МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Барнаульский юридический институт

В.А. Кемпф

Обеспечение информационной безопасности в органах внутренних дел

Учебное пособие

Барнаул 2019

ББК 32.97я73 + 67.401.133.1я73
К 352

Кемпф, В.А.
К 352 Обеспечение информационной безопасности в органах внутренних дел : учебное пособие. – Барнаул : Барнаульский юридический институт МВД России, 2019. – 63 с.

ISBN 978-5-94552-378-4

Рецензенты:

Бенцлер А.В. – начальник отдела защиты информации центра информационных технологий, связи и защиты информации ГУ МВД России по Алтайскому краю;

Еськов А.В. – доктор техн. наук, доцент, профессор кафедры информационной безопасности Краснодарского университета МВД России.

Работа посвящена исследованию актуальных вопросов обеспечения информационной безопасности в органах внутренних дел: нормативно-правового регулирования защиты информации ограниченного доступа на объектах ОВД; организационных и технических мероприятий, обеспечивающих защиту информации ограниченного доступа, контроля эффективности защиты информации; вопросов ответственности за совершение информационных и компьютерных правонарушений; обеспечения информационной безопасности в ведомственной информационной системе ИСОД МВД России. Рассматриваются нормативные документы в области информационной безопасности, теоретические и практические аспекты обеспечения безопасности ведомственной информации.

Учебное пособие предназначено для учебно-методического обеспечения образовательного процесса обучающихся в образовательных организациях высшего образования системы МВД России по дисциплине «Основы информационной безопасности в ОВД».

ББК 32.97я73 + 67.401.133.1я73

ISBN 978-5-94552-378-4

Введение

Актуальность проблемы обеспечения информационной безопасности органов внутренних дел определяется рядом взаимосвязанных факторов, бóльшая часть из которых непосредственно является следствием процесса информатизации современного общества:

- применения в правоохранительной деятельности новейших информационных технологий высокой сложности;
- высокой уязвимости инфраструктуры, определяемой сложностью используемых систем;
- интенсивного развития и совершенствования технических средств разведывательного назначения.

В настоящее время Министерством внутренних дел Российской Федерации вопросы развития и внедрения автоматизированных информационных систем в деятельности органов внутренних дел, в т.ч. применения передовых подходов и технологий информатизации МВД России, стоят на одном из первых мест.

В марте 2012 г. руководством Министерства внутренних дел Российской Федерации был принят целый ряд нормативных правовых актов в области информационных технологий и обеспечения защиты ведомственной информации, заложивших принципиально новый подход к информатизации органов внутренних дел.

Концепция создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012-2014 гг., утвержденная приказом МВД России от 30.03.2012 № 205, определила основную цель преобразований в этом направлении – создание на базе единой информационно-телекоммуникационной системы органов внутренних дел (ЕИТКС МВД России) единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России).

При разработке Концепции создания ИСОД МВД России были максимально учтены и положительные, и отрицательные результаты, достигнутые в ходе реализации программных мероприятий по созданию единой информационно-телекоммуникационной системы органов внутренних дел.

При этом сам подход к дальнейшему развитию информатизации деятельности органов внутренних дел, изложенный в Концепции информатизации, кардинально отличался от системы взглядов, действующих ранее. И в первую очередь это связано с переходом к совершенно новой общей концепции построения информационного пространства Министерства.

Ранее действующая концепция, базирующаяся на создании обособленных информационных систем по каждому направлению деятельности – специализированных территориально распределенных автоматизированных информационных систем (СТРАС), в ИСОД МВД России заменилась принципом централизации информационных систем и ресурсов с использовани-

ем для обработки практически всей информации единой технологической платформы.

Очевидными плюсами использования единой системы информационно-аналитического обеспечения МВД России при новом подходе стали:

- применение современных технологий централизованной обработки данных и виртуализации, обусловивших снижение эксплуатационных расходов,
- применение высокопроизводительных программно-технических комплексов обработки информации,
- обеспечение доступа сотрудника к объему информации, необходимому для его служебной деятельности.

Кроме того, в единой системе информационно-аналитического обеспечения МВД России регламентирован общий механизм эксплуатации, включающий и ранее созданные, но продолжаемые эксплуатироваться информационные системы при их интеграции в ИСОД МВД России, а также предусмотрена система мониторинга, обеспечивающая непрерывный контроль процесса предоставления государственных услуг в электронном виде.

Основной целью создания единой системы информационно-аналитического обеспечения деятельности МВД России стало улучшение качества информационно-аналитического обеспечения деятельности МВД России.

В основе единой системы информационно-аналитического обеспечения деятельности МВД России лежит технология облачных вычислений, базирующаяся на использовании общей для всего информационного пространства МВД России технологической платформы и обеспечении сотрудников органов внутренних дел информационными сервисами.

При внедрении новых технологий основное внимание было уделено автоматизации основных направлений деятельности сотрудников, реализованной благодаря разработке и внедрению типовых программно-технических решений, что позволило освободить сотрудников от выполнения повседневной рутинной работы и значительно повысить эффективность использования рабочего времени для выполнения прямых служебных задач.

Совершенствуется и развивается пришедшая на смену ЕИТКС интегрированная мультисервисная телекоммуникационная система органов внутренних дел (ИМТС). В настоящее время активно отрабатываются решения, обеспечивающие увеличение производительности транспортной среды органов внутренних дел, вопросы безопасного мобильного доступа к ресурсам ИСОД МВД России.

В настоящее время практически создана эффективная система информационной безопасности органов внутренних дел, использующая комплекс современных методов технической и криптографической защиты информации, позволяющая достичь необходимого уровня защиты информации органов внутренних дел от средств технических разведок, ее утечки по техническим каналам и несанкционированного доступа к ней.

Глава 1. Защита информации как обеспечение информационной безопасности и безопасности информации

1.1. Основные понятия и определения в области защиты информации

Согласно новой Доктрине информационной безопасности Российской Федерации, «обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления».

В Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 г., утвержденной приказом МВД России от 14.03.2012 № 169, **информационная безопасность органов внутренних дел** определяется 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».

В соответствии с ГОСТом Р 50922–2006 «Защита информации. Основные термины и определения» под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

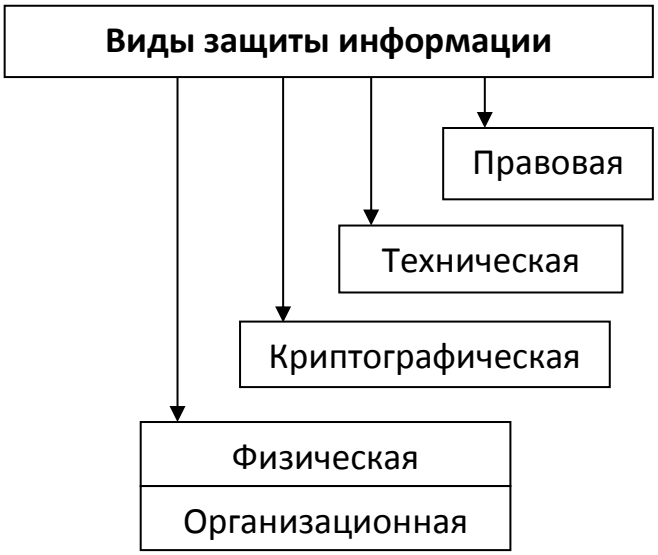


Рис. 1. Виды защиты информации

Выделяют следующие виды защиты информации: правовую, техническую, криптографическую, физическую и организационную *(рис. 1)*.

Правовая защита информации включает в себя разработку нормативно-правовых документов, регламентирующих отношения, которые возникают при осуществлении права на поиск, получение, передачу, производство и распространение информации, а также применение этих документов, надзор и контроль за их исполнением.

Техническая защита информации – обеспечение безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств без применения криптографических методов.

Криптографическая защита информации осуществляется криптографическими средствами, которые с помощью специальных математических алгоритмов осуществляют преобразование информации, передаваемой по линиям связи или хранящейся в технических средствах таким образом, что при несанкционированном доступе невозможно ознакомиться с ее содержанием.

Физическая защита информации осуществляется путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. К физической защите относятся средства инженерно-технической укрепленности охраняемых объектов и технические средства охраны.

Организационной защитой – мероприятиями по обеспечению защиты информации – устанавливаются режимные, временны́е, территориальные, пространственные ограничения на условия использования и распорядок работы объекта защиты.

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

Защищаемый объект информации – объект информации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Защищаемая информационная система – информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

Безопасность информационных систем является частью общей информационной безопасности, в связи с чем уместно рассматривать ряд общих подходов к безопасности, в значительной степени применимых и в отношении информационных систем.

Информация, получаемая субъектами посредством информационных систем и удовлетворяющая требованиям безопасности информации, должна обладать следующими свойствами:

- доступностью,
- целостностью,
- конфиденциальностью.

Доступность информации – свойство информационных ресурсов, определяющее возможность за приемлемое время выполнить ту или иную операцию над данными или получить нужную информацию уполномоченными на это лицами.

Целостность информации – неизменность информации в процессе ее хранения, обработки и передачи по каналам связи.

Конфиденциальность информации – защищенность информации от несанкционированного доступа.

Безопасность информационных систем – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, нарушающих доступность, целостность или конфиденциальность информации.

Угрозой безопасности информации называют действие или событие, которое может привести к нарушению достоверности, целостности или конфиденциальности хранящейся, передаваемой или обрабатываемой информации.

При этом следует отметить, что речь идет о защите не только хранящейся в информационной базе информации, но и информации, передаваемой по каналам связи или обрабатываемой программным обеспечением.

Определим ряд понятий, наиболее часто используемых при анализе безопасности информационных систем.

Угрозой называют совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Основными видами угроз безопасности информационных систем и угроз интересам субъектов информационных отношений являются:

- стихийные бедствия (пожар, наводнение, землетрясение и т.п.) и аварии;
- сбои и отказы технических средств вычислительных систем;
- последствия ошибок проектирования программных и аппаратных средств, процессов обработки информации, структур данных и т.п.);
- ошибки эксплуатации операторов, пользователей и обслуживающего персонала;
- преднамеренные действия злоумышленников и нарушителей.

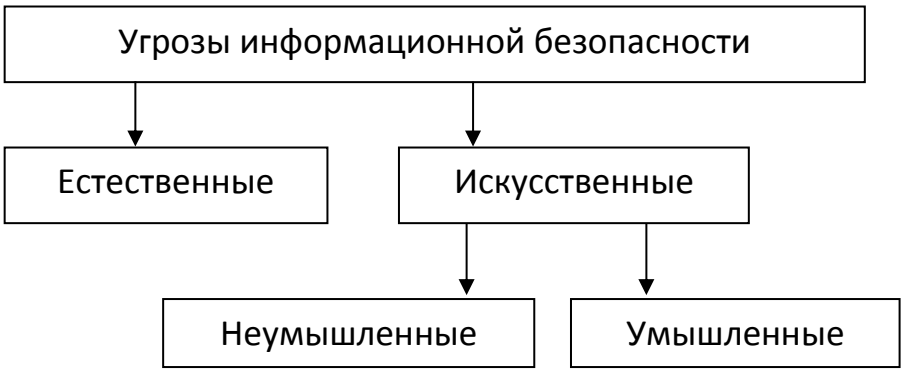


Рис. 2. Классификация угроз информационной безопасности

Таким образом, потенциальные угрозы по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на компьютерную систему и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

Искусственные угрозы – это угрозы компьютерной системе, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные.

Непреднамеренные (неумышленные) угрозы – угрозы, вызванные ошибками при проектировании информационной системы и ее элементов, ошибками персонала.

Преднамеренные (умышленные) угрозы – угрозы, связанные с корыстными устремлениями.

С целью обеспечения защиты информации и противостояния вышеперечисленным угрозам современные информационные системы включают в себя подсистемы безопасности, которые реализуют принятую политику безопасности.

1.2. Основные объекты информационной безопасности в ОВД

Информацию, рассматриваемую как объект защиты, как правило, классифицируют по следующим признакам:

- по форме представления;
- имущественным правам;
- категориям доступа.

Основными формами информации, циркулирующими в системе органов внутренних дел и представляющими интерес с точки зрения защиты, являются: акустическая (речевая), оптическая, документальная, телекоммуникационная.

Документальная информация – форма информации, наиболее представленная в работе органов внутренних дел. Документированием информации (процессом создания документа) называют ее фиксацию на материальном носителе, выполненную по установленным правилам. Документы, созданные по установленным правилам, приобретают в органах внутренних дел статус официальных или служебных документов.

В связи с возрастающим количеством информации, которая хранится и используется в электронно-цифровом виде, все чаще применяется понятие «электронный документ», под которым понимается документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информация, циркулирующая в настоящее время в органах внутренних дел, преимущественно представлена в электронном виде, что и определяет основные направления и усилия по обеспечению *информационной безопасности органов внутренних дел (рис. 3).*

В соответствии с Доктриной информационной безопасности Российской Федерации к наиболее важным объектам обеспечения информационной безопасности в правоохранительной сфере относятся:

•информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

•информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

•информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами для этих объектов являются:

•разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

•деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Рис. 3. Структура понятия «информационная безопасность ОВД»

Внутренними угрозами для объектов являются:

•нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

•недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

•отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;

•отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

•преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Основными объектами защиты при обеспечении информационной безопасности в органах внутренних дел являются:

- все виды информационных ресурсов (документированная информация, т.е. информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать);
- права граждан, юридических лиц и государства на получение, распространение и использование информации;
- система формирования, распространения и использования информации (информационные системы и технологии, персонал, нормативные документы и т.д.);
- система формирования общественного сознания (СМИ);
- объекты информатизации.

К объектам информатизации относятся: средства информатизации вместе с помещениями, в которых они установлены; технические средства, предназначенные для обработки, хранения и передачи защищаемой информации; выделенные помещения.

Глава 2. Основные способы защиты информации в ОВД

Согласно статье 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Таким образом, защита информации должна быть комплексной, т.е. сочетать в себе правовое, организационное и техническое направления защиты.

2.1. Нормативные документы в области информационной безопасности в органах внутренних дел

Нормативно-правовое регулирование мероприятий по защите объектов ОВД от утечки информации ограниченного доступа является основополагающим направлением в обеспечении информационной безопасности органов внутренних дел.

Информация как непосредственный объект защиты по правовому режиму доступа разделяется на ряд видов, и к обеспечению защиты различных видов информации применяется дифференцированный подход *(рис. 4)*.

Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет разделение информации (в зависимости от категории доступа к ней) на общедоступную информацию и информацию с ограниченным доступом.

