность содержащейся в них информации и ее защиту от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и (или) распространения. К тому же, он обеспечивает защиту сведений, составляющих государственную и иную охраняемую законом тайну, в территориальном органе, подчиненных органах и организациях[1].

Территориальный орган МВД России на районном уровне обеспечивает защиту сведений, составляющих государственную и иную охраняемую законом тайну, и осуществление мероприятий по технической защите информации[2].

Законодатель предъявляет требования в этой области и к сотрудникам ОВД. Так, к их обязанностям относится следующее:

---

[1] Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации: Указ Президента РФ от 21 декабря 2016 г. № 699 // СЗ РФ. 2016. № 52. Ч. V. Ст. 7614.

[2] Об утверждении Типового положения о территориальном органе Министерства внутренних дел Российской Федерации на районном уровне: приказ МВД России от 21 апреля 2011 г. № 222 // Бюллетень нормативных актов федеральных органов исполнительной власти. № 28. 2011.

– обязанность не разглашать сведения, составляющие государственную и иную охраняемую законом тайну, а также сведения, ставшие ему известными в связи с выполнением служебных обязанностей (сведений, касающихся частной жизни и здоровья граждан или затрагивающих их честь и достоинство)[1].

В случае если сотрудник (работник) допускает однократное нарушение им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны, то допуск такого лица к государственной тайне может быть прекращен, что является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в трудовом договоре (контракте)[2].

Все вышесказанное, на наш взгляд, обуславливает актуальность изучения вопросов, связанных с обеспечением информационной безопасности в целом и защиты информации в частности ОВД.

Вопрос 2. Правовые основы защиты информации в Российской Федерации

Одним из важнейших направлений обеспечения защиты информации является дальнейшее развитие сбалансированной системы правовых норм и механизмов, направленных на противодействие и нейтрализацию угроз как государственным интересам России в этой сфере, так и ОВД.

Объектом правового регулирования в области защиты информации являются отношения между органами законодательной, исполнительной и судебной власти, органами местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о защите информации по поводу реализации своих прав и обязанностей относительно предметов правовых отношений.

Предметом правовых отношений в области защиты информации являются информация и формируемые на ее основе информа-

[1] О полиции: федер. закон РФ от 7 февраля 2011 г. № 3-ФЗ (п. 8, ч. 1, ст. 27) // СЗ РФ. 2011. № 7. Ст. 900; О службе в органах внутренних дел РФ и внесении изменений в отдельные законодательные акты РФ: федер. закон РФ от 30 ноября 2011 г. № 342-ФЗ (п. 7, ч.1, ст. 12) // СЗ РФ. 2011. № 49. Ч. 1. Ст. 7020.

[2] О государственной тайне: Закон РФ от 21 июля 1993 г. № 5485-1 (ст. 23) // СЗ РФ. 1997. № 41. Стр. 8220–8235.

ционные ресурсы (прежде всего ограниченного доступа), информационные технологии и средства обработки информации.

Государственное регулирование отношений в данной сфере осуществляется путем установления требований о защите информации и установлении ответственности за нарушение законодательства Российской Федерации о защите информации.

Оператор, Министерство внутренних дел Российской Федерации обязано обеспечивать защиту всей информации, которая обрабатывается в информационных системах и содержащейся в базах данных.

С точки зрения обеспечения безопасности информации, важным является классификация информации, в зависимости от категории доступа к ней. В соответствии с федеральным законом, информация делится на общедоступную и информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). Ограничение доступа к информации устанавливается Конституцией Российской Федерации и Федеральными законами. В свою очередь информация ограниченного доступа делится на два вида: сведения, составляющую государственную тайну («секретно», «совершенно секретно», «особой важности») и конфиденциальную информацию.

В России занятие отдельными видами деятельности требует лицензирования, т. е. ими разрешено заниматься только после предварительного получения разрешения от властей – лицензии.

В области защиты информации к законодательным актам, регулирующим процедуру лицензирования, относятся: Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» и Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», а также ряд постановлений Правительства Российской Федерации. Законами устанавливаются общие принципы и назначается государственный орган, уполномоченный выдавать лицензии. Порядок выдачи лицензий определяется подзаконными актами.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны осуществляется путем получения ими лицензий на проведение работ со сведениями соответствующей степени секретности[1].

