Воронежский институт МВД России

ОРГАНИЗАЦИЯ РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Учебное пособие

Воронеж 2022

УДК 005:922.1(0.067.2):004
ББК 32.973-018.2
О-64

Коллектив авторов: Т.В. Мещерякова, Е.А. Рогозин, Е.А. Пидусов, О.И. Нестеровский
Рецензенты:

Организация работы с конфиденциальной информацией в органах внутренних дел Российской Федерации: учебное пособие / [Т.В. Мещерякова и др.] /– Воронеж: Воронежский институт МВД России, 2022. – 146 с.

ISBN

Защита (обеспечение безопасности) информации является неотъемлемой составной частью вопроса обеспечения информационной безопасности, роль и значимость которой во всех сферах жизни и деятельности общества и государства на современном этапе неуклонно возрастают. Это в полной мере относится и к органам внутренних дел Российской Федерации.

Неправомерное искажение, уничтожение или разглашение служебной информации, ограниченного распространения, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах могут нанести ущерб в различных сферах повседневной деятельности подразделений органов внутренних дел, участвующих в процессах автоматизированного информационного взаимодействия.

Учебное пособие предназначено для курсантов и слушателей образовательных организаций МВД России для их практического обучения работе со сведениями ограниченного распространения, не относящимися к государственной тайне.

УДК 005:922.1(0.067.2):004
ББК 32.973-018.2

СОДЕРЖАНИЕ

Введение 4
Глава 1. Методические рекомендации по работе с документами, содержащими информацию ограниченного распространения, в органах внутренних дел Российской Федерации 8
1.1. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения, персональные данные и коммерческую тайну 8
1.2. Методические рекомендации по инвентаризации информационных ресурсов 30
Глава 2. Технические каналы утечки конфиденциальной информации, организационные и технические мероприятия по ее защите на объектах информатизации органов внутренних дел 41
2.1. Технические каналы утечки конфиденциальной информации, оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации 41
2.2. Организационные и технические мероприятия по защите конфиденциальной информации 51
2.3. Содержание и основы организации защиты конфиденциальной информации в автоматизированных системах от несанкционированного доступа 63
2.4. Обязанности и права должностных лиц по защите конфиденциальной информации, планирование и организация работ по технической защите конфиденциальной информации 88
2.5. Организация работ по созданию системы защиты конфиденциальной информации 95
2.6. Контроль состояния технической защиты конфиденциальной информации, порядок аттестации объектов информатизации 99
2.7. Взаимодействие с предприятиями, учреждениями и организациями при проведении совместных работ с конфиденциальной информацией 105
Заключение 109
Список литературы 111
Приложение 1 115
Приложение 2 117
Приложение 3 118
Приложение 4 120
Приложение 5 134
Приложение 6 138
Приложение 7 142
Приложение 8 145

Введение

В современном мире информационная безопасность является неотъемлемой составной частью общей проблемы обеспечения безопасности, роль и важность которой во всех сферах жизнедеятельности общества и государства неуклонно возрастают. В каждую историческую эпоху используемые методы и средства защиты информации были тесно связаны с уровнем развития науки и техники. Категории защищаемой информации определялись экономическими, политическими и военными интересами государства.

Производство и управление, оборона и связь, транспорт и энергетика, банковское дело, финансы, наука и образование, средства массовой информации в настоящее время все больше зависят от интенсивности информационного обмена, полноты, своевременности, достоверности и безопасности информации. Поэтому проблема безопасности информации актуальна и является предметом острой озабоченности руководителей органов государственной власти, предприятий, организаций и учреждений независимо от их организационно-правовых форм и форм собственности.

В соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02 июля 2021 г. № 400, одним из основных направлений деятельности государственных органов является укрепление государственной безопасности [1]. Обеспечение безопасности государства невозможно без принятия необходимых мер по защите сведений конфиденциального характера. Защита такого информационного ресурса является одной из важнейших задач Министерства внутренних дел Российской Федерации (МВД России).

Информационная безопасность включает [2]:

- состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;
- состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;
- состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;
- экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решений и координации действий в чрезвычайных

ситуациях, информационные и телекоммуникационные системы);

- финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).

Обеспечение информационной безопасности должно начинаться с анализа интересов субъектов отношений, связанных с использованием информационных систем (Приложение 1). Спектр их интересов применительно к используемому информационному ресурсу может быть разделен на следующие основные категории: доступность информации (возможность за приемлемое время получить требуемую информацию), целостность информации (актуальность, непротиворечивость и полнота требуемой информации), конфиденциальность информации (обеспечение доступа к требуемой информации только субъектам информационного взаимодействия).

Бурное развитие средств вычислительной техники (СВТ) открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационно-телекоммуникационных и управляющих систем, к возникновению принципиально новых так называемых информационных технологий. Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации.

Неправомерное искажение или фальсификация, уничтожение или разглашение части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах могут нанести ущерб безопасности субъектам, участвующим в процессах информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их безопасности, экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования, нежелательного разглашения, фальсификации, незаконного тиражирования или уничтожения.

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин.

Прежде всего – это расширение сферы применения СВТ и возросший уровень доверия к автоматизированным системам (далее – АС) управления и обработки информации [3]. Компьютерным системам доверяют самую

ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию.

Изменился подход и к самому понятию «информация». Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость информационно-телекоммуникационных систем, в рамках которых он существует. Осуществляется переход к рыночным отношениям в области создания и предоставления информационных услуг с присущей этим отношениям конкуренцией и промышленным шпионажем.

Вопросы защиты АС становятся еще более серьезными и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам.

Доступность СВТ и, прежде всего, персональных ЭВМ привела к распространению компьютерной грамотности в широких слоях населения, что привело к увеличению числа попыток неправомерного вмешательства в работу АС государственных и коммерческих структур.

Положение усугубляется недостаточной проработкой вопроса в области создания стройной и непротиворечивой системы законодательно-правового регулирования отношений в сфере накопления и использования информации, что создает условия для возникновения и распространения компьютерной преступности.

Еще одним весомым аргументом в пользу повышенного внимания к вопросам защиты информации является бурное развитие и распространение компьютерных вирусов, способных скрытно существовать в информационно-телекоммуникационных системах и предоставлять злоумышленникам возможности к совершению противоправных действий.

При выработке подходов к решению проблемы компьютерной, информационной безопасности следует всегда исходить из того, что защита информации в АС не является самоцелью. Конечной целью создания системы компьютерной безопасности является защита всех категорий субъектов, прямо или косвенно участвующих в процессах информационного взаимодействия, от нанесения им различного вида ущерба в результате случайных или преднамеренных воздействий на информацию и системы ее обработки и передачи.

В качестве возможных нежелательных воздействий на информационно-телекоммуникационные системы должны рассматриваться [3]:

- преднамеренные действия злоумышленников;
- ошибочные действия обслуживающего персонала и пользователей системы;
- проявления ошибок в ее программном обеспечении;
- сбои и отказы оборудования;

- аварии и стихийные бедствия.

В качестве защищаемых объектов должны рассматриваться информация и все ее носители.

По принадлежности к виду собственности информационные ресурсы могут быть государственными или негосударственными, находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных организаций.

Перечень сведений конфиденциального характера регламентирован указом Президента Российской Федерации от 6 марта 1997 г. № 188 [4]. Локальными нормативно-правовыми документами может определяется также перечень сведений, представляющих значимость для предприятия или организации, и, как следствие, подлежащих охране (например, устав, контракт и т.п.).

Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 утверждено «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» определен общий порядок обращения с документами и другими материальными носителями информации, содержащими такую служебную информацию [5].