Информацию с ограниченным доступом, в свою очередь, относят:

- к государственной тайне – в соответствии с Законом Российской Федерации «О государственной тайне»;
- информации, содержащей сведения конфиденциального характера.

Соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами Российской Федерации, является обязательным.

В соответствии с Указом Президента РФ № 188 от 06.03.97 «Об утверждении перечня сведений конфиденциального характера» к конфиденциальной информации относят:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Рис. 4. Классификация информации по категориям доступа

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Одним из фундаментальных понятий, связанных с обеспечением информационной безопасности в государственном масштабе, является понятие «государственной тайны». В законе Российской Федерации «О государственной тайне» значение этого термина определяется следующим образом: «Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

К государственной тайне относятся сведения:

- в военной области;
- о внешнеполитической и внешнеэкономической деятельности;
- в области экономики, науки и техники;
- в области разведывательной, контрразведывательной и оперативно-разыскной деятельности.

Степень секретности сведений, отнесенных к государственной тайне, является ее основным признаком.

В Российской Федерации законодательно закреплена следующая система обозначения сведений, составляющих государственную тайну:

- особой важности;
- совершенно секретно;
- секретно.

Гриф секретности указывается либо непосредственно в реквизитах документов, либо в сопроводительных или регламентирующих документах.

В соответствии с Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности (утв. Постановлением Правительства РФ от 4 сентября 1995 г. № 870), отнесены:

- сведения *особой важности.* Это сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях;
- *совершенно секретные* сведения – такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях;
- *секретные* сведения – все иные сведения из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам организации.

В соответствии с законом для организации, обрабатывающей государственную тайну, обязательным условием является наличие лицензии ФСБ «На осуществление работ с использованием сведений, составляющих государственную тайну». В «Положении по аттестации объектов информатизации по требованиям безопасности информации» от 25.11.1994 предусмотре-

на обязательная аттестация объектов, обрабатывающих государственную тайну.

Один из распространенных в органах внутренних дел видов информации ограниченного доступа – служебная тайна, что непосредственно связано с функционированием самой системы ОВД. Отношения, возникающие в связи с отнесением сведений к служебной тайне, их защитой и снятием ограничений на доступ к указанным сведениям в целях обеспечения прав, свобод и законных интересов граждан и организаций, осуществления установленных законодательством Российской Федерации полномочий федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации на момент написания работы регулируются «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденным Постановлением Правительства РФ от 3 ноября 1994 г. № 1233.

Согласно Положению, «к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью».

В системе МВД России служебную тайну составляет информация, которая:

- образуется в процессе деятельности органов, подразделений и учреждений системы МВД России и внутренних войск МВД России или передана им из других федеральных органов исполнительной власти;
- не составляет государственной тайны, однако ее разглашение (распространение) может нанести ущерб интересам МВД России;
- имеет действительную или потенциальную ценность и может являться предметом посягательств в силу неизвестности ее другим лицам и отсутствия к ней свободного доступа на законных основаниях.

В целях обеспечения информационной безопасности документы, содержащие сведения, составляющие служебную тайну, не включаются в электронные информационные системы, имеющие подключение к сети связи общего пользования. Кроме того, для защиты сведений, составляющих служебную тайну, должны использоваться средства защиты информации, прошедшие сертификацию в порядке, установленном законодательством Российской Федерации.

МВД России продолжает активную работу по совершенствованию нормативно-правового регулирования вопросов обращения со служебной информацией ограниченного распространения. Результатом этой работы стало появление приказа МВД России от 09.11.2018 № 755, определяющего порядок обращения со служебной информацией ограниченного распространения в системе МВД России, и устанавливающего требования, обязательные для

сотрудников, федеральных государственных гражданских служащих и работников системы МВД России, при обращении с документами и другими материальными носителями, содержащими служебную информацию ограниченного распространения.

Другая разновидность информации ограниченного доступа, в больших объемах обрабатываемой в информационных системах МВД – персональные данные.

Персональные данные – это любая информация, относящаяся к определенному физическому лицу, в т.ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

Регулирование вопросов защиты персональных данных в России начато непосредственно с Конституции Российской Федерации 1993 г. Согласно ст. 23 и 24 Конституции РФ каждый гражданин Российской Федерации имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Запрет собирать, хранить, использовать и распространять информацию о частной жизни лица особое значение приобретает в связи с широкой эксплуатацией в настоящее время информационных систем, позволяющих накапливать и обрабатывать значительные массивы информации.

К персональным данным относят следующие сведения:

- идентификационные данные;
- биографические данные;
- личные характеристики;
- сведения о семейном положении;
- сведения о социальном положении;
- сведения о состоянии здоровья;
- особенности половой жизни гражданина и его половая ориентация;
- политические взгляды и религиозные убеждения.

Сведения, относящиеся к персональным данным, необходимы сотрудникам органов внутренних дел для предотвращения преступлений и административных правонарушений; выявления обстоятельств, способствующих их совершению; осуществления оперативно-разыскной деятельности; производства дознания и предварительного следствия; экспертно-криминалистической деятельности; розыска лиц и похищенного имущества; выдачи гражданам различного рода лицензий и разрешений и т.д.

В период до 2014 г. в системе МВД на всей территории Российской Федерации эксплуатировалось около 200 разнообразных информационных си-

стем персональных данных (ИСПДн), нуждающихся в защите в соответствии с требованиями законодательства. В настоящее время все они перенесены в единую информационно-аналитическую систему обеспечения деятельности МВД России – ИСОД МВД России.

Основным нормативным документом, определяющим требования к защите ИСПДн, является Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, меры по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных, а также обязанности должностных лиц определяет приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации».

Приказом МВД от 15 июля 2013 г. № 538 «О внесении изменений в приказ МВД России от 6 июля 2012 г. № 678 “Об утверждении инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации”», утверждена замена устаревшей терминологии в соответствии с Постановлением Правительства № 1119 и введены в качестве методических документов, регламентирующих установление класса защищенности информационной системы и уровня защищенности ПДн, Постановление Правительства № 1119 от 1 ноября 2012 г., приказы ФСТЭК № 17 от 11.02.2013 и № 21 от 18.02.2013.

Для информационных систем, обрабатывающих персональные данные (ИСПДн), устанавливаются четыре класса защищенности, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Определение классов защищенности информационных систем персональных данных производится в соответствии с требованиями приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Определение уровней защищенности персональных данных в ИСПДн проводится в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В информационных системах устанавливаются четыре уровня защищенности персональных данных.

В соответствии с информационным сообщением ФСТЭК от 15 июля 2013 г. № 240/22/2637 в качестве методического документа при реализации

защиты технических средств государственных информационных систем, обрабатывающих конфиденциальную информацию, в целях защиты от утечки по техническим каналам применяется методический документ Гостехкомиссии «СТР-К», имеющий гриф «для служебного пользования».

При применении криптографических средств защиты в информационных системах, обрабатывающих персональные данные, обязателен для исполнения приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Приказом МВД России от 29 декабря 2016 г. № 925 «О некоторых вопросах обработки персональных данных в МВД России» сформулирован перечень персональных данных, обрабатываемых в МВД России в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций.

Приказ МВД России от 21 декабря 2017 г. № 949 «О некоторых мерах, направленных на обеспечение выполнения МВД России обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ “О персональных данных”» определяет правила обработки персональных данных в системе МВД России, а также правила осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных.

Одним из эффективных методов защиты персональных данных является их обезличивание. Под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. В случае обезличивания персональных данных правила обработки таких данных в Министерстве внутренних дел Российской Федерации утверждены приказом МВД России от 14 ноября 2017 г. № 852.

2.2. Организационная и техническая защита информации ограниченного доступа

Организационная защита информации ограниченного доступа – регламентация на нормативно-правовой основе деятельности и взаимоотношений сотрудников и иных лиц, исключающая либо существенно затрудняющая несанкционированный доступ к информации за счет проведения организационных мероприятий.

Организационные мероприятия, по сути, выступают вторым эшелоном защиты в структуре обеспечения информационной безопасности, выступая промежуточным звеном между правовой и технической защитой информации. Организационная защита играет значительную роль в обеспечении информационной безопасности ведомства, т.к. возможности несанкционированного использования информации ограниченного доступа в значительной мере определяются именно человеческим фактором (халатностью, небрежностью, умыслом), а не применяемыми техническими средствами защиты.

К организационным мероприятиям относят:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных зданий и помещений. Целью этих мероприятий является исключение возможности нелегального проникновения на территорию и в защищаемые помещения; разделение территории, зданий и помещений на зоны по типу конфиденциальности циркулирующей в них информации, организация в зонах самостоятельных систем доступа и т.п.;
- мероприятия, выполняемые при подборе персонала: обучение правилам работы с информацией ограниченного доступа, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организация хранения и использования документов и носителей информации ограниченного распространения, включающая порядок учета, выдачи, исполнения и возвращения;
- организация охраны помещений и территории;
- организация и поддержание пропускного режима;
- организация защиты информации;
- организация регулярного обучения сотрудников.

Многогранность сферы организационной защиты информации в органах внутренних дел требует существования специальной службы, обеспечивающей и направляющей реализацию всех организационных мероприятий.

Приказом МВД России от 2 июля 2012 г. № 660 утверждено Типовое положение о подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации. В соответствии с данным положением подразделение ИТСиЗИ является структурным подразделением территориального органа, обеспечивающим и осуществляющим в пределах своей компетенции в т.ч. функции по противодействию техническим разведкам; технической (в т.ч. криптографической) защите информации; радиоэлектронной борьбе; использованию электронной подписи; защите персональных данных при их автоматизированной обработке; а также функции шифровального органа.

Основными задачами подразделения ИТСиЗИ в области защиты информации являются:

•организация и реализация мероприятий по технической (в т.ч. криптографической) защите информации и противодействию техническим разведкам;

•обеспечение функционирования и безопасности шифрованной связи в территориальном органе.

В целях реализации указанных задач подразделения ИТСиЗИ выполняют следующие функции в области защиты информации:

•осуществление в пределах своей компетенции мероприятий по защите государственной тайны, информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, защите персональных данных при их автоматизированной обработке и контроля за их проведением подразделениями территориального органа;

•осуществление мероприятий по противодействию техническим разведкам; радиоэлектронной борьбе; технической (криптографической) защите информации;

•осуществление контроля за обеспечением в подразделениях территориального органа исполнения предписаний нормативных правовых актов в области защиты информации, в т.ч. за порядком обращения с шифрованной информацией;

•информирование руководства территориального органа, а также по его поручениям руководителей подразделений территориального органа о выявленных и возможных угрозах информационной безопасности территориального органа;

•осуществление мероприятий по внедрению и использованию в территориальном органе средств электронной подписи;

•организация шифровальной службы в территориальном органе, руководство органами криптографической защиты информации по специальным вопросам и контроль за их деятельностью;

•подготовка и направление в установленном порядке в уполномоченное подразделение МВД России сведений и донесений по вопросам шифровальной службы МВД России;

•организация и обеспечение бесперебойной шифрованной связи в интересах руководства и подразделений территориального органа с органами управления, соединениями и воинскими частями внутренних войск МВД России, организациями и подразделениями системы МВД России, временными формированиями МВД России, развернутыми в регионах, где введено чрезвычайное положение, в зонах вооруженных конфликтов, в местах со сложной оперативной обстановкой, другими федеральными органами исполнительной власти в мирное время, при наступлении чрезвычайных об-

стоятельств, при введении режима чрезвычайного положения, а также в период мобилизации и в военное время;

•разработка и реализация мероприятий по обеспечению безопасности шифрованной связи в территориальном органе;

•обеспечение ведения учета шифрработников территориального органа.

Организационные меры защиты информации тесно связаны с физической защитой объектов. Вопросы обеспечения физической защиты и инженерно-технической укрепленности и повышения уровня антитеррористической защищенности объектов органов внутренних дел Российской Федерации от преступных посягательств нашли отражение в ряде ведомственных приказов, в частности, в приказе МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств». В зависимости от степени потенциальной угрозы объекты подразделяются на четыре категории (I, II, III и IV – низшая). Каждой категории объектов должен соответствовать определенный класс (степень) защиты конструктивных элементов: ограждающих конструкций и элементов инженерно-технической укрепленности.

Организационная защита информации определяет порядок и условия комплексного применения имеющихся сил и средств, эффективность которых во многом зависит от используемых методов **технической защиты.**

Техническая защита информации, используемая в комплексе с организационными мерами, играет исключительную роль в обеспечении защиты информации.

Технические средства защиты информации – устройства и приборы, предназначенные для обеспечения защиты информации, исключения ее утечек, создания помех (препятствий) техническим средствам съема информации.

Технические средства применяются для решения следующих задач:

•препятствия визуальному наблюдению и дистанционному подслушиванию;

•нейтрализации побочных электромагнитных излучений и наводок (ПЭМИН);

•обнаружения технических средств подслушивания и аудиофиксации, несанкционированно устанавливаемых или проносимых в защищаемые помещения и объекты;

•защиты информации, передаваемой в средствах связи и системах автоматизированной обработки информации.

Технические средства по функциональному назначению подразделяются на средства защиты и средства выявления несанкционированного доступа.

2.3. Технические каналы утечки информации

В общем случае информация передается полем или веществом: акустической волной, электромагнитным излучением, электрическим током, листом бумаги с текстом и т.д. Система передачи информации состоит из передатчика, канала передачи информации, приемника и получателя информации. Однако ввиду физической природы передачи информации при выполнении определенных условий возможно возникновение системы передачи информации, которая передает информацию вне зависимости от желания отправителя или получателя информации. Такую систему называют *техническим каналом утечки информации*.

Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации, называют *утечкой информации по техническому каналу.*

Рис. 5. Структура технического канала утечки информации

На рисунке 5 приведена структура технического канала утечки информации. Так же как и канал передачи информации, технический канал утечки информации состоит из источника сигнала, физической среды его распространения и приемной аппаратуры, осуществляющей несанкционированный доступ к информации.

Основными техническими каналами возможной утечки информации на объектах системы ОВД являются:

- акустический,
- электромагнитный,
- визуально-оптический.

Акустическая информация возникает в помещениях в ходе речевого общения, а также при функционировании систем звукоусиления и звуковоспроизведения.

Электромагнитный канал утечки информации образуется при функционировании практически любого радиоэлектронного устройства и проявляется появлением побочных излучений электромагнитных полей, которые мо-

гут содержать защищаемую информацию. Побочные электромагнитные излучения способны наводить в сторонних проводниках информационные сигналы, называемые наводками, достаточные для выделения аппаратурой технической разведки.