[1] О государственной тайне: Закон РФ от 21 июля 1993 г. № 5485-1 // СЗ РФ. 1997. № 41. Стр. 8220–8235.

Порядок получения лицензий устанавливается Правительством Российской Федерации. Допуск организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, осуществляют органы, определенные Правительством Российской Федерации. К ним относятся ФСБ России и ее территориальные органы (на территории Российской Федерации) и СВР России (за рубежом).

Лицензирование деятельности организаций на право проведения работ, связанных с созданием средств защиты информации, осуществляет ФСТЭК России, СВР России, Минобороны России и ФСБ России (в пределах их компетенции).

На право осуществления мероприятий и оказания услуг в области защиты государственной тайны лицензирование осуществляет ФСБ России и ее территориальные органы, ФСТЭК России и СВР России (в пределах их компетенции)[1].

Вопросы установления обязательных технических норм и правил подтверждения соответствия продукции, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, работ, услуг или иных объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров, стандартизации, государственного контроля (надзора) за соблюдением требований технических регламентов и т. д. регламентируются Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». В данном законе[2] определены особенности технического регулирования в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа. В отношении указанной продукции (работ, услуг), а также, соответственно, процессов обязательными требованиями, наряду с требованиями технических регламентов, являются требования, установленные:

---

[1] О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны: постановление Правительства РФ от 15 апреля 1995 г. № 333 // СЗ РФ. 1995. № 17. Ст. 1540.

[2] О техническом регулировании: федер. закон РФ от 27 декабря 2002 г. № 184-ФЗ // СЗ РФ. 2002. № 52. Ч. 1. Ст. 5140.

– государственными заказчиками;

– федеральными органами исполнительной власти – ФСБ России[1], Минобороны России[2], СВР России[3], ФСТЭК России[4];

– государственными контрактами (договорами).

Перечисленные федеральные органы исполнительной власти соответственно их компетенции наделены полномочиями по разработке и установлению своими нормативными правовыми актами и технической документацией обязательных требований в области технического регулирования продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа.

Сертификация продукции (средств защиты информации), используемой в целях защиты сведений, составляющих государственную тайну. В Российской Федерации средства защиты информации подлежат обязательному подтверждению соответствия в форме обязательной сертификации (система сертификации СЗИ-ГТ). Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Обязательная сертификация в системе сертификации СЗИ-ГТ проводится на основании требований законодательства Российской Федерации[5].

Сертификация осуществляется на основании требований государственных стандартов и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Организация сертификации средств защиты информации возлагается на ФСТЭК России, ФСБ России и МО России в соответствии с функциями, возложенными на них законодательством. С целью организации сертификации средств защиты информации указанные органы, являясь федеральными органами по сертификации, создают свои системы сертификации.

---

[1] Вопросы федеральной службы безопасности Российской Федерации: Указ Президента РФ от 11 августа 2003 г. № 960 // СЗ РФ. 2003. № 33. Ст. 3254.

[2] Вопросы Министерства обороны Российской Федерации: Указ Президента РФ от 16 августа 2004 г. № 1082 // СЗ РФ. 2004. № 34. Ст. 3538.

[3] О внешней разведке: федер. закон РФ от 10 января 1996 г. № 5-ФЗ // СЗ РФ. 1996. № 3. Ст. 143.

[4] Вопросы Федеральной службы по техническому и экспортному контролю: Указ Президента РФ от 16 августа 2004 г. № 1085 // СЗ РФ. 2004. № 34. Ст. 3541.

[5] О государственной тайне: Закон РФ от 21 июля 1993 г. № 5485-1 // СЗ РФ. 1997. № 41.

Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. Срок действия сертификата не может превышать пяти лет.

В Госстандарте России зарегистрирована «Система сертификации средств криптографической защиты информации РОСС. RU.0001.030001.», а также «Система сертификации средств защиты информации по требованиям безопасности информации РОСС. RU.0001.01БИ00».