Вышеизложенное в полной мере относится и к деятельности органов внутренних дел (ОВД) Российской Федерации, неразрывно связанной с получением, обработкой и анализом большого количества информации, включая сведения ограниченного доступа, разглашение которых может повлечь нарушение конституционных прав граждан, а также снижение эффективности работы правоохранительных органов по предупреждению, раскрытию и расследованию преступлений.

АС ОВД следует отнести к системам критического применения, выход из строя которых ведет к существенным негативным последствиям в сфере деятельности ОВД. Следовательно, вопросы, связанные с защитой информационных ресурсов АС, содержащих сведения конфиденциального характера, эксплуатируемых на объектах информатизации ОВД, являются весьма актуальными [6]. Их актуальность основывается на основных положениях Доктрины информационной безопасности, в которой отмечается необходимость как повышения защищенности критической информационной структуры и устойчивости ее функционирования, так и развития механизмов обнаружения, защиты и предупреждения информационных угроз [2].

Глава 1. Методические рекомендации по работе с документами, содержащими информацию ограниченного распространения, в органах внутренних дел Российской Федерации

1.1. Порядок обращения с документами, содержащими информацию ограниченного распространения, не относящуюся к государственной тайне.

Защищаемая информация включается в документы, входящие в состав информационных ресурсов ограниченного доступа, что ограничивает к ним доступ персонала. В соответствии действующей нормативной базой:

документ – материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения [35];

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель [11];

электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах [11].

В системе МВД России разработан Приказ от 9 ноября 2018 г. № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России», приложением к которому является инструкция, определяющая порядок обращения со служебной информацией ограниченного распространения в системе МВД России [9]. Инструкция устанавливает требования, обязательные для сотрудников, федеральных государственных гражданских служащих и работников системы МВД России, при обращении с документами и другими материальными носителями сведений, содержащими служебную информацию ограниченного распространения, в подразделениях центрального аппарата МВД России, территориальных органах МВД России, образовательных, научных, медицинских (в том числе санаторно-курортных) организациях системы МВД России, окружных управлениях материально-технического снабжения системы МВД России, а также иных организациях и подразделениях, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России.

Важно отметить, что требования инструкции не распространяются на порядок обращения с документами, содержащими сведения, составляющие

государственную тайну.

Согласно Приказу МВД России от 9 ноября 2018 г. № 755 к служебной информации ограниченного распространения в системе МВД России относится несекретная информация, касающаяся деятельности органов, организаций, подразделений системы МВД России, ограничения на распространение которой диктуется служебной необходимостью.

Можно утверждать, что потенциальными носителями к служебной информации ограниченного распространения являются все служащие, которые работают в государственных органах, органах законодательной, исполнительной и судебной власти, а также в подведомственных им предприятиях, учреждениях и организациях.

Если следовать данному подходу, то любые сведения о внутрисистемной деятельности ОВД могут быть ограничены в распространении, если это вызвано служебной необходимостью.

Процесс выявления и регламентации реального состава информации ограниченного доступа важен для эффективной работы системы защиты информации.

Например, информация ограниченного доступа формируется в следующих направлениях деятельности организации:

- прогнозирование и планирование деятельности (расширение подразделений, программы развития);
- управление организацией (сведения о подготовке и принятии решений, применяемые методы управления);
- финансовая деятельность (баланс, сведения о состоянии счетов и уровне доходности);
- переговоры и совещания по направлениям деятельности организации (информация о подготовке и результатах проведения переговоров);
- формирование ценовой политики на продукцию и услуги (информация о структуре цен, методах расчета, размерах скидок);
- формирование состава партнеров, поставщиков и потребителей;
- научная и исследовательская деятельность по созданию новой техники и технологий;
- использование новых технологий;
- подбор и управление персоналом;
- организация безопасности предприятия.

Уполномоченными должностными лицами, имеющими право относить служебную информацию к разряду ограниченного распространения в системе МВД России, являются:

- Министр внутренних дел Российской Федерации;
- заместители Министра внутренних дел Российской Федерации;
- начальники подразделений центрального аппарата МВД России и их заместители;
- начальники управлений, входящих в состав подразделений центрального аппарата МВД России, и их заместители;

- руководители (начальники) территориальных органов МВД России и их заместители;

- начальники структурных подразделений территориальных органов МВД России и их заместители;

- начальники образовательных, научных, медицинских (в том числе санаторно-курортных) организаций системы МВД России, окружных управлений материально-технического снабжения системы МВД России и их заместители;

- руководители (начальники) иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России, и их заместители.

Служебная информация ограниченного распространения не подлежит разглашению (распространению) без письменного разрешения уполномоченного должностного лица, которым были введены ограничения доступа к данной информации, либо вышестоящего руководителя.

За разглашение (несанкционированное распространение) служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, сотрудник привлекается к дисциплинарной или иной предусмотренной законодательством ответственности.

Работы по организации защиты служебной информации ограниченного распространения в органах, организациях, подразделениях системы МВД России проводятся в соответствии с законодательством Российской Федерации.

Организация защиты служебной информации ограниченного распространения осуществляется в целях:

- предотвращения утечки, хищения служебной информации ограниченного распространения по техническим каналам;

- предотвращения несанкционированного уничтожения, искажения, подделки, копирования, распространения, блокирования служебной информации ограниченного распространения;

- предотвращения неправомерного или несанкционированного доступа к служебной информации ограниченного распространения;

- обеспечения полноты, целостности и достоверности служебной информации ограниченного распространения.

Руководители (начальники) органов, организаций, подразделений системы МВД России организуют своевременное проведение мероприятий по обеспечению сохранности служебной информации ограниченного распространения и ограничению доступа к ней при ее использовании, обработке, регистрации, пересылке, хранении и уничтожении.

Организация защиты служебной информации ограниченного распространения, в том числе при ее обработке и хранении с использованием информационных систем, информационно-телекоммуникационных сетей, средств вычислительной техники, имеющих аттестаты соответствия по требованиям безопасности информации, осуществляется сотрудниками, на

которых возложены данные функции в соответствии с их должностными инструкциями (должностными регламентами).

Хранение документов, содержащих служебную информацию ограниченного распространения, в том числе правовых актов, осуществляется в надежно запираемых шкафах, ящиках или хранилищах, оборудованных приспособлениями для опечатывания.

Обработка (накопление, размножение или передача) служебной информации ограниченного распространения с использованием информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники допускается при наличии аттестатов соответствия указанных систем, сетей и средств по требованиям безопасности информации и условий, исключающих возможность ее разглашения и несанкционированного доступа к ней.

В случае реорганизации или ликвидации органа, организации, подразделения системы МВД России его руководитель (начальник) принимает меры по обеспечению защиты служебной информации ограниченного распространения.

Документы реорганизуемого или ликвидируемого органа, организации, подразделения системы МВД России, содержащие служебную информацию ограниченного распространения, в соответствии с решением ликвидационной комиссии подлежат уничтожению, передаче на архивное хранение либо правопреемнику.

О фактах разглашения служебной информации ограниченного распространения либо утраты документов, ее содержащих, незамедлительно ставится в известность руководитель (начальник) органа, организации, подразделения системы МВД России, в котором выявлены указанные факты. Руководитель (начальник) органа, организации, подразделения системы МВД России назначает комиссию для проведения расследования обстоятельств утраты или разглашения.

На утраченные документы, дела и издания, содержащие служебную информацию ограниченного распространения, составляется акт, на основании которого делаются соответствующие отметки в учетных формах [9].

В связи с тем, что в органах внутренних дел Российской Федерации активно используется система электронного документооборота, рассмотренные выше положения по обращению со служебной информацией ограниченного распространения должны применяться и в работе с электронными документами.