Визуально-оптический канал утечки информации образуется в результате распространения электромагнитных волн оптического диапазона, отраженных от объектов и окружающей обстановки, и реализуется путем применения специальных технических средств, расширяющих возможности органа зрения человека по ви́дению в условиях малой освещенности, при удаленности объектов наблюдения и недостаточности углового разрешения. При этом часто осуществляют документирование зрительной информации с применением электронных носителей.

Выделяют следующие мероприятия по выявлению технических каналов утечки информации:

- специальные проверки;
- специальные обследования;
- специальные исследования, включающие в себя:
  - ✓ выявление внедренных закладок в защищаемом помещении;
  - ✓ выявление схемотехнических и других доработок технических средств и систем (ТСС), приводящих к усилению естественных свойств ТСС;
  - ✓ выявление программных закладок, имеющих процессорное управление.

Специальная проверка технических средств и систем является комплексом инженерно-технических мероприятий, проводимых с использованием технических средств с целью исключения перехвата информации, содержащей государственную тайну, с помощью внедренных в защищаемое помещение закладок и других технических средств разведки. Основные определения приведены в ГОСТе Р 51583–2014 «Порядок создания автоматизированных систем в защищенном исполнении»:

Специальные обследования выделенных помещений – комплекс инженерно-технических мероприятий, проводимых с использованием необходимых, в т.ч. и специализированных технических средств. Цель специальных обследований – выявление внедренных технических средств перехвата информации, содержащей государственную тайну, в ограждающих конструкциях, предметах мебели и интерьера выделенных помещений.

Специальные исследования – мероприятия с использованием контрольно-измерительной аппаратуры, целью которых является выявление возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответ-

ствия защиты информации требованиям нормативных документов по защите информации.

Задача специального исследования сводится к измерению сигнала передатчика защищаемой информации и пересчету измеренных значений к величине, которая может поступить на вход технического средства съема информации. Затем по специальным методикам происходит вычисление отношения сигнал/шум и сравнение его с нормированными величинами.

Оценка защищенности объектов от утечек информации по акустическому, виброакустическому, электрическому и электромагнитному каналам является задачей, требующей большой квалификации операторов и наличия дорогой аппаратуры. Документы ФСТЭК и Гостехкомиссии, по которым оценивается защищенность на объектах, обрабатывающих информацию, составляющую государственную тайну, не доступны для общего пользования, поэтому для оценки защищенности таких привлекаются организации, у которых есть лицензия ФСТЭК на проведение специальных исследований: они имеют в своем арсенале методики ограниченного доступа, квалифицированных специалистов и необходимые технические средства.

Глава 3. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации

3.1. Единая информационно-аналитическая система обеспечения деятельности МВД России

В конце 2004 г. был принят приказ МВД России от 06.12.2004 № 813 «О мерах по созданию единой информационно-телекоммуникационной системы органов внутренних дел» (ЕИТКС).

В ходе реализации трех этапов программа создания ЕИТКС обозначила в качестве основной задачи объединение информационных ресурсов и обеспечение доступа к ним в реальном масштабе времени.

Основным итогом создания ЕИТКС стало формирование единого информационного пространства МВД России. ЕИТКС позволила осуществлять глобальный поиск информации по всем видам информационных ресурсов в реальном масштабе времени. Также была создана возможность передачи данных, обеспечения телефонной и видеоконференцсвязи.

Однако необходимо отметить, что взаимодействие между разными видами информационных ресурсов было налажено недостаточно, полноценное единое информационное пространство МВД России не создано, удобный для пользователя интерфейс и система поиска для ЕИТКС не реализованы, а система электронного документооборота не получила широкого распространения.

С 2011 г. в Министерстве в соответствии с приказом МВД России от 30.07.2011 № 891 «О мероприятиях по созданию единой системы информационно-аналитического обеспечения деятельности МВД России» создается единая система информационно-аналитического обеспечения деятельности МВД России. После опытной эксплуатации было принято решение о реализации программы по созданию единой системы информационно-аналитического обеспечения деятельности МВД России на базе ранее созданной ЕИТКС в полном объеме.

С этого момента ЕИТКС стала развиваться как интегрированная мультисервисная телекоммуникационная система (ИМТС) – такое название в итоге получила переименованная компьютерная сеть МВД России.

Перевод информационных систем обеспечения деятельности ОВД МВД России с платформы ЕИТКС на современную – ИМТС, произошедший в большинстве регионов в 2014 г., был обусловлен сменой общей концепции развития информационных систем МВД России.

Результатом этого явилось создание ИСОД МВД России – единой информационно-аналитической системы обеспечения деятельности органов внутренних дел МВД России, реализованной в формате сервисов.

3.2. Технологические основы ИСОД МВД России

В техническом отношении основой ИСОД МВД России являются три технологии:

- централизованной обработки данных,
- виртуализации,
- облачных вычислений.

Централизованная обработка данных (ЦОД) – это комплексное организационно-техническое решение, предназначенное для создания высокопроизводительной и отказоустойчивой информационной инфраструктуры.

Все системы ЦОД состоят из собственно ИТ-инфраструктуры и инженерной инфраструктуры, которая отвечает за поддержание оптимальных условий для функционирования системы.

Современная система ЦОД включает серверный комплекс, систему хранения данных, систему эксплуатации и систему информационной безопасности, которые интегрированы между собой и объединены высокопроизводительной сетью.

Серверный комплекс строится на основе многоуровневой архитектуры *(рис. 6).*

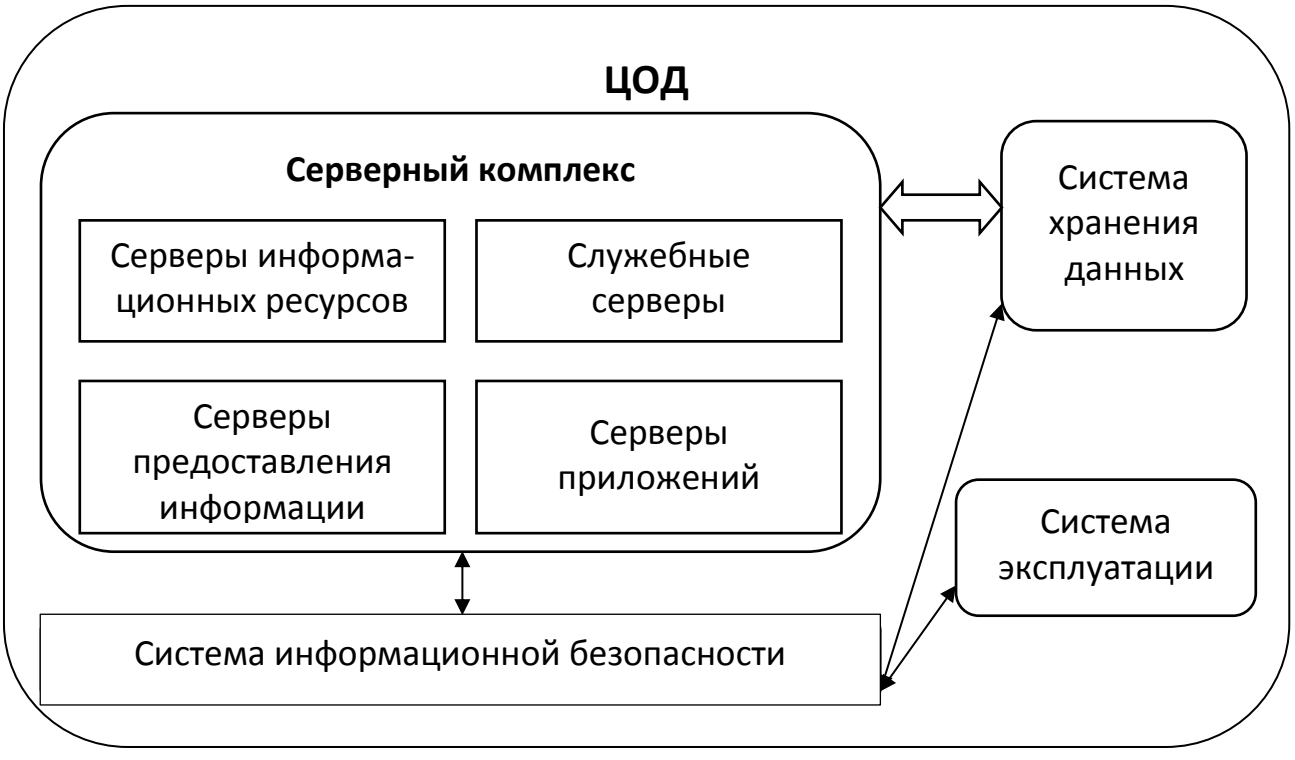


Рис. 6. Общая структура ЦОД

В архитектуре ЦОД выделяется несколько групп серверов:

•серверы информационных ресурсов отвечают за сохранение и предоставление данных серверам приложений;

•серверы приложений выполняют обработку данных в соответствии с логикой системы;

•серверы представления информации осуществляют интерфейс между пользователями и серверами приложений; например web-серверы;

•служебные серверы обеспечивают работу других подсистем ЦОД, например серверы управления системой резервного копирования.

К серверам разных групп предъявляются различные требования в зависимости от условий их эксплуатации.

Для серверов представления информации характерен большой поток коротких запросов от пользователей, поэтому они должны хорошо горизонтально масштабироваться (возможность увеличения количества серверов) для обеспечения распределения нагрузки.

Для серверов приложений требование горизонтальной масштабируемости остается, но оно не является критичным. Для них обязательна достаточная вертикальная масштабируемость (возможность наращивания количества процессоров, объемов оперативной памяти и каналов ввода-вывода) для обработки мультиплексированных запросов от пользователей и выполнения логики решаемых задач.

Современный ЦОД невозможно представить без систем виртуализации.

Технологии виртуализации позволяют создавать на одном сервере несколько логических систем – изолированных виртуальных машин с полным набором функций физических устройств. Виртуализация возможна не только в рамках одного физического сервера, но и в рамках нескольких серверов, ЦОД или нескольких географически разнесенных ЦОД. На современном уровне развития технологий возможна реализация виртуализации не только виртуальных машин, а также систем хранения и полнофункциональной сети.

Первые системы виртуализации возникли в рамках операционных систем и позволяли создать виртуальные ПК параллельно с выполнением основных задач. Развитие данного направления привело к появлению отдельного класса программного обеспечения – гипервизоров.

Гипервизор – это программное или аппаратное решение, работающее на сервере, создающее и контролирующее работу виртуальных машин.

Гипервизор устанавливается напрямую на аппаратную платформу и представляет все доступные ресурсы – мегагерцы процессора, мегабайты оперативной памяти, гигабайты места хранения и пропускную полосу сети для большого количества виртуальных машин. Гипервизор не только создает эти ресурсы для каждой виртуальной машины, но и перераспределяет ре-

сурсы между большим количеством потребителей и обеспечивает полный жизненный цикл виртуальных серверов.

Виртуализация центра обработки данных не ограничивается лишь серверами, к виртуализации применяется комплексный подход, использующий ряд технологий:

- виртуализацию серверов,
- виртуализацию хранилищ,
- виртуализацию служб,
- виртуализацию сети,
- управление виртуализацией.

Система хранения данных (СХД) является неотъемлемой частью виртуальной инфраструктуры. При виртуализиации СХД такое хранилище создается на базе тех же самых вычислительных узлов, что и виртуальные серверы, и использует серверные диски как часть единого хранилища. Это позволяет радикально сократить затраты на построение и обслуживание, выделить оптимизированные ресурсы хранения для каждой виртуальной машины. В дополнение система виртуализации СХД сама строит отказоустойчивую схему хранения с балансировкой нагрузки и в соответствии с политикой обслуживания для каждой виртуальной машины. Системы виртуализации СХД успешно применяются в ЦОД.

Для построения полностью программно определяемого ЦОД необходимо не только виртуализировать стандартные устройства для сервера, но и на основе принятых политик безопасности гибко управлять конфигурацией сетевой топологии и правил межсетевых экранов. Такая задача решается применением специальных программных продуктов – средств виртуализации сети (*Microsoft Windows Server Datacenter* совместно с *System Center, Cisco*).

Совершенствование технологий виртуализации привело к созданию полностью программно определяемых инфраструктур. Для управления такими инфраструктурами применяются мощные инструменты, учитывающие специфику установленного физического оборудования, имеющие возможность быстро предоставлять необходимые ресурсы, и являющиеся при этом прозрачными и защищенными. Для этих целей и служат системы управления и автоматизации виртуализацией (например, *Microsoft System Center*).

Виртуализированные ЦОД наиболее полно отвечают потребностям информационного обеспечения ОВД, значительно увеличивая надежность работы IT-систем, и обладают целым рядом преимуществ.

1. Виртуализация позволяет объединять системы и уменьшать количество физических серверов, что в конечном итоге приводит к освобождению дополнительного места в ЦОД, снижению стоимости оборудования, сокращению расходов на охлаждение и электрическую энергию.

2. Объединение серверов виртуализации в кластеры приводит к увеличению отказоустойчивости и масштабируемости информационной инфраструктуры (при выходе из строя физического сервера виртуальные машины перемещаются на другие серверы кластера, число же таких серверов гибко изменяется в зависимости от потребностей).

3. Благодаря специальным соглашениям на использование программного обеспечения в виртуальных средах достигается значительная экономия на лицензиях.

4. Системы резервного копирования виртуальной среды обеспечивают непрерывную защиту данных, результатом чего является быстрое восстановление данных и уменьшение времени простоя серверов.

5. Процесс развертывания новых серверов значительно ускоряется возможностью создания виртуальной машины из заранее подготовленного шаблона.

Концепция «облаков» является развитием идеи виртуализации.

Облачная технология – технология распределенной обработки данных, основанная на предоставлении пользователям вычислительных ресурсов как клиентам интернет-сервисов.

Под интернет-сервисом в данном случае понимается не доступ к сервису через интернет, а возможность широкого использования распространенных веб-технологий.

При реализации облачных технологий в качестве абонентских устройств могут быть использованы не только традиционные ПЭВМ в стационарном или портативном исполнении, но и современные телекоммуникационные устройства: смартфоны, карманные персональные компьютеры, планшеты.

Облачный сервис является, таким образом, клиент-серверной технологией, при которой клиент пользуется группой серверов как единым виртуальным сервером и может гибко регулировать объемы потребляемых ресурсов.

Вместе с тем между виртуализированным ЦОД и облачным ЦОД существует два важных отличия:

- клиенты облачного ЦОД имеют возможность самостоятельно изменять объемы потребляемых ресурсов;
- облачный ЦОД имеет более высокий уровень автоматизации (вплоть до полной автоматизации) и значительно большие возможности масштабирования.