Данные документы определили организационную структуру системы сертификации шифровальных средств и средств защиты информации, а также установили основные правила проведения сертификационных исследований и испытаний данных средств защиты информации.

Перечень средств защиты информации, подлежащих сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации (РОСС.RU.0001.01БИ00), а также виды средств защиты информации, подлежащие сертификации в системе сертификации СЗИ-ГТ, определены в нормативных правовых актах ФСТЭК России и ФСБ России соответственно.

Лекция V. Основы технической защиты информации

Вопрос 1. Технические каналы утечки информации

Повышенные требования к обеспечению информационной безопасности предъявляет нынешний уровень и темпы технического прогресса. За последние годы количество физических процессов и объектов, используемых информационными технологиями, многократно увеличилось. И появление в информационной сфере каждого нового технического и технологического процесса вызывает новые специфические требования к защите информации.

Под защитой информации в соответствии с Федеральным законом № 149-ФЗ[1] понимается принятие правовых, организационных и технических мер, направленных:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– на соблюдение конфиденциальности информации ограниченного доступа;

– на реализацию права на доступ к информации.

Под техническим каналом утечки информации принято понимать систему, в состав которой входят:

1) объект разведки;

2) техническое средство, используемое для несанкционированного получения сведений;

3) физическая среда, в которой распространяется информационный сигнал.

Объектом разведки могут быть помещение, группа помещений или здание с хранящимися материалами ограниченного пользования, технические каналы связи, используемые для передачи сведений, отнесенных к различным видам тайн.

Физической средой, в которой распространяются информационные сигналы, могут быть строительные конструкции зданий и сооружений, токопроводящие линии, среда распространения акустических (речевых) сигналов, электромагнитные поля.

---

[1] Об информации, информационных технологиях и защите информации: федер. закон РФ от 27 июля 2006 г. № 149-ФЗ (в ред. от 21 июля 2014 г.) // СЗ РФ. 2006. № 31. Ч. 1. Ст. 3448.

Средой распространения информации являются также технические средства обработки информации (далее – ТСОИ), находящиеся в помещении, – средства вычислительной техники, автоматические телефонные станции, системы звукозаписи.

Классификация технических каналов утечки информации

Выделим следующие группы основных технических каналов утечки информации:

1) электромагнитные;
2) электрические;
3) каналы утечки видовой информации;
4) каналы утечки акустической (речевой) информации.

Заметим, что это неполный перечень всех возможных технических каналов утечки информации и методов ее несанкционированного перехвата.

Электромагнитные каналы утечки информации. Вся работающая электронная аппаратура и электронные системы, на какой бы технической базе они ни создавались, от телефонного аппарата до современных компьютерных систем, от релейно-контактных и электронно-вакуумных модулей до сверхбольших интегральных схем и проводных коммуникаций создают электромагнитные поля, называемые побочными электромагнитными излучениями. Они способны создавать электромагнитные наводки в расположенных рядом слаботочных, силовых и осветительных сетях, линиях и аппаратуре охранно-пожарной сигнализации, проводных линиях связи, различных приемниках электромагнитных излучений.

В результате таких процессов возникают каналы утечки информационных сигналов, т. к. электромагнитное поле, создаваемое работающей аппаратурой, является носителем обрабатываемой или передаваемой информации. Специальные широкополосные приемники позволяют «считывать» электромагнитные излучения, а затем восстанавливать и отображать содержащуюся в них информационную составляющую.

Электрические каналы утечки информации возникают за счет:

– наводок электромагнитных излучений ТСОИ на коммутационные линии вспомогательных технических систем и средств (далее – ВТСС);

– утечек информационных сигналов в цепях электропитания ТСОИ;

– утечек информационных сигналов в цепь заземления ТСОИ.

Например, побочные электромагнитные поля работающих компьютеров производят наводки на близко расположенные коммутационные линии ВТСС (охранно-пожарная сигнализация, телефонные

провода, сети электропитания, металлические трубопроводы). Наводимая в них ЭДС существенна и распознаваема на частотах от десятков кГц до десятков мГц. В этом случае возможен съем информации путем подключения специальной аппаратуры к коммуникационным линиям за пределами контролируемой территории.