Однако порядок обращения электронных документов имеет ряд особенностей.

Документ такого вида должен быть оформлен по общим правилам делопроизводства и иметь реквизиты, установленные для аналогичного документа на бумажном носителе, за исключением реквизита «Государственный герб Российской Федерации».

В федеральном органе исполнительной власти используются

электронные документы (без предварительного документирования на бумажном носителе) и электронные копии документов.

Состав электронных документов, создаваемых в федеральном органе исполнительной власти, устанавливается перечнем документов, создание, хранение и использование которых осуществляются исключительно в форме электронных документов при организации внутренней деятельности федерального органа исполнительной власти, разрабатываемым на основе рекомендаций Федерального архивного агентства.

Перечень документов, создание, хранение и использование которых осуществляются исключительно в форме электронных документов при организации внутренней деятельности федерального органа исполнительной власти, утверждается руководителем этого органа исполнительной власти по согласованию с Федеральным архивным агентством.

Электронные документы, направляемые в органы государственной власти и органы местного самоуправления, подписываются усиленной квалифицированной электронной подписью должностного лица федерального органа исполнительной власти в соответствии с Федеральным законом «Об электронной подписи».

Под электронной подписью понимают информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [36].

В системе электронного документооборота федерального органа исполнительной власти могут использоваться способы подтверждения действий с электронными документами, при которых используются иные виды электронных подписей в соответствии с Федеральным законом «Об электронной подписи».

Получение и отправка электронных документов осуществляются подразделениями делопроизводства и режима.

После получения электронных документов, подписанных электронной подписью, подразделения делопроизводства и режима осуществляет проверку действительности электронной подписи.

После включения электронных документов в систему электронного документооборота формируются регистрационно-учетные данные о документе, обеспечивающие управление документом, в том числе его поиск, доступ к документу, контроль, хранение, использование и другие данные.

Документы, создаваемые в федеральном органе исполнительной власти, и (или) поступившие в федеральный орган исполнительной власти на бумажном носителе, регистрируются в системе электронного документооборота с созданием в ней электронной копии такого документа (Приложение 2).

Регистрация и учет электронных документов осуществляются в системе электронного документооборота федерального органа исполнительной власти.

Электронные документы формируются в электронные дела в соответствии с номенклатурой дел.

В номенклатуре дел указывается, что дело ведется в электронной форме, что отмечается в заголовке дела или в графе «Примечание».

Электронные документы после их исполнения или отправки подлежат хранению в установленном порядке в информационных системах федерального органа исполнительной власти в течение сроков, предусмотренных для аналогичных документов на бумажном носителе.

После истечения сроков, установленных для хранения электронных документов, они подлежат уничтожению на основании акта, утвержденного руководителем федерального органа исполнительной власти.

В Указе Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», персональные данные (ПДн) определяются как «сведения о фактах, событиях и обстоятельствах частной жизни, позволяющие идентифицировать субъекта», а позже в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под такими данными стала пониматься «любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту ПДн)» (ст. 3). Исходя из определения, закрепленного в Указе Президента Российской Федерации от 6 марта 1997 г. № 188, персональными данными являются только такие сведения, которые относятся к частной жизни гражданина и носят идентифицирующий его характер. А по смыслу второго определения, данного в Федеральном законе № 152, к ним относится любая информация, даже та, которая не имеет непосредственного отношения к определенному лицу [13]. В данном случае, указания на характер сведений, представляющих собой персональные данные, вообще отсутствуют. Приведенное определение практически дословно воспроизводит определение, закрепленное в Директиве № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных».

Законодательство о ПДн является сравнительно молодым, но динамично развивающимся. Первые упоминания о ПДн в российском законодательстве появились в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации». Однако детальное регулирование было осуществлено лишь с принятием в 2006 г. Закона о ПДн, который не только был основан на положениях Конвенции 1981 г., ратифицированной Россией в 2005 г. [37], но и заимствовал многие нормы Директивы 1995 г. [7] (особенно в массивном пакете поправок, принятых в 2011 г.). Регулирование отношений, связанных с обработкой ПДн, осуществляется исключительно на уровне нормативных правовых актов федерального уровня. Это обусловлено направленностью законодательства о ПДн на защиту конституционного права на неприкосновенность частной жизни, личную и семейную тайну, а также иных прав и свобод, связанных с обработкой ПДн. При этом в соответствии с подпунктом «в» п. 1 ст. 71

Конституции Российской Федерации регулирование и защита прав и свобод человека и гражданина как высших демократических ценностей отнесены к исключительному ведению Российской Федерации.

Закон о ПДн является базовым законодательным актом, регулирующим отношения, связанные с обработкой персональных данных, и определяет принципы, условия и правила обработки ПДн.

Согласно ч. 3 ст. 4, порядок обработки персональных данных, осуществляемой без использования средств автоматизации, может устанавливаться федеральными законами и иными нормативными правовыми актами Российской Федерации. В настоящее время одним из таких актов является Положение об особенностях обработки ПДн, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15 сентября 2008 г. № 687.

К важнейшим международным договорам, имеющим отношение к защите ПДн, следует отнести Международный пакт от 16 декабря 1966 г. «О гражданских и политических правах», ст. 17 которого предусматривает, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию». Кроме того, следует отметить положение ст. 8 Конвенции о защите прав человека и основных свобод 1950 г. [38], по которому «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции».

Основным международным договором в сфере ПДн с участием России является Конвенция 1981 г. [39] Данный документ закрепил фундаментальные принципы обработки ПДн, которые были имплементированы в Закон о ПДн. Следует отметить, что положения Конвенции не устанавливают непосредственно права и обязанности участников отношений, связанных с обработкой ПДн, а создают обязательства для государства по их имплементации в национальное право (ст. 4 (1)). Как следствие, положения данной Конвенции не действуют в России непосредственно. Кроме того, важно подчеркнуть, что Конвенция 1981 г. допускает возможность присоединяющейся стороны сделать заявление об отдельных изъятиях в сфере ее применения. Российская Федерация воспользовалась этим положением, заявив, что не будет применять Конвенцию к ПДн, обрабатываемым физическими лицами исключительно для личных и семейных нужд, а также к данным, отнесенным к государственной тайне. Кроме того, Российская Федерация прямо указала на то, что сохраняет за собой возможность устанавливать ограничения прав субъекта ПДн на доступ к ПДн о себе в целях защиты безопасности государства и общественного порядка.

Рассматривая систему источников законодательства в области ПДн, нельзя не упомянуть акты, которые хотя и не содержат юридически обязательных норм, но фактически оказывают серьезное влияние на

регулирование отношений, связанных с реализацией оператором организационных и технических мер защиты ПДн. К таким актам относятся национальные стандарты, каждый из которых представляет собой документ по стандартизации, который разработан участником или участниками работ по стандартизации, по результатам экспертизы в техническом комитете по стандартизации или проектном техническом комитете по стандартизации, утвержден федеральным органом исполнительной власти в сфере стандартизации, и в нем для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы, применяемые в отношении объекта стандартизации (п. 5 ст. 2 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации). Стандарты, релевантные проблематике защиты ПДн, представлены в Приложении 3.

Рассмотрение вопроса о месте ПДн в системе информации ограниченного доступа требует обращения еще к одному нормативному правовому акту – Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее – Закон об информации). Данный закон определяет информацию как «сведения (сообщения, данные) независимо от формы их представления» (п. 1 ст. 2).

Положения Закона об информации определяют ПДн как информацию ограниченного доступа [6]. В п. 9 статьи 9 «Ограничение доступа к информации» содержится отсылочная норма к специальному законодательству в отношении ПДн.