Среди очевидных достоинств облачных технологий следует выделить: низкую стоимость, гибкость, надежность, концентрацию данных, большие вычислительные мощности.

Низкая стоимость. Основными факторами, снижающими стоимость использования облачных технологий, являются следующие: снижение расхо-

дов на обслуживание виртуальной инфраструктуры, вызванное развитием технологий виртуализации, за счет чего требуется меньший штат для обслуживания всей инфраструктуры; развитие аппаратной части вычислительных систем, обеспечивающее снижение стоимости оборудования.

Гибкость – неограниченность вычислительных ресурсов (память, процессор, диски). За счет использования систем виртуализации процесс масштабирования и администрирования «облаков» становится достаточно легкой задачей, т.к. «облако» самостоятельно может предоставить ресурсы, которые необходимы пользователям.

Надежность «облаков», особенно находящихся в специально оборудованных ЦОД (в случае МВД России – ведомственных), признается очень высокой, т.к. такие ЦОД имеют резервные источники питания, охрану, профессиональных сотрудников, регулярное резервирование данных, высокую пропускную способность канала, высокую устойчивость к DDoS-атакам (от англ. *Distributed Denial of Service,* распределенная атака типа «отказ в обслуживании»).

Концентрация данных. Централизованное хранение и обработка данных в едином хранилище могут обеспечить меньше риска в распределенной информационной системе, чем размещение данных на локальных и портативных компьютерах или съемных носителях, где возможно хищение данных и потеря устройств.

Безопасность. «Облачные» сервисы имеют высокую безопасность при должном ее обеспечении: адекватной реализации организационных и технических мер защиты информации.

Большие вычислительные мощности позволяют значительно сократить время на реализацию информационных процессов, требующих большого количества вычислений и высокой скорости выполнения операций.

В то же время облачным технологиям свойственны определенные **недостатки**: необходимость постоянного соединения с сетью и использование систем виртуализации. Для получения доступа к услугам «облака» необходимо постоянное соединение с ИМТС. Использование систем виртуализации приводит к тому, что в качестве гипервизора применяются ядра стандартных ОС, таких, как *Linux, Windows* и др., что позволяет использовать вредоносное программное обеспечение.

В МВД России изначально крайне серьезно и комплексно подошли как к вопросам технической реализации облачных технологий, так и к вопросам обеспечения их безопасности, что было отражено в приказе МВД России от 16 января 2012 г. № 25 «Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации “облачной архитектуры”».

3.3. Общая структура ИСОД МВД России

В состав ИСОД МВД России входят следующие компоненты:

- облачная инфраструктура, состоящая из совокупности вычислительных средств обработки информации, средств хранения информации, расположенных в центрах обработки данных (СЦОД) и программно-технических комплексов единого информационного пространства (ПТК ЕИП);
- сервисы ИСОД МВД России;
- интегрированная мультисервисная телекоммуникационная сеть (ИМТС);
- автоматизированные рабочие места (АРМ) сотрудников МВД.

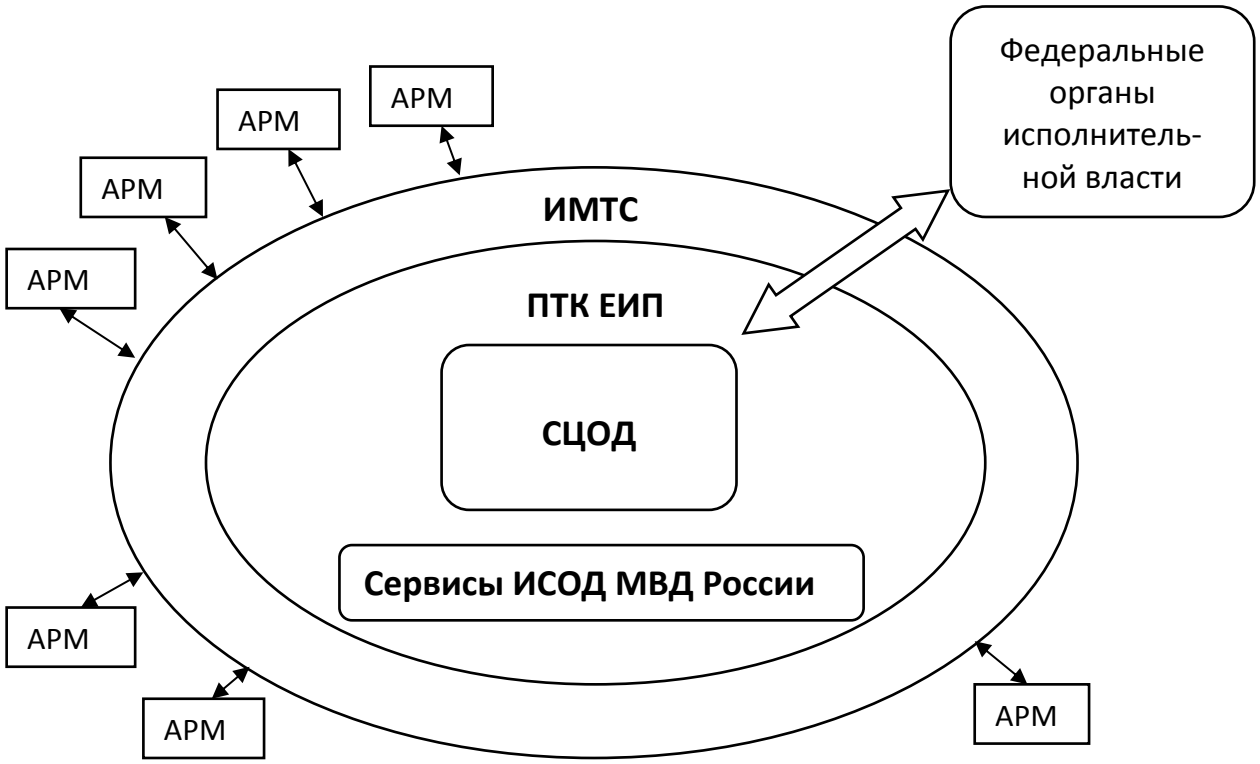


Рис. 7. Структура ИСОД МВД России

Система централизованной обработки данных

Основным элементом инфраструктуры ИСОД является система централизованной обработки данных (СЦОД).

Целями создания СЦОД МВД России явились:

- унификация используемых в МВД России программно-технических решений и приведение архитектуры основных автоматизированных информационных систем МВД России в соответствие с современными требованиями надежности функционирования и доступности данных;

•объединение разнородных данных, содержащихся в различных автоматизированных информационных системах МВД России, и обеспечение единой точки доступа к ним для использования в оперативно-служебной деятельности МВД России;

•уменьшение эксплуатационных расходов при работе автоматизированных информационных систем, используемых в МВД России, а также на поддержку информационно-технологической инфраструктуры МВД России.

Техническая архитектура СЦОД основана, как уже указывалось выше, на «облачных» технологиях.

Применяемые решения технической архитектуры обеспечивают дальнейшее развитие путем замены устаревающих компонентов более современными без кардинальной перестройки СЦОД.

В СЦОД реализована неизменность инфраструктуры для выполнения различных прикладных задач, а также возможность внедрения единой централизованной системы управления сетью и сетевой безопасностью.

Программные приложения, используемые в информационных системах подразделений МВД России в составе ИСОД, в т.ч. унаследованные из ЕИТКС, взаимодействуют между собой через централизованные общесистемные компоненты единого информационного пространства.

Межведомственное электронное взаимодействие, а также предоставление государственных услуг в электронном виде осуществляются через введенные в промышленную эксплуатацию информационно-технологические и телекоммуникационные компоненты инфраструктуры электронного правительства.

Сформированное посредством СЦОД единое информационное пространство обеспечивает надежность функционирования и масштабируемость архитектуры основных информационных систем МВД России, соответствуя при этом современным требованиям по доступности, эффективному использованию информационно-телекоммуникационной инфраструктуры, информационной безопасности и защиты информации, снижению затрат на создание, поддержку и эксплуатацию информационно-телекоммуникационной инфраструктуры, унификации решений и программно-технической платформы, возможности единой точки доступа ко всем информационным системам и информационным ресурсам МВД России. С целью обеспечения требуемой надежности и доступности информационно-телекоммуникационных услуг СЦОД создан на нескольких территориально удаленных площадках. Количество таких площадок увеличивается по мере развития ИСОД МВД России.

Для обеспечения высокой гибкости и масштабируемости работы приложений применяются технологии виртуализации, динамического увеличения

производительности в зависимости от количества одновременно работающих пользователей и обрабатывающихся запросов. При этом обеспечивается использование ведомственных информационных ресурсов исключительно сотрудниками МВД России. Унифицированные программно-технические решения обеспечивают основные направления деятельности территориальных органов МВД России, в них организовано накопление данных, формируемых в ходе повседневного исполнения сотрудниками функциональных обязанностей.

Таким образом, ИСОД МВД России представляет собой единую программно-технологическую платформу, включающую в себя набор сервисов, функционирующих на базе СЦОД, доступ к которым в рамках выполнения повседневных задач подразделениями МВД осуществляется посредством развернутой ИМТС. Все информационные системы размещаются на удаленных серверах (в облаке), и после настройки АРМ для работы в ИСОД МВД России установка дополнительного программного обеспечения для доступа к АИС не требуется. МВД России обеспечивает сопровождение работ по совершенствованию ИСОД МВД России, обновлению программного обеспечения, непрерывность функционирования системы и восстановление работы, нарушенной в результате намеренных или непреднамеренных действий.

Комплексная защита информации в СЦОД реализуется в следующих видах:

- организационная защита, основывающаяся на реализации организационных и организационно-технических мер, используемых для защиты информации;
- техническая защита, основывающаяся на использовании технических устройств, узлов, блоков, элементов, систем как в виде отдельных средств, так и встроенных в процессе единого технологического цикла создания средств обработки информации в СЦОД;
- программно-аппаратная защита, предполагающая использование соответствующего программного обеспечения, а также аппаратных устройств, встроенных в состав технических средств СЦОД.

Сервисы ИСОД

Прикладные сервисы предназначены для непосредственной работы с ними сотрудников. Причем ряд сервисов, например сервис электронного документооборота, сервис электронной почты являются общедоступными для всех сотрудников, ряд же сервисов призван обеспечивать выполнение сотрудником соответствующих служебных функций, и доступ к ним ограничен. Некоторые сервисы предполагают информационный обмен с пользователями за пределами ведомственной сети.

В соответствии с доступностью сервисы делятся на три группы:

•прикладные сервисы обеспечения повседневной деятельности;

•прикладные сервисы обеспечения оперативно-служебной деятельности;

•сервис (подсистема) поддержки взаимодействия с населением, а также межведомственного взаимодействия.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД включают в себя:

•сервис электронного документооборота (СЭД);

•сервис электронной почты (СЭП);

•ведомственный информационно-справочный портал (ВИСП);

•систему видеоконференцсвязи.

Прикладные сервисы обеспечения оперативно-служебной деятельности включают:

•информационно-поисковый сервис «Следопыт-М»;

•сервис обеспечения охраны общественного порядка (СООП);

•сервис обеспечения деятельности дежурных частей (СОДЧ);

•сервис обеспечения деятельности подразделений материально-технического обеспечения МВД (СОМТО);

•федеральную информационную систему ГИБДД (ГИБДД-М);

•сервис обеспечения экономической безопасности (СОЭБ);

•сервис НЦБ Интерпола (СОДИ);

•сервис экспертно-криминалистической деятельности (ЕАИС ЭКП);

•сервис обеспечения государственной защиты лиц (СУОГЗ);

•сервис оформления проезда сотрудников (СОПС);

•сервис ГУ собственной безопасности МВД (СОПД ГУСБ);

•сервис статистической отчетности (МОСТ);

•банк отпечатков пальцев (ЦИАДИС);

•банк данных ДНК («Ксенон-2»).

Подсистема поддержки взаимодействия с населением, а также межведомственного взаимодействия с целью предоставления госуслуг включает:

•сервис предоставления госуслуг (СПГУ);

•систему централизованного учета оружия (СЦУО);

•единый банк данных архивной информации («Ретроспектива»);

•интегрированный банк данных.

В силу того, что ИСОД МВД России является гибкой, постоянно развивающейся и модернизируемой системой, количество и наименование сервисов изменяется.

3.4. Подсистема обеспечения информационной безопасности ИСОД МВД России

В реалиях нашего времени важное место занимают вопросы обеспечения защиты информации. Особую значимость подобные вопросы приобретают при реализации таких масштабных как в географическом, так и в информационном смысле систем, как Единая информационно-аналитическая система обеспечения деятельности МВД России. В связи с этим в Министерстве были своевременно выработаны необходимые организационные и технические меры обеспечения как безопасности информации, обрабатываемой в ИСОД МВД России, так и безопасности функционирования всей системы.

На текущий момент подсистема обеспечения информационной безопасности ИСОД МВД России включает в себя широкий набор современных средств защиты информации, является централизованно управляемой и функционирует с учетом строгого протоколирования событий информационной безопасности, оперативного реагирования на инциденты информационной безопасности и систематического аудита информационной безопасности на предмет уязвимостей на всех уровнях ведомственной информационно-технологической инфраструктуры.

Состав подсистемы обеспечения информационной безопасности ИСОД МВД России включает в себя:

- средства межсетевого экранирования (МЭ);
- средства антивирусной защиты (АВЗ);
- сервис управления доступом к информационным ресурсам и системам ИСОД (СУДИС);
- средства предупреждения и обнаружения компьютерных атак (СОПКА);
- криптографическую защиту каналов связи, средства электронной подписи (ЭП);
- программно-аппаратный комплекс аутентификации и хранения ключевой информации;
- организационную защиту.

В зависимости от правового режима доступа к информации в ИСОД МВД России реализовано два контура защиты. Необходимость использования нескольких контуров защиты продиктована разными требованиями к программно-техническим средствам защиты информации, содержащей государственную тайну, и информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

3.5. Обеспечение информационной безопасности СУДИС

В рамках организации доступа сотрудников МВД России к сервисам ИСОД МВД России используется программное обеспечение сервиса управления доступом к информационным системам и ресурсам (далее – СУДИС), реализующее функции защиты от несанкционированного доступа к информации в части идентификации и строгой аутентификации пользователей в рамках делегированных прав доступа. При этом доступ к ресурсам ИСОД МВД России осуществляется на основе единственно возможной учетной записи со сложным паролем, с использованием персонального электронного идентификатора «Рутокен».