Каналы утечки видовой информации. Несанкционированное получение видовой или, как ее иногда называют, графической информации осуществляют путем наблюдения за объектом, представляющим оперативный интерес. Различных видов технических средств, используемых для этих целей, достаточно много – это бинокли, приборы ночного видения, фото- и видеотехника, и др.

Каналы утечки акустической (речевой) информации. Наиболее распространенным способом несанкционированного доступа к информации является перехват акустической (речевой) информации. Каналы утечки акустической (речевой) информации принято классифицировать следующим образом:

- электроакустический;
- виброакустический;
- оптико-электронный;
- акустический;
- проводной;
- электромагнитный.

Электроакустический канал утечки информации. Ряд элементов ВТСС, прежде всего, громкоговорители трансляционной сети, звонки телефонных аппаратов меняют свои электрические параметры (емкость, индуктивность, сопротивление) под действием акустического сигнала. Изменение названных параметров вызывает модуляцию информационным сигналом токов, протекающих в элементах ВТСС. Такие электроакустические преобразования получили название «микрофонного эффекта».

С точки зрения безопасности, телефонный аппарат имеет существенный недостаток, поскольку его основные узлы (микрофон, мембрана, звонковая цепь) могут выполнять функции приемника и передатчика сигналов при несанкционированном прослушивании помещения, в котором он установлен. Звонковая цепь телефонного аппарата при положенной на рычаг трубке обладает «микрофонным эффектом». Подвижные части звонка вибрируют под действием речевых сигналов (разговор в помещении), что приводит к появлению в нем электрического тока малой амплитуды. Это, в свою очередь, позволяет провести соответствующую обработку возникающего в цепи сигнала и выделить звуковую составляющую за пределами контролируемого помещения.

Виброакустический канал несанкционированного снятия информации из контролируемых помещений. Происходит снятие результатов воздействия акустических речевых сигналов на строительные конструкции и сооружения (панели перегородок стен, пол, потолок, воздуховоды, вентиляционные шахты, трубы и батареи отопления, оконные стекла и т. д.). Под воздействием акустических волн строительные конструкции подвергаются микродеформации, в результате которой возникают упругие механические колебания, хорошо передающиеся в твердых однородных средах. Эти колебания воздействуют на чувствительный элемент электронного стетоскопа (вибродатчик) и преобразуются в электрический сигнал, который затем усиливается и может быть передан по проводным, оптическим или радиоканалам связи.

Оптико-электронный канал утечки информации. Акустический контроль удаленных помещений, имеющих окна, может быть осуществлен с использованием оптико-электронных или, как их нередко называют, лазерных систем (лазерных микрофонов).

Современные лазерные системы позволяют осуществлять прослушивание разговоров, ведущихся в помещении, на расстоянии от 100 м до 1 км. Дальность действия во многом зависит от качества оконного стекла (величины микронеровностей), а также от степени его загрязненности и состояния атмосферной среды (от метеоусловий, задымленности и др.). С улучшением отражающей поверхности увеличивается дальность действия. Для этого применяются следующие приемы: стекло покрывается специальным материалом либо на нем наклеиваются небольшие отражатели. Для отражения лазерного луча могут быть также использованы элементы интерьера и мебели – стеклянные поверхности и зеркала внутри помещения.

*Акустический канал утечки информации***.** Самым простым способом перехвата речевой информации, не требующим использования специальной техники, является подслушивание ведущихся разговоров. Неплотно прикрытая дверь в кабинет должностного лица, обсуждение сведений ограниченного распространения в курительной комнате или за пределами служебных помещений, конфиденциальное совещание, проводимое в помещении с открытыми окнами, – вот те простые, но вместе с тем вполне реальные каналы утечки информации.

*Проводные каналы утечки акустической (речевой) информации***.** В зданиях и сооружениях акустические каналы возникают как за счет имеющихся воздуховодов, вентиляционных шахт, некачественного строительства, так и за счет специально сделанных отверстий в потолках, стенах, полах.