На основании анализа законодательства следует полагать, что не все ПДн охраняются режимом конфиденциальности. Некоторые данные, относящиеся к категории персональных, подлежат опубликованию в открытом доступе в соответствии с федеральными законами.

Законодательство определяет следующие категории персональных данных*:* общедоступные ПДн, специальные категории ПДн, биометрические ПДн и иные [13].

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками данной информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Биометрические персональные данные – это сведения, которые

характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством. Исходя из определения биометрических ПДн, к ним относятся фотографии и видеоизображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения – в системах видеонаблюдения и т.п.

Основные требования к обеспечению защиты ПДн установлены Федеральным законом от 27.07.2006 № 152 и принятыми в его исполнение подзаконными нормативными правовыми актами [13]. Эти требования обращены прежде всего к операторам персональных данных, к которым согласно Федеральному закону от 27.07.2006 № 152 относятся государственные и муниципальные органы, юридические или физические лица, самостоятельно или совместно с другими лицами организующие / осуществляющие обработку персональных данных, а также определяющие цели их обработки, состав данных, подлежащих обработке, действия (операции), совершаемые с ПДн. Типичными примерами операторов ПДн являются:

- организации, которые осуществляют обработку данных своих работников (и) или клиентов – физических лиц;
- лица, которые осуществляют сбор и анализ общедоступных данных в сети Интернет;
- государственные органы и учреждения, которые обрабатывают ПДн граждан в процессе предоставления государственных услуг;
- онлайн-сервисы, которые предусматривают регистрацию пользователей и (или) собирают данные о них в процессе использования такого сервиса.

В настоящее время под обработкой ПДн понимается любое действие (операция), совершаемое с ПДн, как с использованием средств автоматизации, так и без них. К таковым относятся, в частности, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн. К обработке ПДн в полной мере можно отнести любое действие, носящее волевой характер и сопряженное с воздействием на

данные в период их жизненного цикла:

- обычное хранение ПДн на жестком диске компьютерного устройства;
- использование компьютерных алгоритмов по глубинному анализу данных.

Под автоматизированной обработкой понимается любая обработка ПДн, осуществляемая с использованием вычислительных средств. Иными словами, в случае, если производится обработка ПДн, существующих в цифровой форме, то она всегда имеет автоматизированный характер.

Согласие субъекта ПДн является единственным универсальным легитимирующим основанием для любого сбора, использования или иных видов обработки ПДн. Все остальные основания для обработки ПДн в отсутствие согласия их субъекта предполагают наличие либо специальной цели обработки, либо специального субъекта на стороне оператора, либо совокупности указанных факторов.

Такое согласие должно быть:

1) конкретным, т.е. явно выраженным и определенным. Факт дачи согласия не должен быть предметом домыслов, а должен следовать из конкретных действий субъекта, свидетельствующих об этом. Молчание или бездействие субъекта ПДн, даже если такое поведение в соответствии с политикой конфиденциальности оператора будет признаваться согласием, не будет удовлетворять указанному требованию. Аналогичным образом действия субъекта ПДн по использованию устройства или интернет-сервиса с применением настроек конфиденциальности «по умолчанию» в отсутствие каких-либо свидетельств их изменения пользователем также не удовлетворяют указанному требованию;

2) информированным, т.е. даче субъектом согласия должно предшествовать предоставление ему всей необходимой и достоверной информации о целях обработки, обрабатываемых данных, операторе и иных лицах, которые будут осуществлять обработку его ПДн, сроки обработки и все иные релевантные параметры обработки ПДн. Предоставляемая оператором информация должна позволять субъекту получить ответы на вопросы о том, кто, зачем, какие данные, каким образом и в течение какого срока будет обрабатывать. При этом не будет лишним предоставление расшифровки основных терминов, которые используются в соответствующем документе (форма согласия, договор), в противном случае есть риск непризнания данного согласия соответствующим указанному требованию;

3) сознательным, т.е. обдуманным и осмысленным. Соответствующая информация должна быть воспринята субъектом ПДн и отражать его действительные намерения. Вынужденный характер дачи согласия ставит под сомнение его соответствие указанному требованию.

По общему правилу согласие на обработку ПДн может быть дано в любой форме, позволяющей подтвердить факт его получения, если только специальная форма дачи согласия прямо не предусмотрена законом. При этом равнозначным содержащему собственноручную подпись субъекта

персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью (ч. 4 ст.9) [12].

Требования к обработке ПДн вытекают практически из каждой статьи Федерального закона № 152, но есть статьи, непосредственно обращенные к операторам ПДн. Это ст. 18 «Обязанности оператора при сборе персональных данных», ст. 18.1 «Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом», ст. 19 «Меры по обеспечению безопасности персональных данных при их обработке». Оператор обязан принимать меры, необходимые и достаточные для выполнения установленных обязанностей. При этом оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для их обеспечения.

Рассмотрим данные положения более подробно.

Статья 18. Обязанности оператора при сборе персональных данных

Возложенные на оператора обязанности можно разделить на два вида: информационного характера (ч. ч. 1 – 4 ст. 18) и организационно-технического характера (ч. 5 ст. 18).

Обязанности информационного характера:

- обязанность оператора предоставить субъекту ПДн информацию, указанную в ч. 7 ст. 14 ФЗ №152 (данная обязанность возникает только при наличии на то соответствующего волеизъявления со стороны субъекта ПДн);

- обязанность по разъяснению субъекту ПДн последствий отказа от предоставления таких данных. Эта обязанность способствует обеспечению возможности принятия субъектом информированного решения о предоставлении своих данных. Одним из возможных последствий отказа от предоставления персональных данных является отказ оператора от совершения ожидаемого от него действия, которое не может быть осуществлено в отсутствие таких данных, либо в силу существа отношений, либо в силу закона (предоставление услуги, доступ в определенное помещение или транспортное средство, возможность въезда в страну и т.п.).

- обязанность предоставления субъекту, в случае если информация получена не от самого субъекта, содержащуюся информацию, в частности идентифицировать себя, пользователей данных, источник получения данных и цели обработки этих данных. Возложение такой обязанности на оператора имеет своей целью обеспечение еще большей прозрачности процессов перехода ПДн от одного оператора к другому. В идеале ее выполнение может позволить субъекту персональных данных отследить факт нарушения первоначальным оператором условий данного ему согласия на обработку ПДн или факт их обработки новым оператором без достаточных оснований. В отличие от информационной обязанности оператора по предоставлению информации субъекту при сборе данных (ч. 1 настоящей статьи) в рассматриваемом случае закон не обязывает субъекта требовать предоставления ему такой информации, предполагается безусловная обязанность ее выполнения оператором.

Обязанности организационно-технического характера: ч. 5 ст. 18 Федерального закона № 152 закрепила обязанность оператора обеспечивать локализацию отдельных процессов обработки ПДн, собираемых у российских граждан. Положения этой части вступили в силу 1 сентября 2015 г. и не имеют аналогов в зарубежных правопорядках, в связи с чем вопросы их толкования и соотношения с положениями о трансграничной передаче данных приобретают особую актуальность. Немаловажную роль в этом играет и возможность блокировки онлайн-ресурса оператора, который обрабатывает персональные данные граждан Российской Федерации с нарушением требований локализации в соответствии с положениями ст. 15.5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

Следует отметить, что данная норма содержит перечень мер, которые должен принять оператор ПДн в целях соблюдения требований Федерального закона от 27.07.2006 № 152. Этот перечень мер носит ориентировочный характер, окончательное решение относительно таких мер принимает сам оператор по своему усмотрению, за исключением случаев, когда закон обязывает оператора принять конкретные меры.