Обеспечение информационной безопасности при эксплуатации СУДИС осуществляется с применением организационных и технических мер согласно законодательству Российской Федерации в области обеспечения безопасности информации и соответствующим государственным стандартам.

Информационная безопасность в СУДИС достигается путем:

- ограничения доступа посторонних лиц в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также хранятся носители информации;
- разграничения прав доступа посредством системы идентификации и аутентификации пользователей;
- резервного копирования информации;
- защиты технических средств и носителей информации, применяемых при работе с СУДИС;
- использования защищенных каналов связи;
- применения сертифицированных программных и программно-аппаратных средств защиты информации.

При работе с СУДИС не допускается:

- покидать автоматизированное рабочее место до завершения сеанса работы с СУДИС;
- использовать доступ к информационным ресурсам и электронным базам СУДИС в целях, не связанных с выполнением служебных обязанностей;
- распространять сведения, полученные с использованием информационных ресурсов и электронных баз СУДИС, за исключением случаев, предусмотренных законодательством Российской Федерации;
- предоставлять иным лицам персональный логин и пароль для доступа к информационным ресурсам СУДИС, а также использовать их для организации сеанса работы с СУДИС иного лица.

Обязанности лиц, ответственных за поддержание работоспособности СУДИС, по соблюдению требований информационной безопасности СУДИС должны быть закреплены в их должностных регламентах (должностных инструкциях).

3.6. Средства межсетевого экранирования

При реализации прикладных сервисов ИСОД МВД России, связанных с обменом информацией с внешними сетями, – как сетями других ведомств, так и глобальной сети Интернет – первоочередное значение имеет использование средств межсетевого экранирования.

Межсетевое экранирование является одним из наиболее эффективных механизмов обеспечения информационной безопасности в распределенных вычислительных сетях, выполняющим функции разграничения информационных потоков на границе защищаемой сети. Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран,** или брандмауэр (firewall), под которым понимают программное или программно-аппаратное средство, выполняющее контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивающее защиту информационной системы посредством фильтрации информации.

Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Межсетевые экраны с фильтрацией пакетов представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы.

Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Шлюзы сеансового уровня контролируют допустимость сеанса связи, следя за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот) и определяя допустимость запрашиваемого сеанса связи. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т.е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым исключается подмена IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернете на низкоскоростных каналах, но существенно при работе во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И кроме того, брандмауэры экспертного уровня выполняют функции шлюза прикладного уровня, анализируя содержимое каждого пакета в соответствии с принятой политикой безопасности.

Применение межсетевого экрана (МЭ) позволяет опознавать известные типы атак со стороны сети, защитить любые порты системы, контролировать доступ в сеть со стороны программ. Политика доступа специфична для конкретного МЭ и определяет правила, используемые для реализации политики

доступа к сервисам. Реализуется одна из двух базовых политик: разрешить доступ для сервиса, если он явно не запрещен; запретить доступ для сервиса, если он явно не разрешен.

В соответствии с требованием нормативных документов России системы МЭ должны принимать решение на основе как минимум двух атрибутов (адрес отправителя/адрес получателя).

Межсетевые экраны, как средства защиты информации, имеют ряд недостатков:

1) МЭ не может защитить от атак, которые исходят изнутри сети;

2) МЭ не обеспечивает надежную защиту от вредоносных программ. Чтобы обеспечить эффективную защиту от вредоносных программ, необходим целый комплекс мер (как технических, так и административных), включающих установку антивирусных программ на рабочие станции и файл-серверы, обучение сотрудников и безукоризненное следование правилам обеспечения информационной безопасности в органах внутренних дел.

Для дифференциации требований к функциям безопасности межсетевых экранов выделяются шесть классов защиты межсетевых экранов. Самый низкий класс – шестой, самый высокий – первый. Межсетевые экраны, соответствующие 6-му классу защиты, применяются в государственных информационных системах 3-го и 4-го классов защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го и 4-го уровней защищенности персональных данных. Межсетевые экраны, соответствующие 5-му классу защиты, применяются в государственных информационных системах 2-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2-го уровня защищенности персональных данных.

Межсетевые экраны, соответствующие 4-му классу защиты, применяются в государственных информационных системах 1-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1-го уровня защищенности персональных данных, в информационных системах общего пользования 2-го класса.

Межсетевые экраны, соответствующие 3, 2 и 1-му классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Примененные в ИСОД МВД России средства межсетевого экранирования обеспечивают защиту прикладных сервисов по двум контурам защиты. Защиту информационных ресурсов, обрабатывающих информацию, составляющую государственную тайну, обеспечивают в составе 1-го контура защиты межсетевые экраны 1, 2 и 3-го классов защиты. Защита прикладных сервисов ИСОД МВД России с циркулирующей в них информацией ограниченного доступа, относящейся к конфиденциальной, реализована по второ-

му контуру защиты с применением средств межсетевого экранирования 4-го класса защиты.

В связи с тем, что, в соответствии со статистическими экспертными данными, большинство сетевых проблем безопасности связано с вредоносными программами, это направление защиты рассмотрено отдельно.

3.7. Антивирусная защита ИСОД МВД России

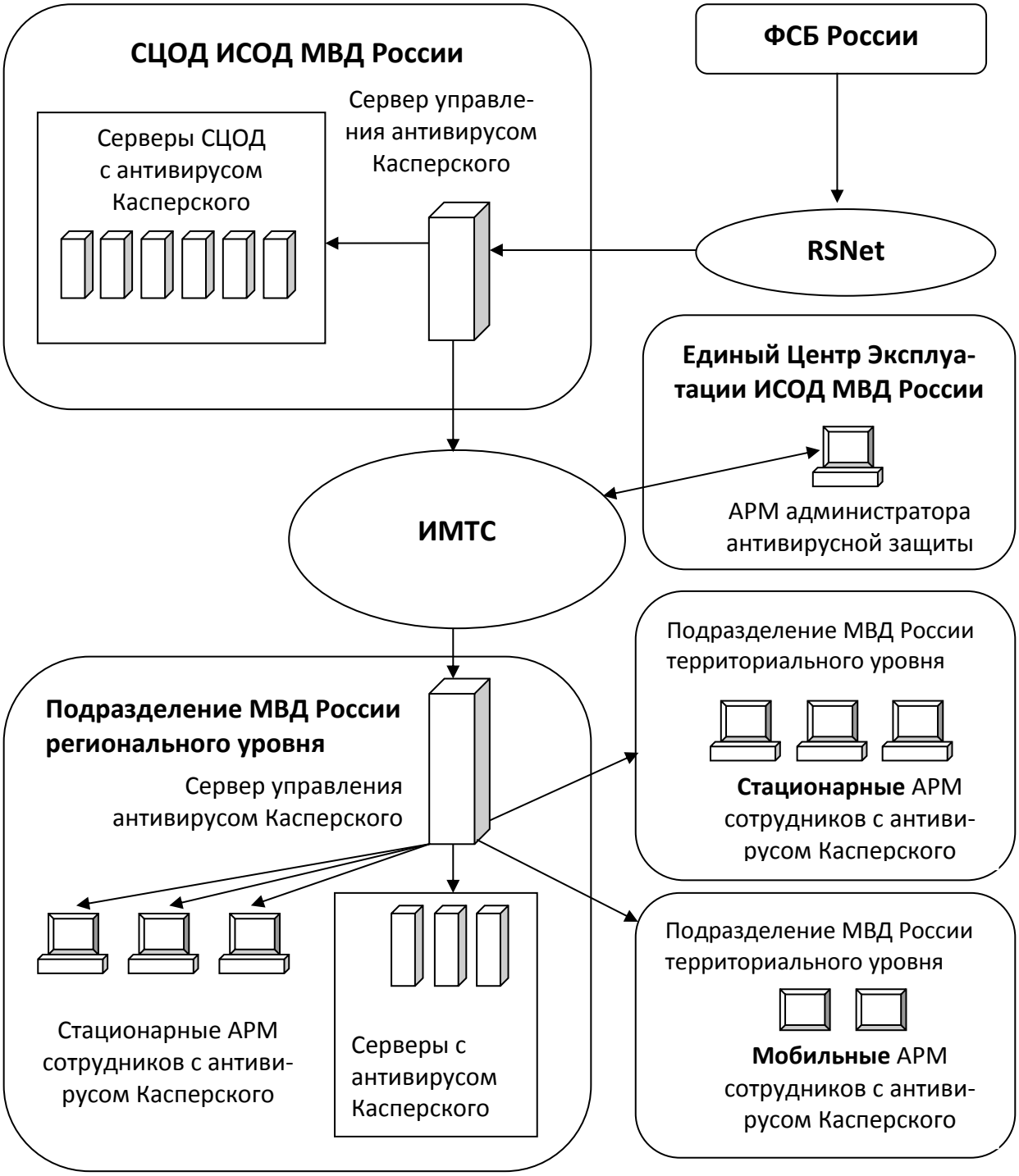


Рис. 8. Система антивирусной защиты информации ИСОД МВД России

Результаты ведомственного мониторинга и исследований показали, что наиболее актуальной угрозой информационной безопасности для МВД России является проникновение в информационные системы вредоносного кода. В целях минимизации этой категории угроз в рамках подсистемы обеспечения информационной безопасности ИСОД МВД России сформирована масштабная технологическая инфраструктура антивирусной защиты на базе программного обеспечения Kaspersky.

В составе инфраструктуры антивирусной защиты в «облачных компонентах» ИСОД МВД России (в т.ч. в 96 территориальных органах МВД России на региональном уровне) развернута иерархическая система серверов антивирусной защиты, управляемая головным компонентом системы – сервером управления, мониторинга и обновления вирусных баз клиентского ПО Kaspersky (далее – управляющий сервер), размещенным на технологической площадке СЦОД.

Во всех подразделениях центрального аппарата и территориальных органах МВД России организовано автоматическое получение обновлений средств антивирусной защиты и баз вирусных сигнатур с управляющего сервера, получающего в автоматическом режиме доверенным способом обновления баз вирусных сигнатур с антивирусного портала ФСБ России.

Средства антивирусной защиты ИСОД МВД России в обязательном порядке должны удовлетворять требованиям, регламентированным нормативными документами ФСТЭК России, классифицирующими защищенность средств антивирусной защиты информации на шесть уровней *(рис. 9)*.

Защита систем, в которых обрабатывается информация, содержащая сведения, отнесенные к государственной тайне, обеспечивается средствами антивирусной защиты 3, 2 и 1-го классов. В ИСПДн для обеспечения 3-го и 4-го уровней защищенности персональных устанавливаются средства антивирусной защиты 6-го класса. Обеспечение 1-го и 2-го уровней защищенности персональных данных обеспечивается применением средств антивирусной защиты 4-го и 5-го классов защиты соответственно. Защиту государственных информационных систем при отсутствии сведений, составляющих государственную тайну, обеспечивают средства антивирусной защиты 4-го класса защиты. Для систем общего пользования 2-го класса применяют средства антивирусной защиты 4-го класса.

В ИСОД МВД России средства антивирусной защиты, так же как и в случае МЭ, обеспечивают защиту по двум контурам защиты. Защиту информационных ресурсов, обрабатывающих информацию, составляющую государственную тайну, обеспечивают в составе 1-го контура защиты антивирусы 1, 2 и 3-го классов защиты. Защиту информационных ресурсов ИСОД МВД России, обрабатывающих информацию, не содержащую сведе-

ния, отнесенные к государственной тайне, обеспечивают антивирусные средства 4-го класса защиты, включенные во второй контур защиты.

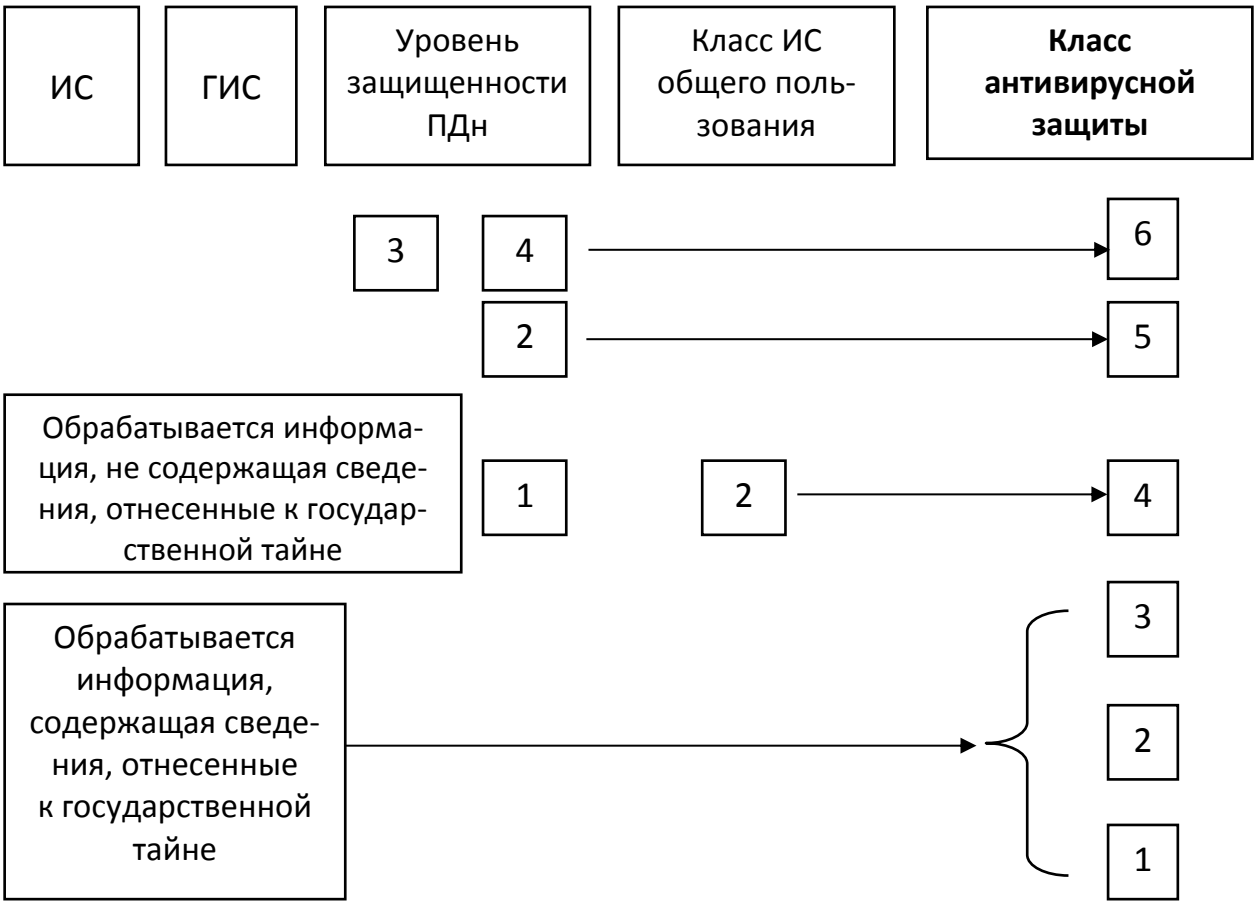


Рис. 9. Классы защиты антивирусов

В ИСОД МВД России средства антивирусной защиты, также как и в случае МЭ, обеспечивают защиту по двум контурам защиты. Защиту информационных ресурсов, обрабатывающих информацию, составляющую государственную тайну, обеспечивают в составе 1-го контура защиты антивирусы 1, 2 и 3-го классов защиты. Защиту информационных ресурсов ИСОД МВД России, обрабатывающих информацию, не содержащую сведения, отнесенные к государственной тайне, обеспечивают антивирусные средства 4-го класса защиты, включенные во второй контур защиты.