В этом случае для снятия акустической информации могут быть использованы проводные микрофоны, которые через линии связи подключаются к звукоусилительной и звукозаписывающей аппаратуре. В открытой периодике упоминается система акустического мониторинга с передачей команд управления и информации от нескольких микрофонных и телефонных входов по одной двухпроводной физической линии.

Электромагнитные каналы утечки акустической (речевой) информации. Наряду с направленными микрофонами, диктофонами и лазерными системами, для несанкционированного съема речевой информации широко используются скрытно установленные акустические закладные устройства или, как их кратко называют, радиомикрофоны.

Вопрос 2. Средства и методы обеспечения информационной безопасности

Немаловажным фактором в защите информации, циркулирующей в информационной инфраструктуре ОВД, является ее защита от несанкционированного снятия со строительных конструкций зданий и сооружений служебных помещений. Развитие средств и систем несанкционированного снятия информации, открытость и относительная доступность их приобретения и изготовления ставят задачи по организации технической защиты на объектах ОВД, устойчивой к потенциальным угрозам несанкционированного снятия.

Устранение акустических и виброакустических каналов утечки информации основано на тех же физических процессах и явлениях, которые лежат в основе построения средств и методов несанкционированного снятия информации по акустическим и виброакустическим каналам – процессах распространения акустических волн в воздушных средах и распространения упругих волн в однородных средах, какими являются строительные конструкции служебных зданий и сооружений ОВД, а также коммуникации водоснабжения и отопления.

Так, защита от акустического снятия информации предполагает использование двух подходов. Первый основан на построении в служебных помещениях т. н. акустических демпферов – метод пассивной акустической изоляции.

Второй метод предполагает активное акустическое и виброакустическое зашумление с помощью специальных генераторов низкочастотных (звуковых) шумовых акустических и виброакустических сигналов, которые предназначены для акустического и виброакустического зашумления каналов утечки информации.

Защита от прямого акустического снятия информации основывается на выявлении и устранении строительных дефектов и изъянов с точки зрения ухудшения звукоизоляции: заделываются щели в стенах и перекрытиях, устанавливается дополнительная звукоизоляция в виде фальшпотолков, фальшстен, акустических и виброакустических экранов, акустических экранов водоотопительной системы, специальных оконных рам и вакуумного застекления.

Кроме того, для зашумления воздуховодов, помещений небольшого объема (салон автомобиля, комнаты переговоров и т. д.), а также создания заградительных шумовых помех от снятия речевых сигналов направленными микрофонами используются устройства активного акустического зашумления.

Для защиты речевых сигналов от несанкционированного снятия по виброакустическим каналам утечки информации используется *метод активного виброакустического зашумления*. Этот метод состоит в наведении в строительных конструкциях служебных зданий и сооружений упругих шумовых виброколебаний, которые распространяются по всему объему строительной конструкций, вызывая шумовые микродеформации, которые в свою очередь подавляют микродеформации, создаваемые воздействием речевых сигналов на те же конструкции, т. е. происходит шумовое виброзашумление упругих волн, создаваемых речевыми сигналами людей, находящихся в контролируемой зоне. В этом случае значительно снижается возможность, как восприятия речевых сигналов, так и их распознавания устройствами несанкционированного съема.

Система виброакустического зашумления состоит из генератора низкочастотных шумовых сигналов, нескольких вибропреобразователей, осуществляющих формирование виброакустических сигналов.

Датчики вибропреобразователей виброакустического зашумления в случае стационарного оборудования объекта защиты монтируются на перекрытиях, стенах, водопроводных коммуникациях и отопительных батареях, вентиляционных шахтах, оконных переплетах и т. д., и создают заградительную виброакустическую помеху в элементах строительных конструкций.

Во время отсутствия в контролируемых помещениях звуковых сигналов вибродатчики находятся в режиме «молчания», при появлении в контролируемых помещениях звуковых сигналов акустические микрофоны воспринимают их и вырабатывают команду для включения шумовых вибропреобразователей.