В частности, перечень мер, которые должны принимать операторы, являющиеся государственными и муниципальными органами, дан в соответствии с ч. 3 ст.18.1 в Постановлении Правительства Российской Федерации от 21 марта 2012 г. № 211 [40]. Данный нормативный правовой акт содержит перечень локальных актов, которые должны приниматься государственными или муниципальными органами, в который входят:

1) правила обработки ПДн, определяющие для каждой цели обработки таких данных содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;

2) правила рассмотрения запросов субъектов ПДн или их представителей;

3) правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

4) правила работы с обезличенными данными в случае обезличивания ПДн;

5) перечень информационных систем ПДн. В таком документе целесообразно указать назначение системы, составляющей основную цель обработки ПДн в ней (например, автоматизация процессов кадрового учета или процессов расчета заработной платы), категории и объем персональных данных в соответствии с Постановлением Правительства Российской

Федерации от 1 ноября 2012 г. № 1119 [10];

6) перечни ПДн, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

7) перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн в случае необходимости обезличивания ПДн;

8) перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

9) должностная инструкция ответственного за организацию обработки ПДн в государственном или муниципальном органе;

10) типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

11) типовая форма согласия на обработку ПДн служащих государственного или муниципального органа, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн;

12) порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка ПДн.

В ст. 19 Федерального закона № 152 определены меры по обеспечению безопасности ПДн при их обработке вне зависимости от установленного оператором режима конфиденциальности, а скорее исходя из самостоятельного режима конфиденциальности ПДн.

Меры, указанные в данной статье, могут относиться к одной из трех групп:

1) правовые (подготовка и принятие соответствующих локальных нормативных актов);

2) организационные (назначение ответственных лиц, обучение работников, непосредственно вовлеченных в процесс обработки персональных данных, правилам информационной безопасности и т.п.);

3) технические (набор мер, направленных как на уменьшение вероятности реализации угроз информационной безопасности вследствие уязвимости информационной системы, так и на минимизацию потерь при реализации таких угроз).

Для выполнения обязанности по определению угроз безопасности ПДн необходимо разработать документ «Модель угроз безопасности персональных данных при их обработке в информационной системе ПДн». При этом целесообразно руководствоваться следующими документами

ФСТЭК России: Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн, утвержденная ФСТЭК России 14 февраля 2008 г.; Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн, утвержденная ФСТЭК России 15 февраля 2008 г.

Перечень организационных и технических мер в соответствии с уровнями защищенности ПДн, установленными Правительством Российской Федерации, предусмотрен в следующих актах:

- Приказ Федеральной службы безопасности (ФСБ) России от 10 июля 2014 г. № 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» [14];
- Приказ 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» [15];
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [16].

Законодательство о коммерческой тайне включает: Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», а также главу 75 IV части Гражданского кодекса Российской Федерации «Право на секрет производства (ноу-хау)».

Под коммерческой тайной понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [17].

Информация, составляющая коммерческую тайну, – это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую значимость в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» в ст. 5 содержит перечень сведений, которые не могут составлять коммерческую тайну [17]. Это сведения:

1) содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.

На практике к информации, составляющей коммерческую тайну (секрет производства), принято относить:

а) информацию о полезных моделях, промышленных образцах, изобретениях и иных объектах интеллектуальной собственности, находящихся на стадии разработки (регистрации);

б) информацию о партнерах и клиентах (покупателях, поставщиках, посредниках, контрагентах и др.), об условиях заключаемых сделок, ценообразовании, предлагаемых скидках, акциях, расчетах цен и формируемых на основе этих сведений клиентских базах;

в) информацию личного характера – все сведения об источниках доходов, личной жизни руководства и главного бухгалтера, членов их семей,

адреса, расписание деловых встреч, данные об их контактных телефонах, пагубных привычках, маршрутах передвижений и т.д.;

г) информацию о технических средствах охраны имущества организации, системах охранной и иной сигнализации, методах и приемах обеспечения безопасности деятельности организации, местах хранения материальных ценностей.

В соответствии с п. 1 ст. 6. Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» обладатель информации, составляющей коммерческую тайну, обязан предоставить данные сведения органу государственной власти, иному государственному органу, органу местного самоуправления. Предоставление осуществляется на безвозмездной основе при наличии мотивированного требованию, которое подписано уполномоченным должностным лицом, содержит цель и правовое основание затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

На основании ст. 6.1 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;

6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой

информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну, и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

Информацию, защита которой является обязанностью субъекта в силу выполняемых им профессиональных полномочий, принято относить к категории «профессиональная тайна».

Субъектом профессиональной тайны может выступать и физическое, и юридическое лицо.

К профессиональной тайне относятся следующие виды тайн:

- банковская тайна;
- нотариальная тайна;
- адвокатская тайна;
- врачебная тайна;
- тайна страхования;
- тайна исповеди;
- иные виды тайн.

Банковская тайна. В Гражданском кодексе РФ, а именно в ст. 857 установлена обязанность банка гарантировать тайну следующих сведений:

- банковского счета;
- банковского вклада;
- операций по счету;
- о клиенте.

Указанные сведения предоставляются:

- самим клиентам или их представителям;
- в бюро кредитных историй;
- государственным органам и их должностным лицам (в определенных случаях).

Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» в ст. 26 устанавливает обязанность служащих кредитной организации хранить в тайне следующие сведения о клиентах и корреспондентах:

- об операциях;
- о счетах;
- о вкладах;
- об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

К банковской тайне относятся сведения, касающиеся:

- клиентов банка – их паспортные данные, сведения о местонахождении (местожительстве), банковских реквизитах юридического лица, сведения о его руководстве;
- банковского счета клиента – вид счета, дата его открытия, номер счета, данные о суммах на счете, количество счетов клиента, сведения о владельце счета;
- банковского вклада – вид вклада, сумма вклада, порядок начисления и размер процентов, срок вклада;
- операций по счетам и вкладам клиентов – валюта счета, суммы, зачисляемые и списываемые со счета, документы, на основании которых проводятся операции по счету, выписки со счетов;
- корреспондентов банка – валюта и сумма операций, условия и даты сделок;
- иной деятельности банка, связанной с управлением финансами, внутренними технологическими процессами, имеющие ценность для банка в силу неизвестности их третьим лицам.

Банковская тайна должна строго соблюдаться банком и не подлежит разглашению, а также опубликованию в средствах массовой информации и передаче третьим лицам.

Рассматриваемые сведения могут быть предоставлены без нарушения законодательства следующим органам и организациям:

- судам и арбитражным судам;
- Счетной палате Российской Федерации;
- налоговым органам;
- таможенным органам;
- федеральному органу исполнительной власти в области финансовых рынков;
- Пенсионному фонду;
- Фонду социального страхования;
- органам принудительного исполнения судебных актов, актов других органов и должностных лиц;

- органам предварительного следствия по делам, находящимся в их производстве;
- органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений;
- уполномоченному органу, осуществляющему меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, в случаях, порядке и объеме, которые предусмотрены Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем»;
- органу валютного контроля.

С согласия юридического лица, индивидуального предпринимателя или физического лица информация по их операциям представляется банками в целях формирования кредитных историй в бюро кредитных историй в соответствии с Федеральным законом «О кредитных историях».

Банки и организации, в силу федеральных законов имеющие отношение к банковской тайне, а также их служащие, имеющие отношение к банковской тайне в силу исполнения своих должностных обязанностей, несут ответственность за разглашение банковской тайны.