В настоящее время к указанной системе подключено более 150 тысяч пользовательских АРМ и серверного оборудования. Благодаря принятым техническим мерам и своевременному реагированию на инциденты, в настоящее время общее количество вирусных заражений АРМ, имеющих подключение к ИСОД МВД России, с показателей, характерных для периода 2014-2016 гг., снизилось более чем на порядок.

3.8. Система предупреждения и обнаружения компьютерных атак МВД России (СОПКА)

Важным компонентом подсистемы информационной безопасности ИСОД МВД России является система предупреждения и обнаружения компьютерных атак (СОПКА).

Система предупреждения и обнаружения компьютерных атак – программное либо программно-аппаратное средство, предназначенное для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность информационной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к банкам данных, а также действия вредоносного программного обеспечения.

Классическая архитектура системы обнаружения вторжений (компьютерных атак) включает в себя *(рис. 10):*

- сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;
- подсистему анализа, предназначенную для выявления атак и подозрительных действий;
- хранилище, обеспечивающее накопление первичных событий и результатов анализа;
- консоль управления, позволяющую конфигурировать систему обнаружения компьютерных атак, наблюдать за состоянием защищаемой системы, просматривать выявленные подсистемой анализа инциденты.

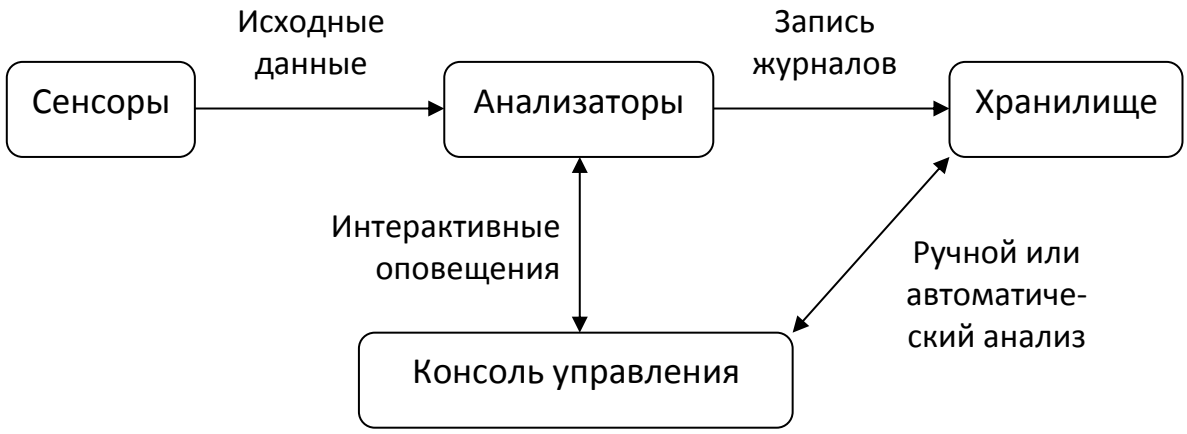


Рис. 10. Классическая архитектура системы обнаружения вторжений

Система предупреждения и обнаружения компьютерных атак МВД России имеет разветвленную структуру и состоит из следующих компонентов *(рис. 11):*

•Ведомственного центра мониторинга (ВЦМ СОПКА ОВД), подключенного к ГЦМ ФСБ России;

•узлов системы предупреждения и обнаружения компьютерных атак, подключаемых к ВЦМ СОПКА ОВД.

Ведомственный центр мониторинга системы предупреждения и обнаружения компьютерных атак МВД России функционирует на базе ведомственной СЦОД и охватывает объекты каждого из четырех уровней управления системы ОВД: Первым является само МВД и его центральный аппарат, второй – Главные управления по федеральным округам, третий – региональные главки, управления полиции на транспорте и подразделения МВД на закрытых территориях и режимных объектах. Последний, низовой уровень – районные отделы полиции.

Система предупреждения и обнаружения компьютерных атак ИСОД МВД России состоит из трех подсистем:

•подсистемы взаимодействия с Главным центром мониторинга (ГЦМ) ФСБ России;

•подсистемы мониторинга компьютерных атак;

•специального оборудования.

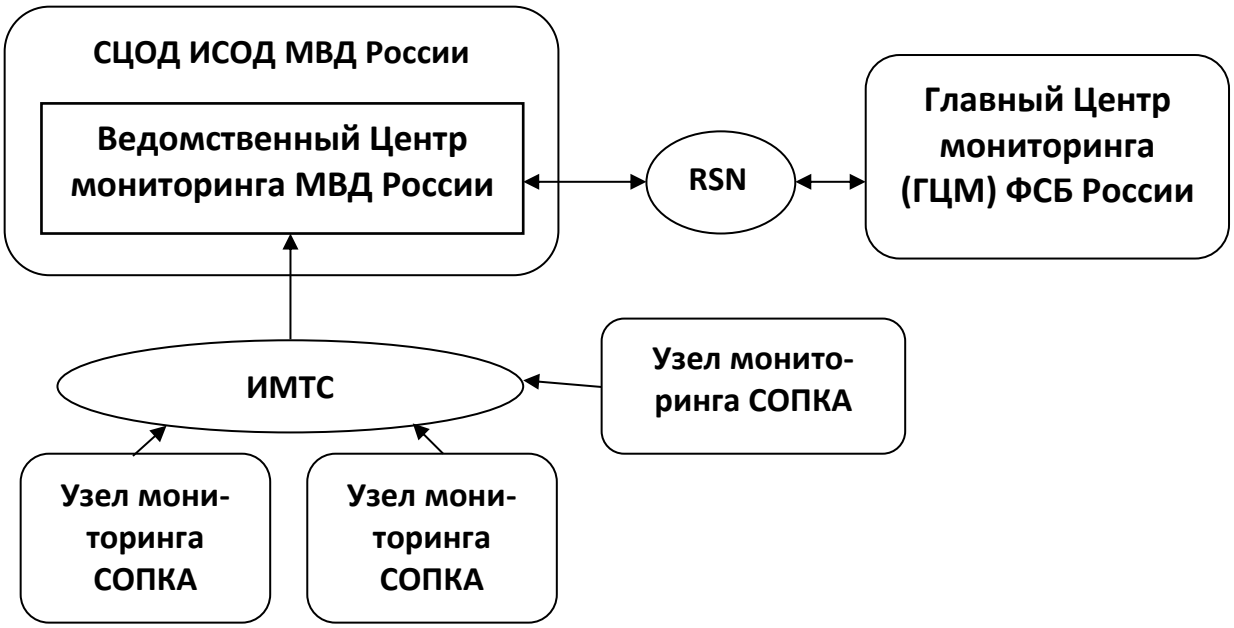


Рис. 11. Структура СОПКА МВД России

Подсистема взаимодействия с Главным центром мониторинга ФСБ России предназначена для обеспечения выполнения следующих задач:

1) передача по криптографически защищенному каналу связи статистических данных об обнаружении компьютерных атак на узлах СОПКА ОВД в согласованном формате и предусмотренные регламентом периоды;

2) доведение информации о возможных компьютерных атаках на объектах эксплуатации в ГЦМ ФСБ России;

3) направление в ГЦМ ФСБ России запросов о проведении экспертизы критических событий (действий компьютерных атак, в результате которых нанесен или может быть нанесен значительный ущерб информационным ресурсам ОВД);

4) получение из ГЦМ ФСБ России базы решающих правил.

Подсистема мониторинга компьютерных атак включает следующие компоненты:

- компоненты анализа событий и распознавания компьютерных атак (анализаторы);
- средства организации взаимодействия компонентов;
- хранилище данных подсистемы мониторинга компьютерных атак;
- консоль управления;
- компонента архивирования текущего журнала компьютерных атак;
- компонента печати на бумажном носителе отчета о проведении компьютерных атак.

Специальное оборудование предназначено для взаимодействия элементов СОПКА, хранения, отображения и защиты данных системы.

В состав специального оборудования входят компоненты регистрации событий (сенсоры), предназначенные для обнаружения компьютерных атак в заданном сегменте и/или узлах сети объекта ОВД.

Основным методом обнаружения атак является анализ трафика на соответствие анализируемой информации набору сигнатур. Анализаторы сетевого трафика реализованы в виде подключаемых модулей. Предусмотрена возможность анализа на предмет атаки как входящего, так и исходящего трафика. Анализу подвергается трафик протоколов TCP, IP, UDP, ICMP, ARP, вместе с тем проводится анализ в ряде сегментов сети на предмет попыток атак сетевых пакетов протоколов прикладного уровня (FTP, telnet и т.д.).

При обнаружении компьютерной атаки система уведомляет администратора безопасности информации об атаке практически в режиме реального времени. Система сохраняет все данные, по которым было принято решение об атаке, для проведения дальнейшего анализа.

Также в системе предусмотрена возможность регистрации событий с возможностью сортировки информации по адресу источника (инициатора), получателя (цели) и типу события.

Таким образом, система обнаружения и предупреждения компьютерных атак МВД России отличается высокой степенью взаимодействия с ФСБ России и обеспечивает:

•выявление компьютерных атак в сетях объектов ОВД, построенных на базе протоколов TCP/IP разных уровней управления МВД России на основе баз решающих правил;

•автоматизированное получение обновлений баз решающих правил из ГЦМ ФСБ России и доверенную доставку обновлений на объекты ОВД разных уровней управления МВД России;

•взаимодействие с ГЦМ ФСБ России с целью передачи статистической информации и информации об обнаруженных компьютерных атаках.

Используемые в МВД России средства обнаружения компьютерных атак, включая требования по контролю отсутствия недекларированных возможностей, в обязательном порядке должны соответствовать следующим руководящим документам: «Требования к программным, программно-аппаратным или аппаратным средствам обнаружения компьютерных атак» ФСБ России и «Требования к системам обнаружения вторжений» (утв. приказом ФСТЭК России от 06.12.2011 № 638) ФСТЭК России.

Приказом ФСТЭК устанавливается шесть профилей защиты для двух типов средств обнаружения компьютерных атак – уровня сети и уровня узла. Профили защиты для 4, 5 и 6-го классов обоих типов содержатся на сайте ФСТЭК России (за исключением систем обнаружения вторжений 1, 2 и 3-го классов, предназначенных для защиты информации, содержащей сведения, отнесенные к государственной тайне).

Системы обнаружения вторжений 6, 5 и 4-го классов применяются в информационных системах персональных данных. Системы обнаружения вторжений 3, 2 и 1-го классов защиты применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Комплексные решения, реализованные в системе предупреждения и обнаружения компьютерных атак, унифицированы в рамках ИСОД МВД России и учитывают базовую модель нарушителя и модель угроз единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) с учетом «облачной архитектуры».

3.9. Средства криптографической защиты ИСОД МВД России

Для создания защищенной транспортной среды передачи данных на всех уровнях технологической инфраструктуры ИСОД МВД России сформирована сеть конфиденциальной связи с использованием программных средств криптографической защиты конфиденциальной информации (СКЗИ), а также программно-аппаратных СКЗИ.

Основой криптографической защиты ведомственной сети конфиденциальной связи является технология VPN.

VPN (*Virtual Private Network* – виртуальная частная сеть) – логическая сеть, создаваемая поверх другой сети. Несмотря на то, что коммуникации осуществляются по публичным неконтролируемым сетям с использованием небезопасных протоколов, за счет шифрования создаются закрытые каналы обмена информацией.

С помощью метода туннелирования пакеты данных транслируются через общедоступную сеть, как и в случае обычного двухточечного соединения. Между каждой парой «отправитель-получатель данных» устанавливается «туннель» – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого. Таким образом, организацию виртуальной частной сети можно сравнить с прокладкой защищенного кабеля через глобальную сеть.

Основными компонентами туннеля являются:

- инициатор;
- маршрутизируемая сеть;
- туннельный коммутатор;
- один или несколько туннельных терминаторов.

Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате решается проблема взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации.

Таким образом, VPN состоит из двух частей: «внутренней» (подконтрольной) сети и «внешней» сети, по которой проходит инкапсулированное соединение.

В ИСОД МВД России VPN-каналы используются в нескольких направлениях, во многом определяющих техническую реализацию каналов:

1) для объединения в единую защищенную сеть региональных частей ИМТС, обменивающихся данными по открытым каналам связи;

2) для обмена информацией с подключенными к ведомственным информационным ресурсам «внешними» пользователями (реализация межведомственного взаимодействия);

3) для создания защищенного канала между сегментом ведомственной сети и сотрудником, который, осуществляя служебную деятельность, подключается к ведомственным ресурсам с портативного ПК (ноутбука, планшета, смартфона).

Инфраструктура ИСОД МВД России территориально распределена, поэтому на базе ИМТС МВД России сформирована VPN-сеть с использованием криптографических средств линейки ViPNet.

Таким образом, во всех территориальных органах МВД России:

- организован защищенный VPN-канал до ЦОД МВД России;
- развернуты центры управления региональными защищенными сетями;
- созданы региональные защищенные VPN-каналы.

В ИСОД МВД России сеть конфиденциальной связи реализована на основе:

- программных СКЗИ *(ViPNetAdministrator, ViPNetStateWatcher, ViPNetClient),*
- программно-аппаратных СКЗИ *(ViPNetCoordinatorHW 1000, ПАК ViPNet, Coordinator HW 2000).*

Как мы видим, существующая сетевая инфраструктура МВД использует VPN как с помощью программного, так и с помощью программно-аппаратного обеспечения. Реализация VPN, осуществляемая при помощи специальных комплексов программно-аппаратных средств, обеспечивает наиболее высокую производительность и степень защищенности.