В качестве перспективных разработок систем виброакустического зашумления выбрано направление на построение адаптивных

систем, которые вырабатывают шумовую помеху в зависимости от материала и толщины строительных конструкций, определена тенденция на уменьшение габарито-весовых показателей. Такие системы позволяют автоматически оценивать результат виброакустического зашумления и выдавать данные о выполнении поставленной задачи. Результаты такого анализа сопровождаются в виде голосового сообщения.

Наиболее опасными с точки зрения несанкционированного снятия информации за счет побочных электромагнитных излучений и наводок (далее – ПЭМИН) являются мониторы компьютеров со стандартами разверток телевизионных систем. Во всех указанных случаях даже использование мощных криптографических средств и методов защиты не приводит к желаемым результатам, и только применение специальных методов и аппаратуры защиты от ПЭМИН способно устранить возникший канал утечки информации.

Активное радиотехническое подавление и маскировка ПЭМИН заключаются в формировании и излучении в непосредственной близости от устройств вычислительной техники широкополосного шумового сигнала с уровнем излучения, превышающим уровень излучения информационного сигнала во всем частотном диапазоне, где имеются эти излучения, а также в осуществлении наводок, подавляющих побочные электромагнитные излучения, создаваемые информационными сигналами, в отходящие цепи коммутации и линии электропитания.

Для осуществления электромагнитного подавления ПЭМИН разработан класс генераторов электромагнитных колебаний «белого электромагнитного шума», создающих шумовое электромагнитное поле в диапазоне частот от десятков килогерц до единиц и десятков гигагерц со спектральным уровнем излучаемого сигнала, существенно превышающим уровни электромагнитных излучений создаваемых средствами вычислительной техники.

Существует *два типа изделий электромагнитного зашумления:*

1. Генераторы объемного электромагнитного зашумления.
2. Генераторы локального электромагнитного зашумления.

Средства телефонной связи достаточно часто используются для несанкционированного получения информации, как конкурентами, так и криминальными структурами, этому в немалой степени способствует отсутствие элементарного порядка в телефонном хозяйстве городов, предприятий и организаций.

Структурные методы защиты речевых сообщений с использованием телефонных линий связи и слаботочной аппаратуры можно классифицировать по следующим направлениям:

– обнаружение несанкционированного подключения устройств снятия речевых сигналов и активная защита телефонных линий;

– скремблирование речевых сигналов;

– шифрование речевых сигналов.

Наиболее вероятными каналами утечки речевой информации являются телефонные линии связи. Устройства активной защиты предназначены для нейтрализации несанкционированно подключаемых устройств на участке «абонентский аппарат – телефонная станция».

В этом случае нейтрализация устройств несанкционированного снятия осуществляется путем генерации в телефонную сеть низкочастотных и высокочастотных помех, а также управлением потребления тока в линии связи при ведении разговоров, что приводит к снижению соотношения сигнал/шум на входе несанкционированно подключенных устройств снятия речевых сигналов и блокировке акустопуска звукозаписывающей аппаратуры. То есть полезный сигнал на входе устройства снятия по отношению к специально создаваемой шумовой помехе становится такой величины, что несанкционированно подключенное устройство не срабатывает. Это исключает или уменьшает вероятность приема и распознавания полезного речевого сигнала.

Для активной защиты телефонных линий применяются следующие методы:

– блокирование (нейтрализация) устройств несанкционированного снятия за счет снижения отношения сигнал/шум на входе подслушивающего устройства;

– размывание спектра радиопередающего подслушивающего устройства;

– сдвиг рабочей частоты радиопередающего устройства в более высокочастотный диапазон, что приводит к невозможности восприятия и распознавания информационных сигналов приемниками несанкционированных пользователей;

– блокирование акустопуска звукозаписывающей аппаратуры;

– защита телефонного тракта от ВЧ-навязывания;

– осуществление гальванической развязки телефонного аппарата от линии связи за счет оптоэлектронных преобразователей;

– полное подавление устройств несанкционированного снятия специальными генераторами;

– методы скремблирования и шифрования телефонных переговоров.

В качестве активных методов защиты речевых сообщений в системах конфиденциальной связи нашли широкое применение

различного рода скремблирующие устройства и устройства шифрования речевых сигналов.