Врачебная тайна. В соответствии со ст. 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ врачебную тайну составляют следующие сведения:
- о факте обращения гражданина за оказанием медицинской помощи;
- о состоянии его здоровья и диагнозе;
- иные сведения, полученные при его медицинском обследовании и лечении.

По общему правилу не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей.

При этом допускается разглашение указанных сведений с письменного согласия гражданина или его законного представителя в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

Законодательством установлены случаи, когда предоставление сведений, составляющих врачебную тайну, возможно без согласия гражданина (п. 4 ст. 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ):

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу

органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача, либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

4) в случае оказания медицинской помощи несовершеннолетнему больного наркоманией при оказании ему наркологической помощи или при медицинском освидетельствовании несовершеннолетнего в целях установления состояния наркотического либо иного токсического опьянения (за исключением установленных законодательством Российской Федерации случаев приобретения несовершеннолетними полной дееспособности до достижения ими восемнадцатилетнего возраста), а также несовершеннолетнему, не достигшему возраста пятнадцати лет (в соответствии с ч. 2 ст. 54 № 323-ФЗ), для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с ч. 6 ст. 34.1 Федерального закона от 4 декабря 2007 года № 329-ФЗ «О физической культуре и спорте в Российской Федерации» несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом

требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности.

Нарушение врачебной тайны – это разглашение ее хотя бы одному лицу, умышленное или неосторожное (небрежное хранение документации или беседа медиков в людном месте). Необходимый обмен информацией в ходе оказания специалистами медицинской помощи не рассматривается как нарушение врачебной тайны. Вся информация в медицинских документах гражданина также является врачебной тайной.

Адвокатская тайна. Статья 8 Федерального закона от 31.05.2002 № 63-ФЗ (ред. от 11.07.2011) «Об адвокатской деятельности и адвокатуре в Российской Федерации» определяет, что адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Режим адвокатской тайны распространяется на следующие сведения:

- факт обращения к адвокату;
- о доказательствах, подготовленных адвокатом по делу;
- сведения, переданные доверителем адвокату;
- сведения о самом доверителе, которые стали известны адвокату в ходе рассмотрения дела;
- содержание юридических рекомендаций доверителю;
- делопроизводство адвоката по делу;
- условия соглашения об оказании юридической помощи;
- иные сведения, связанные с оказанием юридических услуг.

Гарантии обеспечения адвокатской тайны реализуются в следующем:

- адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах дела, имеющегося у него в производстве;
- оперативно-розыскные мероприятия и следственные действия в отношении адвоката проводятся только на основании судебного решения, причем полученные сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей (за исключением орудия преступления, а также предметов, запрещенных к обращению или с ограниченным оборотом).

Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации» установлено: «помощник адвоката и стажер адвоката обязаны хранить адвокатскую тайну».

Нотариальная тайна (*тайна нотариальных действий*). Согласно ст. 5 Основ законодательства Российской Федерации о нотариате (утв. ВС Российской Федерации 11.02.1993 № 4462-1) нотариусу при исполнении служебных обязанностей, лицу, замещающему временно отсутствующего нотариуса, а также лицам, работающим в нотариальной конторе, запрещается

разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных настоящими Основами. Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия.

Справки о совершенных нотариальных действиях выдаются по требованию суда, прокуратуры, органов следствия в связи с находящимися в их производстве уголовными, гражданскими или административными делами, а также по требованию судебных приставов-исполнителей в связи с находящимися в их производстве материалами по исполнению исполнительных документов.

Тайна страхования. В соответствии со ст. 946 Гражданского кодекса Российской Федерации тайну страхования составляют сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности.

В соответствии с Законом Российской Федерации от 27.11.1992 № 4015-1 «Об организации страхового дела в Российской Федерации» в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так и физические лица – страховые агенты и страховые брокеры.

Доступ к сведениям, составляющим тайну страхования, на законных основаниях имеют:

1) представитель страхователя (выгодоприобретателя) – на основании нотариально удостоверенной доверенности;

2) орган дознания и предварительного следствия – по находящимся в его производстве уголовным делам;

3) суд – на основании определения суда по находящимся в его производстве делам;

4) прокурор – на основании постановления о производстве проверки в пределах его компетенции по находящимся у него на рассмотрении материалам.

Тайна усыновления. В соответствии со ст. 139 Семейного кодекса Российской Федерации тайна усыновления ребенка охраняется законом. Тайны усыновления распространяется на:

- судей, вынесших решение об усыновлении, и всех работников суда, причастных к судебному делопроизводству, и всех участвующих в рассмотрении дела лицам;
- должностные лица, осуществляющие государственную регистрацию усыновления (работники органов записи актов гражданского состояния, представители органов опеки и попечительства, медицинские работники).

Тайна исповеди. Тайна исповеди – это самостоятельный вид охраняемых законом тайн, одна из гарантий свободы вероисповедания.

Обеспечение тайны исповеди является внутренним делом

священника, юридической ответственности за ее разглашение он не несет. Согласно ч. 2 ст. 51 Конституции Российской Федерации и ч. 7 ст. 3 Федерального закона «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Согласно церковному каноническому праву, священник не может нарушить тайну исповеди ни при каких условиях. Это строго запрещено 120-м правилом Номоканона при Большом Требнике: за открытие греха исповедовавшегося духовный отец отстраняется на три года от служения и каждый день должен класть сто поклонов.

1.2. Методические рекомендации по инвентаризации информационных ресурсов

Информационные ресурсы законом «Об информации, информатизации и защите информации» определяются как отдельные документы и массивы документов в информационных системах (библиотеках, фондах, архивах и т.д.) [11]. Таким образом, под определение «информационные ресурсы» подпадает практически весь спектр продуктов информационной деятельности общества.

В информационно-вычислительных системах информационные ресурсы, т.е. документы, массивы документов, представляются в виде данных.

Для удобства хранения и обработки данные объединяются в файлы. Причем необходимо отметить, что в машинном виде документ может быть представлен как одним, так и группой файлов, точно так же, как и массив документов может быть заключен в один файл. Соответствие «файл-документ» определяется информационной технологией, используемой для обработки файлов (работы с документами).

В общем виде под информационной технологией понимается система реализации операций по преобразованию данных в информационно-вычислительной системе с учетом этапов достижения цели [11]. Преобразование данных в вычислительных системах осуществляется с помощью программного обеспечения. Программное обеспечение по назначению делится на системное и прикладное. Причем необходимо отметить, что информационная технология может либо включать в свой состав системное программное обеспечение, либо базироваться на нем.

Информационные технологии могут быть классифицированы по функциональному предназначению как технологии прогнозирования, планирования, оперативного управления, анализа, учета, контроля, многофункциональные. По назначению информационные технологии могут быть технологиями сбора, хранения и отображения информации, оценки обстановки, выработки, принятия и доведения (передачи) решений, а также комбинированные.

Таким образом, информационный ресурс в информационно-вычислительной системе может быть представлен как совокупность файлов данных, составляющих информацию пользователей и программных продуктов, определяющих информационную технологию. Отдельные файлы пользователей и информационные технологии, предназначенные для их обработки, составляют информационную систему.

Необходимо отметить, что свойства информационной системы в значительной мере определяются ее ориентацией на организационный, организационно-технологический или технологический тип управления.

Информационные системы, предназначенные для работы в системе организационного управления, доступны для большого числа пользователей и базируются на широко распространенных информационных технологиях. Информационные системы, использующиеся в организационно-технологических и технологических системах управления, закрыты для общего использования и зачастую строятся на уникальных информационных технологиях.