Подключение удаленных пользователей к VPN производится посредством СУДИС. При подключении удаленного пользователя (либо при установке соединения с другой защищенной сетью) сервер доступа СУДИС требует прохождения процесса авторизации. После успешного прохождения процесса удаленный пользователь наделяется полномочиями для работы в сети в соответствии с установленными разрешениями.

3.10. Электронная подпись и идентификация в ИСОД МВД России

Электронная подпись (ЭП) представляет собой комбинацию символов, которая формируется в результате математического преобразования исходного документа при помощи специального программного обеспечения. ЭП добавляется к исходному документу при пересылке, и любое изменение исходного документа делает эту ЭП недействительной. ЭП является уникальной для каждого документа, и невозможность подделки ЭП обеспечивается беспредельно высоким количеством математических вычислений, необходимых для ее подбора.

Таким образом, ЭП безошибочно указывает на подлинность и авторство, не переносится с одного документа на другой документ, защищает подписанный документ от подделки, а также от изменения или искажения информации (целостность) и несет принцип неотрекаемости, что предотвращает

отказ от авторства. ЭП позволяет убедиться в том, что после подписи документа конкретным человеком документ не изменялся, проверяет надежность отправителя электронного документа и сохранность содержания документа, однозначно определяет автора электронного документа и указывает дату подписания.

Электронная подпись основана на асимметричном криптографическом алгоритме. Особенностью такого алгоритма является то, что используются два разных ключа. Первый ключ является секретным (личным) – закрытым ключом, он известен только лицу, подписывающему документ. Второй (открытый, несекретный) ключ может быть известен любому получателю электронного документа. Оба этих ключа создаются с помощью специальной криптографической программы (в ИСОД МВД России – «КриптоПро CSP»).

Сначала создается закрытый ключ, затем на основании закрытого ключа создается открытый ключ. Подбор закрытого ключа по открытому ключу невозможен. Открытый ключ публикуется на сайте удостоверяющего центра, услугами которого пользуется владелец ключа. Закрытый ключ владелец электронной подписи хранит со всеми необходимыми мерами предосторожности.

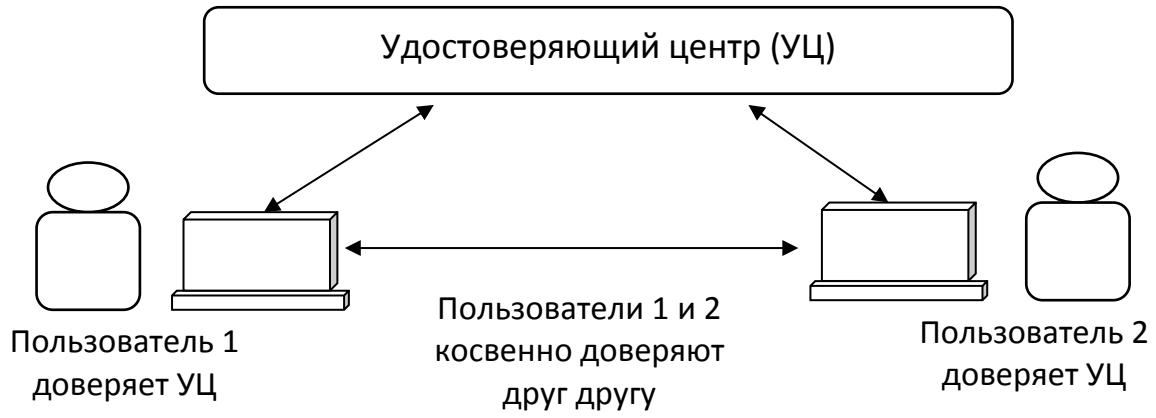


Рис. 12. Роль удостоверяющего центра

В области применения ЭП удостоверяющий центр выполняет такую же роль, как нотариус в жизненном цикле взаимодействия юридических или физических лиц, для которых необходимо убедиться в подлинности документа, подписанного владельцем *(рис. 12).*

Удостоверяющий центр (УЦ) является системой управления ключами в рамках криптографической системы на основе *инфраструктуры открытых ключей* (англ. *PKI*). Удостоверяющий центр создает сертификат открытого ключа и таким образом удостоверяет этот ключ, подтверждает или опровергает принадлежность открытого ключа лицу, которое владеет соответствующим закрытым ключом.

Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

Для того чтобы закрытым ключом мог воспользоваться только владелец подписи, он записывается на съемный носитель ключа (в системе МВД России – «Рутокен»). Для дополнительной защиты носитель снабжают PIN-кодом и, соответственно, перед тем, как воспользоваться ключом для создания электронной подписи, необходимо ввести правильное значение PIN-кода.

Процедура электронной подписи документов происходит следующим образом:

1. Программа преобразует исходный текст документа в набор символов (контрольная сумма – хэш-функция), который точно соответствует тексту документа. Если документ будет изменен, то контрольная сумма тоже изменится.

2. Затем полученная контрольная сумма шифруются закрытым ключом отправителя.

3. Вместе с электронным документом отправляются контрольная сумма и открытый ключ отправителя.

4. Когда электронный документ получен, программа получателя берет открытый ключ отправителя, присланный с письмом, и с его помощью расшифровывает полученную контрольную сумму.

5. Затем программа генерирует контрольную сумму для текста письма и сверяет обе контрольные суммы. Если присланная контрольная сумма и вторично полученная программой контрольная сумма совпадают, значит, письмо не изменялось.

Таким образом, процедура проверки подлинности ЭП при обработке документов определяет целостность электронного документа и авторизацию владельца сертификата, т.е. ЭП подлинна (проверка подписи по действующему стандарту – ГОСТу Р 34.10–2012 прошла успешно), владелец сертификата имел право подписывать документ (сертификат вступил в силу, не просрочен, не отозван, содержит необходимые идентификаторы).

Приказом МВД России от 28.05.2013 № 294 введена в эксплуатацию Система удостоверяющих центров органов внутренних дел Российской Федерации (СУЦ ОВД).

Основными задачами СУЦ ОВД являются:

1. Обеспечение сотрудников ОВД средствами ЭП, в т.ч. квалифицированными сертификатами ключей проверки электронной подписи (сертификат).

2. Обеспечение проверки ЭП электронного документа и статуса (действительности) сертификатов ключей проверки ЭП пользователей.

3. Реализация в СУЦ ОВД методов по обеспечению функционирования средств защиты информации от несанкционированного доступа с целью осуществления сохранности конфиденциальной информации, обрабатываемой в СУЦ ОВД.

4. Обеспечение возможности реализации механизмов строгой аутентификации при доступе пользователей к информационным ресурсам.

5. Обеспечение возможности формирования ЭП электронного документа в целях подтверждения его целостности и авторства и обеспечения юридической значимости.

6. Выполнение процедур по разрешению конфликтных ситуаций, возникающих при использовании средств ЭП.

СУЦ, таким образом, составляет основу инфраструктуры открытых ключей (PKI) в ОВД. В рамках СУЦ обеспечивается контроль выполнения всех процедур, связанных с ключами и цифровыми сертификатами открытых ключей.

Одной из основных целей создания и развития ИСОД МВД России являлось обеспечение разграниченного доступа к информационным ресурсам.

В ИСОД МВД России реализована единая политика информационной безопасности, которая обеспечивает санкционированный доступ сотрудников ОВД к информационным системам и ресурсам с автоматизированных рабочих мест и осуществляет контроль и анализ произведенных ими действий.

Для обеспечения санкционированного доступа к сервисам ИСОД на сотрудника заводится учетная запись пользователя для авторизации в системе по логину и паролю. Создание, изменение и блокирование учетной записи пользователей осуществляется при помощи сервиса управления доступом к информационным системам и ресурсам ИСОД МВД России (СУДИС). СУДИС является одним из ключевых элементов подсистемы информационной безопасности ИСОД МВД России.

Основным механизмом доступа к сервисам ИСОД МВД России (кроме сервиса электронной почты) является реализация процедуры авторизации пользователя с использованием ЭП. Использование процедуры авторизации пользователя по логину и паролю допускается при первичной регистрации в системе и временном отсутствии возможности получения сотрудником ЭП.

Технически доступ к ресурсам ИСОД МВД России осуществляется на основе единственно возможной учетной записи с использованием персонального электронного идентификатора «Рутокен».

«Рутокен» предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования, ключей электронной подписи, цифровых сертификатов и других данных, а также для выполнения шифрования и электронной подписи.

Аппаратная реализация национальных стандартов электронной подписи, шифрования и хэширования позволяет использовать персональный электронный идентификатор «Рутокен» в качестве интеллектуального ключевого носителя и средства электронной подписи в российских системах PKI, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной подписи. Персональный электронный идентификатор «Рутокен» позволяет выполнять криптографические операции таким образом, что закрытая ключевая информация никогда не покидает пределы токена. Таким образом, исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.

После получения учетной записи и «Рутокена» с сертификатом проверки электронной подписи сотрудник проходит процедуру идентификации и аутентификации на портале СУДИС. Это делается для того, чтобы привязать полученный сертификат ЭП к своей учетной записи путем загрузки его в хранилище СУДИС.

После проведения процедуры привязки сертификата ЭП к учетной записи становится возможным осуществлять вход в систему и на сервисы ИСОД МВД России без дополнительного ввода логина и пароля. При необходимости временно покинуть рабочее место блокировка АРМ производится автоматически путем извлечения идентификатора «Рутокен».

Таким образом, использование «Рутокена» с записанным на него сертификатом проверки ЭП обеспечивает санкционированный доступ сотрудника ОВД к сервисам ИСОД МВД России, идентифицирует его в сети информационной системы МВД в любой географической точке России с доступом в ИСОД, являясь, по сути, электронным аналогом служебного удостоверения сотрудника ОВД.

3.11. Интегрированная мультисервисная телекоммуникационная сеть

Интегрированная мультисервисная телекоммуникационная сеть МВД России (ИМТС) является информационной средой размещения программных средств, данных и сервисов, образующих ИСОД МВД России.

Целью создания ИМТС являлась интеграция имеющихся ресурсов связи, достигнутая в первую очередь на уровне первичной сети за счет объединения потоков информации всех видов для передачи по общему цифровому каналу на основе коммутационного оборудования с функциями IP/MPLS.

ИМТС объединяются по протоколу TCP/IP по собственным (принадлежащим МВД России) или арендованным каналам связи сторонних собственников, например «Ростелекома».

Группа протоколов TCP/IP – набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет. Название TCP/IP происходит из двух важнейших протоколов семейства – *Transmission Control Protocol (TCP) и Internet Protocol (IP),* которые были разработаны и описаны первыми в данном стандарте. Имеют историческое происхождение от сети ARPANET из 1970-х гг. (под управлением DARPA, Министерства обороны США).

TCP ответственен за разбивку сообщения на пакеты данных и соединение их в конечном пункте отправки. IP отвечает за передачу (с контролем получения) отдельных пакетов.

Уровни протоколов TCP/IP расположены по принципу стека (англ. *stack* – стопка). Это означает, что протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы инкапсуляции. Например, протокол TCP работает поверх протокола IP.

Основной для передачи данных в ИМТС является технология MPLS (канальный уровень эталонной модели OSI).

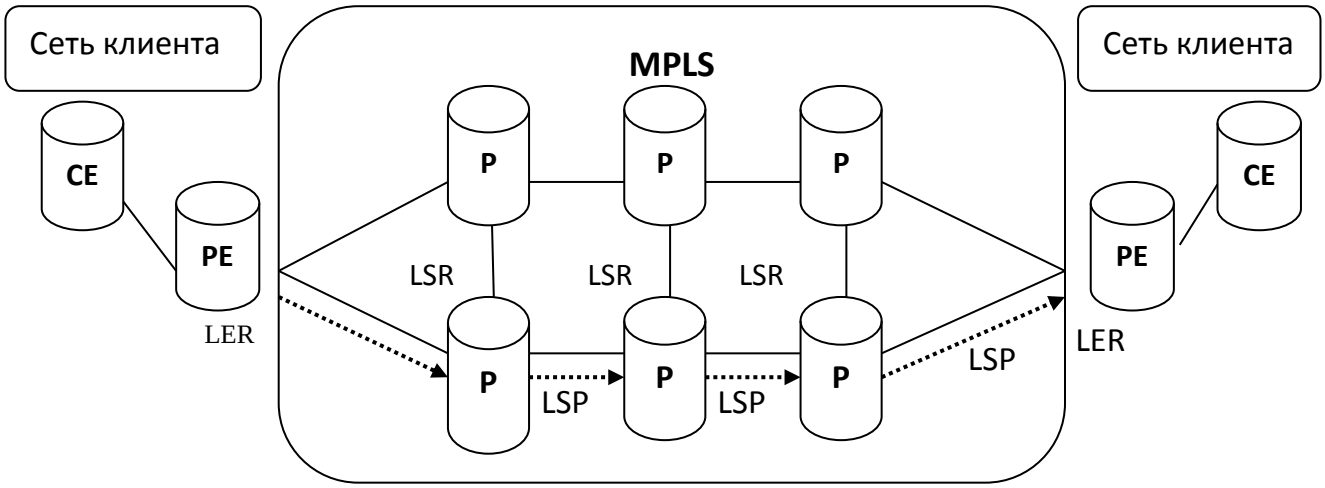
MPLS (англ. *multiprotocol label switching* — многопротокольная коммутация по меткам) – механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток.

MPLS является масштабируемым и не зависимым от каких-либо протоколов механизмом передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счет этого возможно создание сквозного виртуального канала, не зависимого от среды передачи и использующего любой протокол передачи данных *(рис. 13).*

В качестве LSR *(Label Switch Routers)* применяются коммутирующие P-маршрутизаторы (маршрутизаторы провайдеров), которые совмещают в себе функции маршрутизатора IP и коммутатора. P-маршрутизаторы определяют топологию сети, строят свои таблицы коммутации меток, выбирают эффективные пути следования пакетов и, кроме того, обеспечивают коммутирование трафика по меткам и таблицам коммутации.

Порядок назначения IP-адресов в сети ИМТС определяется требованиями приказа МВД России от 23 сентября 2015 г. № 926 «Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации» (в ред. приказа МВД России от 01.12.2016 № 784, от 28.12.2016 № 914 дсп). Выделение IP-адресов ИМТС для территориальных органов

МВД России и технологических IP-адресов для телекоммуникационного оборудования осуществляется подразделениями информационных технологий, связи и защиты информации территориальных органов МВД России с учетом требований функционирования специализированных аппаратно-программных комплексов и топологии сети. Подразделения информационных технологий, связи и защиты информации территориальных органов МВД России при обосновании потребности запрашивают дополнительные IP-адреса у главного администратора ИМТС.