Методы защиты речевых сообщений по степени стойкости к несанкционированному воздействию подразделяются:

– на методы обеспечения временной стойкости речевых сообщений от несанкционированного доступа;

– на методы гарантированной защиты информации от несанкционированного доступа.

К способам обеспечения временной стойкости речевых сообщений от несанкционированного доступа относят методы аналогового скремблирования, которые обеспечивают временную стойкость передаваемых сообщений за счет изменения характеристик исходного речевого сигнала таким образом, что выходной преобразованный речевой сигнал становится неразборчивым для несанкционированного пользователя.

Преимуществом такого метода защиты речевых сообщений является относительная простота технической реализации, что определяет относительно низкую стоимость и малые габариты, возможность передачи заскремблированных сигналов по стандартным телефонным каналам и хорошее качество восстановления исходного речевого сигнала приемником при дескремблировании.

Рассмотренные методы защиты информации в комплексном применении способны обеспечить надежную защиту информации, циркулирующей в информационных инфраструктурах ОВД, и создать надежный заслон несанкционированному восприятию и распознаванию сообщений со стороны несанкционированных пользователей.

Таким образом, можно заключить, что разработка практических рекомендаций по проведению мероприятий, направленных на достижение требуемого уровня защиты информации, возможна лишь после всестороннего изучения объекта защиты. Кроме того, необходимо получить достоверные оценки уровня защищенности циркулирующей в нем информации, определить, каким путем может быть организован несанкционированный съем информации, и обоснованно выявить вероятные каналы ее утечки.

Утечки могут быть связаны с работой персонала, имеющего непосредственный контакт с циркулирующей информацией (например, сотрудники, обслуживающие программно-аппаратные средства вычислительной техники). Причем эти утечки могут возникнуть не только за счет эксплуатационных ошибок или халатных действий, но и стать результатом преднамеренных противоправных действий отдельных сотрудников.

Неправоверный доступ к конфиденциальным сведениям может быть также организован «извне», путем проведения разведывательных мероприятий, реализующих перехват информации по техническим каналам.

Техническая защита выделенных и защищаемых помещений проводится с целью обеспечения безопасности акустической информации ограниченного доступа, циркулирующей в данных помещениях. Защита осуществляется с применением как пассивных, так и активных методов и технических средств, путем ослабления уровня информационных сигналов или снижения соотношения сигнал/шум в тракте передачи до величин, исключающих возможность перехвата за пределами контролируемой зоны.

К пассивным методам защиты относятся:

– звуко- и виброизоляция строительных конструкций и инженерных коммуникаций;

– звуко- и вибропоглощение акустических сигналов;

– встраивание во вспомогательные технические средства и системы, обладающие «микрофонным» эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров и ограничителей сигналов.

К активным методам защиты информации относятся:

– акустическое и виброакустическое зашумление строительных конструкций и инженерных коммуникаций;

– постановка прицельных помех на частотах работы радиозакладных устройств;

– подавление устройств записи акустической информации, беспроводных систем связи и передачи данных.

Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, т. к. возможен ее перехват с помощью специальных технических средств контроля. С целью исключения возможности перехвата информации в соответствии с требованиями руководящих документов по защите информации ФСБ России и ФСТЭК России для защиты объектов информатизации используются как пассивные, так и активные способы защиты от побочных электромагнитных излучений и наводок (ПЭМИН).

Заключение

В современных условиях функционирования органов внутренних дел управленческая деятельность лица, принимающего решение, сопряжена с огромным объемом поступающих данных. Наибольшую сложность вызывает обработка неструктурированных «сырых» данных, которые значительно повышают степень неопределенности и риска при принятии управленческих решений. Переработать такой объем данных возможно только за счет применения современных информационных технологий, основанных на перспективных методах анализа данных. Значительная роль в процессе принятия решений отводиться системе информационно-аналитического обеспечения как одного из ключевых компонентов системы управления.

Деятельность руководителя органа внутренних дел связана с широким кругом решаемых задач в сфере информационных технологий. Разнообразный перечень направлений оперативно-служебной деятельности – организации оказания государственных услуг, анализа оперативной обстановки, обеспечения информационной безопасности и другое – предполагает широкий спектр знаний в области математического моделирования, прогнозирования, теории управления и принятий решений.