Как показывает анализ, наибольшее распространение и, следовательно, уязвимость получили информационные системы, использующиеся в системах организационного управления. При этом необходимо заметить, что ущерб от нарушения работы информационных систем в системах технологического управления может быть в ряде случае значительно большим.

Информационный ресурс информационной системы, ориентированной на организационное управление, может быть представлен как единичный файл или база данных, в том числе совокупность файлов.

С точки зрения пользователей, информационный ресурс как объект авторского права, может состоять из двух частей: уникальной, созданной пользователем, и стандартной, заимствованной у других авторов.

К уникальной части информационного ресурса относятся отдельные файлы и базы данных, созданные пользователями прикладные программы. К стандартной части информационного ресурса – операционные системы, системы управления базами данных, программы расчетов и т.д.

Как показывает анализ функционирования систем организационного управления, к уникальной части информационной системы относятся в первую очередь файлы и базы данных заполняемые пользователями, реже базы данных, составляемые пользователями. Как исключение встречаются прикладные программные продукты, разработанные пользователями.

Анализ деятельности органов, организаций, подразделений в системе МВД России показывает, что рядовыми пользователями всех направлений деятельности создаются файлы и поддерживаются базы данных. Сотрудниками информационно-технических подразделений создаются базы данных, сотрудниками научно-технических подразделений разрабатывается программное обеспечение.

Таким образом, в информационно-вычислительных системах ОВД можно выделить два основных типа ресурсов – основные информационные

ресурсы и вспомогательные информационные ресурсы. К основным информационным ресурсам относятся информационные ресурсы, содержащие признаки уникальности (уникальных частей). К вспомогательным – информационные ресурсы, содержащие только признаки стандартных частей в принятой классификации. Другими словами, к основным информационным ресурсам можно отнести отдельные файлы, группы файлов (папки), информационные системы, содержащие файлы и группы файлов, подверженных прямому изменению пользователем. К вспомогательным информационным ресурсам могут быть отнесены информационные продукты, обеспечивающие работу других информационных систем и не подверженные прямому изменению пользователем их файлового состава.

Основной информационный ресурс информационно-вычислительных систем можно рассматривать как законченный и незаконченный. При проведении процедуры инвентаризации наибольшую трудность представляет учет незаконченного информационного ресурса в части отдельных файлов и групп файлов. Его учет возможен только в том случае, когда размещение этой информации на компьютере некоторым образом структурировано.

Для обеспечения учета информационного ресурса в больших подразделениях ОВД целесообразно использование АС ведения документооборота, позволяющих внутренними средствами осуществлять учет документов и контролировать адреса их перемещения.

Однако принятие таких мер не всегда оправдано с экономической точки зрения и часто затруднительно в связи с различием задач, решаемых пользователями персональных ЭВМ.

Поэтому при определении перечня информационных ресурсов в подразделениях, в первую очередь, необходимо систематизировать материалы, хранящиеся в отдельных файлах по какому-либо из признаков информации, например, по тематикам работы или функциональному предназначению, а также перераспределить пространство носителей информации, выделив ее часть для хранения учитываемых информационных ресурсов.

При повышении эффективности информационного ресурса информационно-вычислительных систем через обеспечение его свойств доступности и защищенности при учете основным объектом выступают данные, составляющие уникальную часть АС, а, следовательно, основные информационные ресурсы.

Процедуру учета и регистрации рекомендуется выполнять в два этапа. На первом этапе ответственными за организацию и проведение инвентаризации выступают руководители структурных подразделений органа (организации) системы МВД России. Они по указанию руководителя органа (организации) проводят первичный учет и регистрацию информационных ресурсов своих подразделений и представляют полученные данные в подразделение по защите информации органа (организации) системы МВД России. На втором этапе подразделением по защите информации проводится рассмотрение материалов

по результатам первичного учета, составляется единый перечень информационных ресурсов органа (организации) системы МВД России, определяются ограничения и возможности дальнейшего использования информационных ресурсов, назначаются ответственные в подразделениях за поддержание и сохранность информационного ресурса.

Порядок проведения государственного учета и регистрации баз данных и учет банков данных определен Постановлением Правительства Российской Федерации от 14 ноября 2015 г. № 1235 «О федеральной государственной информационной системе координации информатизации» [18].

Государственный учет баз данных осуществляется на этапе их разработки. Государственная регистрация баз данных осуществляется после передачи их в эксплуатацию.

Схема алгоритм учета информационных ресурсов в органах (организациях) системы МВД России представлена на рисунке 1.

Первый этап

На первом этапе руководитель структурного подразделения должен, в первую очередь, составить перечень информационных ресурсов своего подразделения (рис. 1, блок 1) в следующей последовательности:

- определить информационные системы, представляющие законченный информационный ресурс;
- определить информационные системы, представляющие не законченный информационный ресурс;
- сгруппировать по какому-то признаку (например, по тематикам) файлы, созданные пользователями, не отнесенные ни к одной из информационных систем, но представляющие определенную информационную значимость;
- определить не учитываемую информацию, которая не представляет значимости для сотрудников подразделений.

Следующей задачей (рис. 1, блок 2) является определение степени конфиденциальности каждого из выделенных информационных ресурсов в соответствие с перечнем конфиденциальной информации, принятым в органе (организации) МВД России. Причем не учитываемую информацию (рис. 1, блок 3), которая подпадает под категорию конфиденциальной, целесообразно уничтожить.

После соотнесения перечня информационных ресурсов перечню конфиденциальной информации, в целях систематизации хранения информации на магнитных носителях (рис. 1, блок 4), необходимо выделить отдельные области памяти накопителей на жестких магнитных дисках для хранения и обработки информации различных категорий конфиденциальности.