CE – граничный маршрутизатор сети клиента
PE – граничный маршрутизатор провайдера
P – маршрутизаторы провайдера
LER – метка граничного маршрутизатора провайдера
LSR – метка коммутирующего маршрутизатора
LSP – метки пути переключений

Рис. 13. Сеть, основанная на технологии MPLS

Для повышения качества информационного сопровождения повседневной и оперативно-служебной деятельности должностных лиц ОВД РФ предусмотрено внедрение мобильных устройств в интегрированную мультисервисную телекоммуникационную сеть с обязательным обеспечением безопасности передачи информации.

Доступ пользователей к ресурсам централизованных информационных систем МВД России теоретически возможен как с автоматизированных рабочих мест, так и с ведомственных мобильных устройств.

Со стационарных автоматизированных рабочих мест доступ осуществляется по проводным каналам, с ведомственных мобильных устройств – по спутниковому либо беспроводному каналам *(рис. 14).*

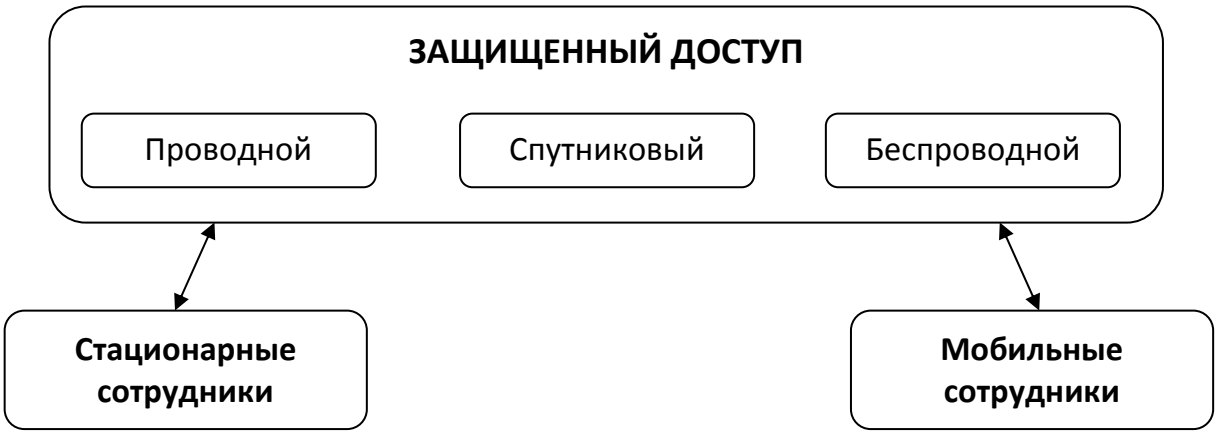


Рис. 14. Виды защищенного доступа, реализуемые ИМТС

Одной из задач, решаемых Интегрированной мультисервисной телекоммуникационной сетью (ИМТС), является обеспечение мобильного доступа к сервисам ИСОД МВД России сотрудников ОВД, входящих в состав нарядов патрульно-постовой службы полиции, дорожно-патрульной службы ГИБДД МВД России и участковых уполномоченных полиции, к информационным ресурсам системы. С этой целью используются 3G/4G/5G-сети операторов связи либо системы спутниковой связи, а также доступ к ГЛОНАСС или GPS.

При реализации защищенного доступа подсистема информационной безопасности ИСОД обеспечивает защиту информации на всех технологических стадиях и уровнях ее обработки, используя при этом шифрование протоколов передачи данных, защиту на уровне операционных систем, баз данных и приложений.

Для обеспечения передачи информации ограниченного доступа необходимо использовать специализированную операционную систему для мобильных устройств, с обязательным включением таких элементов защиты, как скремблирование, криптографическая защита, антивирусное программное обеспечение, а также проверка целостности аппаратной и программной части.

В настоящее время активно ведутся работы по созданию защищенной ОС для мобильных устройств, функционально аналогичной операционной системе *Android.* В плане защиты информации в устройствах на *Android* на сегодняшний день существует несколько существенных проблем, основной из которых является особенность самой разрабатываемой ОС: отсутствие обновлений и, как следствие, возрастание угрозы применения новых и модифицированных вредоносных программ, использующих необнаруженные уязвимости операционной системы.

Заключение

Актуальность проблемы обеспечения информационной безопасности органов внутренних дел вызвана целым рядом взаимосвязанных факторов, большинство из которых являются следствием процесса информатизации и становления информационного общества.

Органы внутренних дел МВД России, являясь основой противодействия информационным посягательствам криминальных сообществ на права и свободы граждан, безопасность государства, общества и личности, все активнее применяют в своей деятельности новейшие информационные технологии высокой сложности. Качественно улучшенная эффективность информационного обеспечения деятельности в органах внутренних дел создала и целый комплекс проблем обеспечения ведомственной информационной безопасности. Этому способствовали и высокая уязвимость инфраструктуры в силу сложности используемых систем, и появление дополнительных угроз, связанных с внедрением новых технологий, и стремительный прогресс в развитии технических средств разведывательного назначения. МВД России в создавшихся условиях ведет целенаправленную активную работу по всем основным направлениям обеспечения информационной безопасности:

- совершенствуется нормативно-правовая база в области защиты информации;
- тщательно прорабатываются организационные меры по защите информации и ведомственных объектов информатизации;
- широко внедряются отечественные технические, программные, программно-аппаратные и криптографические средства защиты информации.

Комплекс реализованных мер позволил МВД России построить к настоящему времени одну из самых масштабных информационных систем, реализованную с применением новейших информационных технологий и обеспечивающую высокую степень защиты как самой системы, так и обрабатываемой в ней информации и всей ведомственной информационной инфраструктуры.

Основным проблемным звеном, пока не позволяющим реализовать все преимущества созданной единой системы информационно-аналитического обеспечения деятельности МВД России, на данный момент является ее транспортная сеть. Необходимо существенное увеличение пропускной способности ИМТС, т.к. возрастающая из года в год активность пользователей сервисов ИСОД МВД России и увеличение потоков передаваемых данных предъявляет все более высокие требования к каналам передачи данных.

С переходом в ближайшей перспективе к отечественному программному обеспечению качественно решится еще одна проблема информационной безопасности, связанная с угрозой использования недекларированных возможностей зарубежного программного обеспечения и аппаратных компонентов.

Список литературы

1. О безопасности [Электронный ресурс]: федеральный закон от 28.12.2010 № 390-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. О государственной тайне [Электронный ресурс]: федеральный закон от 21 июля 1993 г. № 5485-1 (в ред. федер. закона от 21 декабря 2013 г. № 377-ФЗ). Доступ из справ.-правовой системы «КонсультантПлюс».

3. О персональных данных [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 152-ФЗ (действ. ред. 2016). Доступ из справ.-правовой системы «КонсультантПлюс».

4. О связи [Электронный ресурс]: федеральный закон от 07.07.2003 № 126-ФЗ (в ред. федер. закона от 06.07.2016 № 374-ФЗ). Доступ из справ.-правовой системы «КонсультантПлюс».

5. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 149-ФЗ (действ. ред. 2016). Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об электронной подписи [Электронный ресурс]: федеральный закон от 6 апреля 2011 г. № 63-ФЗ (в ред. федер. закона от 2 июля 2013 г. № 185-ФЗ). Доступ из справ.-правовой системы «КонсультантПлюс».

7. О стратегии национальной безопасности Российской Федерации до 2020 года [Электронный ресурс]: Указ Президента РФ от 12 мая 2009 г. № 537 (ред. от 01.07.2014). Доступ из справ.-правовой системы «КонсультантПлюс».

8. Перечень сведений конфиденциального характера: утв. Указом Президента РФ от 6 марта 1997 г. № 188 (в ред. указов Президента Российской Федерации от 23.09.2005 № 1111, от 13.07.2015 № 357) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Государственная программа Российской Федерации «Информационное общество (2011-2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 15.04.2014 № 313 (ред. от 21.10.2016) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности [Электронный ресурс]: постановление Правительства Российской Федерации от 03.11.1994 № 1233 (ред. от 18.03.2016). Доступ из справ.-правовой системы «КонсультантПлюс».

11. Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности [Электронный ресурс]: постановление Правительства Российской Федерации от 04.09.1995 № 870 (ред. от 18.03.2016). Доступ из справ.-правовой системы «КонсультантПлюс».

12. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства Российской Федерации от 01.11.2012 № 1119. Доступ из справ.-правовой системы «КонсультантПлюс».

13. ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (введ. 01.01.2013) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

14. Защита информации. Основные термины и определения: ГОСТ Р 50922–2006 «Национальный стандарт Российской Федерации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 28.01.2014 № 3-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

15. Концепция создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012-2014 гг.: приказ МВД России от 30 марта 2012 г. № 205.

16. О внесении изменений в приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» [Электронный ресурс]: приказ МВД России от 15.07.2013 № 538 (зарег. в Минюсте России 16.09.2013 № 29960). Доступ из справ.-правовой системы «КонсультантПлюс».

17. О мерах по обеспечению режима секретности в органах внутренних дел Российской Федерации: приказ МВД России от 11.03.2012 № 015. М.: МВД России, 2012. 249 с.

18. О некоторых вопросах обработки персональных данных в МВД России [Электронный ресурс]: приказ МВД России от 29 декабря 2016 г. № 925. Доступ из справ.-правовой системы «КонсультантПлюс».

19. О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России [Электронный ресурс]: приказ МВД России от 09.11.2018 № 755. Доступ из справ.-правовой системы «КонсультантПлюс».

20. О некоторых мерах, направленных на обеспечение выполнения МВД России обязанностей, предусмотренных Федеральным законом от 27.07.2006

№ 152-ФЗ «О персональных данных» [Электронный ресурс]: приказ МВД России от 21 декабря 2017 г. № 949. Доступ из справ.-правовой системы «КонсультантПлюс».

21. Об упорядочении организации и проведении мероприятий по технической защите информации в ОВД РФ: указание МВД России от 10.03.2015 № 1/176 дсп. М.: МВД России, 2015. 23 с.

22. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 06.07.2012 № 678 (ред. от 20.04.2015). Доступ из справ.-правовой системы «КонсультантПлюс».

23. Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры»: приказ МВД России от 16 января 2012 г. № 25.

24. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14 марта 2012 г. № 169.

25. Об утверждении Правил работы с обезличенными данными в случае обезличивания персональных данных в Министерстве внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 14 ноября 2017 г. № 852. Доступ из справ.-правовой системы «КонсультантПлюс».

26. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: приказ ФСТЭК России от 18.02.2013 № 21 (зарег. в Минюсте России 14.05.2013 № 28375). Доступ из справ.-правовой системы «КонсультантПлюс».

27. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности [Электронный ресурс]: приказ ФСБ России от 10.07.2014 № 378 (зарег. в Минюсте России 18.08.2014 № 33620). Доступ из справ.-правовой системы «КонсультантПлюс».

28. Об утверждении Типового положения и подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации [Электронный ре-

сурс]: приказ МВД России от 2 июля 2012 г. № 660. Доступ из справ.-правовой системы «КонсультантПлюс».

29. Об утверждении Требований к межсетевым экранам [Электронный ресурс]: информационное сообщение ФСТЭК от 28 апреля 2016 г. № 240/24/1986. Доступ из справ.-правовой системы «КонсультантПлюс».

30. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: приказ ФСТЭК России от 11.02.2013 № 17 (зарег. Минюсте России 31.05.2013 № 28608). Доступ из справ.-правовой системы «КонсультантПлюс».

31. По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: информационное сообщение ФСТЭК России от 15.07.2013 № 240/22/2637. Доступ из справ.-правовой системы «КонсультантПлюс».

32. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией РФ 25.11.1994) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

33. Кемпф В.А., Осинцева Л.М. Специальная техника органов внутренних дел: технические средства защиты информации: учеб. пособие. Барнаул: БЮИ МВД России, 2017. 44 с.

34. Лагашин М.С. О развитии и эксплуатации ИСОД МВД России // Информационные технологии, связь и защита информации МВД России – 2017. С. 32-35. URL: https://mvd.informost.ru/2017/pdf/1-18.pdf.

35. Лангин А.И. Возимый навигационно-связной терминал — унифицированное абонентское устройство нового поколения в составе ИСОД МВД России // Информационные технологии, связь и защита информации МВД России – 2017. С. 35-38. URL: https://mvd.informost.ru/2017/pdf/1-18.pdf.

36. Ляшенко С.Н. Основные этапы развития информационных технологий, связи и защиты информации в МВД России // Информационные технологии, связь и защита информации МВД России – 2016. С. 18-22. URL: https://mvd.informost.ru/2016/pdf/1-17.pdf.

37. Питолин В.М., Мачтаков С.Г. Построение единой системы информационно-аналитического обеспечения МВД России // Общие и комплексные

проблемы естественных и точных наук – 2016. С. 175-177. URL: https://cyberleninka.ru/article/v/postroenie-edinoy-sistemy-informatsionno-analiticheskogo-obespecheniya-deyatelnosti-mvd-rossii.

38. Специальная техника органов внутренних дел: хрестоматия / сост. В.Э. Баумтрог. Барнаул: БЮИ МВД России, 2014. 142 с.

39. Солдатов В.В., Макаров Д.А. Становление и развитие системы управления доступом к сервисам ИСОД МВД России // Информационные технологии, связь и защита информации МВД России – 2016. С. 34-38. URL: https://mvd.informost.ru/2016/pdf/1-17.pdf.

40. Султанов Р.А. Электронная подпись // Информационные технологии, связь и защита информации МВД России – 2015. С. 66-69. URL: https://mvd.informost.ru/2015/pdf/1-16.pdf.

Содержание

Учебное издание

Кемпф Виктор Александрович

Обеспечение информационной безопасности в органах внутренних дел

Учебное пособие

Редактор	Е.Г. Авдюшкин
Корректура, компьютерная верстка	С.В. Калининой
Дизайн обложки	Е.О. Ифутиной

Лицензия ЛР № 02213552 от 14.07.1999 г.
Лицензия Плр № 020109 от 05.07.1999 г.

Подписано в печать 26.09.2019. Формат 60х90 1/16.
Ризография. Усл. п.л. 3,9. Тираж ___ экз. Заказ _____
Барнаульский юридический институт МВД России.
Научно-исследовательский и редакционно-издательский отдел.
656038, Барнаул, ул. Чкалова, 49; бюи.мвд.рф.