В предложенном курсе лекций в сжатом виде представлены два основных направления: информационные технологии управления и организация зашиты информации. Данные курс лекций не претендует на полноту описания затрагиваемых проблем и решаемых задач в рассматриваемой сфере. Вместе с тем изложенные материалы могут являться эффективным инструментом в информационно-аналитической деятельности подразделений органов внутренних дел.

Список литературы

Нормативные правовые акты

Конституция РФ [Электронный ресурс]: принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».

О полиции [Электронный ресурс]: федер. закон Российской Федерации от 7 февраля 2011 г. № 3-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

О безопасности [Электронный ресурс]: федер. закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: федер. закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

О государственной тайне [Электронный ресурс]: Закон Российской Федерации от 21 июля 1993 г. № 5485-1 (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

О персональных данных [Электронный ресурс]: федер. закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ (ред. от 31 декабря 2017 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

Об информации, информационных технологиях и защите информации [Электронный ресурс]: федер. закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Об организации предоставления государственных и муниципальных услуг: федер. закон Российской Федерации от 27 июля 2010 г. № 210-ФЗ // СЗ РФ. 2010. № 31. Ст. 4176.

Об электронной подписи [Электронный ресурс]: федер. закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: Указ Президента РФ от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

Вопросы организации информационно-аналитической работы в управленческой деятельности органов внутренних дел Рос-

сийской Федерации [Электронный ресурс]: приказ МВД России от 26 сентября 2018 г. № 623. Доступ из справ.-правовой системы «КонсультантПлюс».

Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 31 декабря 2013 г. № 1040. Доступ из справ.-правовой системы «КонсультантПлюс».

Основная литература

Информационные технологии в управлении и организация защиты: учебник / В. В. Баранов и др.; под ред. И. В. Горошко. Москва: Академия управления МВД России, 2018.

Информационные технологии в управлении органами внутренних дел: учебник / В. В. Баранов и др.; под ред. И. В. Горошко. Москва: Академия управления МВД России, 2015.

Горошко И. В., Торопов Б. А., Гонов Ш. Х. Математические методы исследования социальных систем: курс лекций. Москва: Академия управления МВД России, 2019.

Торопов Б. А., Гонов Ш. Х. Статистические методы принятия управленческих решений: сборник задач (задачник). Москва: Академия управления МВД России, 2019.

Лукашов Н. В., Лебедев В. Н., Макаров В. Ф. Информатизация и информационная безопасность органов внутренних дел: курс лекций. Москва: Академия управления МВД России, 2012.

Торопов Б. А., Апульцин В. А. Технологии многокритериального оценивания результатов деятельности территориальных органов МВД России на региональном уровне: учебное пособие. Москва: Академия управления МВД России, 2016.

Защита информации: учебник в 2-х ч. / В. Н. Лебедев и др.; под ред. В. И. Кирина. Москва: Академия управления МВД России, 2013.

Электронные ресурсы

Сайт МВД России. URL: http://www.mvd.ru.

Сайт ФКУ «ГИАЦ МВД России». URL: http://10.5.0.15.

Сайт ЦСИ ФКУ «ГИАЦ МВД России». URL: http://10.5.0.16.

Сайт Единой межведомственной информационно-статистической системы. URL: http://www.fedstat.ru.

Сайт Федеральной службы государственной статистики. URL: http://www.gks.ru.

Единое окно доступа к образовательным ресурсам. URL: window.edu.ru.

Справочная правовая система «КонсультантПлюс».

Справочная правовая система СТРАС «Юрист».

Электронная библиотечная система. URL: www.iprbookshop.ru.

ДЛЯ ЗАМЕТОК

Учебное издание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ И ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Курс лекций

Редактор *В. А. Яровая*
Верстка *С. Н. Портнова*

Подписано в печать 27.07.2021. Формат 60x84 $^{1}/_{16}$.
Усл. печ. л. 4,19. Уч. изд. л. 3,38. Тираж 289 экз. Заказ № 31у

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России.
125993, Москва ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907187-76-4