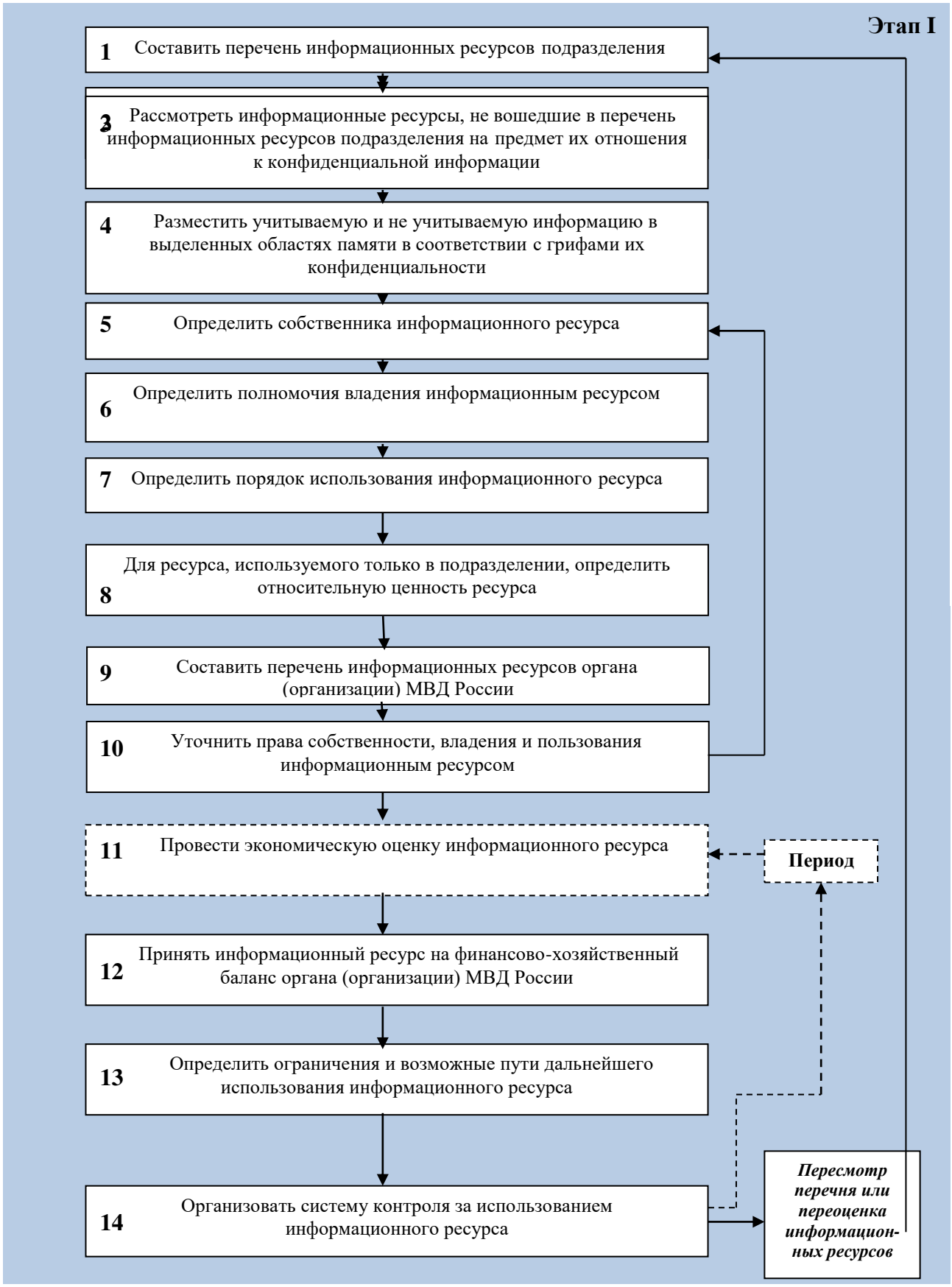

Рисунок 1. Алгоритм инвентаризации информационных ресурсов в ОВД

Такая система хранения информации наиболее удобна и в дальнейшем, при использовании программных средств защиты информации. Далее (рис. 1, блок 5) необходимо определить собственника информационных ресурсов. Информационные ресурсы, созданные за счет (или же с участием) средств федерального бюджета и бюджета субъекта Российской Федерации, являются государственными информационными, остальные – частными. При определении информационного ресурса как негосударственного необходимо указать его форму, а также собственника информационного ресурса. После определения собственника информационного ресурса руководителю подразделения необходимо определить свои полномочия относительно владения и пользования информационным ресурсом (рис. 1, блок 6).

Следующим шагом инвентаризации информационных ресурсов в подразделении (рис. 1, блок 7) является определение порядка их использования. Здесь необходимо уточнить – используется ли указанный информационный ресурс только в интересах данного подразделения или же используется совместно, указать количество пользователей информационного ресурса – сотрудников подразделения, а также определить ответственного за его поддержание и сохранность.

На заключительной стадии первого этапа, руководитель подразделения должен определить относительную ценность перечисленного им информационного ресурса (рис. 1, блок 8).

По завершении своего этапа инвентаризации информационных ресурсов подразделения его руководитель подает руководителю органа (организации) МВД России докладную записку с указанием полученных результатов. В приложении к докладной записке помещается «Ведомость информационных ресурсов подразделения», составленная по форме, представленной в таблице 1.

Второй этап

На втором этапе в органе (организации) МВД России по представлению руководителя подразделения по защите информации создается комиссия по инвентаризации информационных ресурсов. В состав комиссии обязательно включаются ответственные за защиту информации в подразделениях.

К задачам комиссии относится:

1. По полученным из подразделений материалам формирование и представление руководителю на утверждение перечня информационных ресурсов органа (организации) системы МВД России.

2. Определение комплекса мероприятий по периодическому уточнению перечня информационных ресурсов.

3. Уточнение собственности информационного ресурса и полномочий владения им.

4. Определение ограничений и возможных направлений дальнейшего использования информационных ресурсов органа системы МВД России.

5. Уточнение комплекса мероприятий по поддержанию, развитию, совершенствованию и защите информационных ресурсов органа

(организации) системы МВД России.

6. Определение сроков переоценки незаконченных информационных ресурсов.

7. Представление руководителю обоснования для проведения экспертных оценок стоимости информационных ресурсов.

На основе «Сводных ведомостей информационных ресурсов подразделений» комиссией по инвентаризации информационных ресурсов составляется перечень информационных ресурсов органа (организации) в системе МВД России (рис. 1, блок 9). Форма «Перечня информационных ресурсов» органа (организации) представлена в таблице 2.

8. Анализ показывает, что наиболее сложным вопросом при разработке, эксплуатации и поддержании информационного ресурса является определение прав собственности на него и уточнение полномочий владения. Поэтому при инвентаризации информационных ресурсов предлагается в качестве следующего этапа включить уточнение этих позиций (рис. 1, блок 10).

9. Одним из направлений политики государства в области информатизации является создание рынка информационных продуктов и цивилизованного введения их в хозяйственный оборот.

10. Для части информационных ресурсов это возможно только лишь при их качественной экономической оценке, требующей привлечения специалистов-оценщиков. Поэтому, учитывая особенности сегодняшней экономики, предлагается провести оценку информационных ресурсов поэтапно, в соответствии с планами развития информационного рынка в субъекте Российской Федерации и участия в нем органов (организаций) системы МВД России (рис. 1, блок 11). Оцененные информационные ресурсы должны быть в обязательном порядке, согласно требованию закона «Об информации, информатизации и защите информации», приняты на баланс в финансово-хозяйственном подразделении органа (организации) МВД России (рис. 1, блок 12).

Таблица 1

Сводная ведомость информационных ресурсов _____

Наименование ресурса	Форма представления	Реферат	Степень конфиденциальности	Форма собственности[1]		Полномочия владения[2]		Порядок использования[3]			Относительная ценность ресурса	Стоимость ресурса
				Форма собственности	Собственник[1]	Форма[2]	Чем определено	Порядок[3]	Число пользователей	Ответ.		
ИАС «Петербург»	ИС		ДСП	Государственная		владелец		только в подразд.	6	Иванов		45000$
ГИС «Прогноз»	ИС		ДСП	Частная	ОАО «НПО Заря»	пользователь	Договор №	совмест. с ОАО «НПО Заря»	6	Иванов		90$/ мес.
БД «Отчет»	БД на ИС «Accses»		нет	Государственная		владелец		только в подразд.	6	Иванов	0,9	
Архив «Приказы»	Файловый архив		ДСП	Государственная		владелец		только в подразд.	6	Иванов	0,65	

[1]**Собственник** информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами. Информационные ресурсы, созданные с участием средств федерального бюджета или бюджета субъекта Российской Федерации являются государственными.

[2]**Владелец** информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом. **Пользователь** (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

[3]Используется только в подразделении или совместно с кем.

Таблица 2

Перечень информационных ресурсов _____

				Наименование ресурса	
				Форма представления	
				Реферат	
				Степень конфиденциальности	
				Форма собственности	**Форма Собственности**
				Собственник	
				Форма	**Полномочия Владения**
				Чем определено	
				Перечень подразделений	**Порядок использования**
				Внешние организации	
				Общее число пользователей	
				Подразделение	**Информация о закреплении**
				Отв. должностное лицо	
				Относительная ценность ресурса	
				Стоимость ресурса	
				Прибыло	**Движение на этапе жизненного цикла**
				Убыло	
				Срок следующей переоценки	
				Предложения по дальнейшему использованию	
				Примечания	

Для части информационных ресурсов это возможно только лишь при их качественной экономической оценке, требующей привлечения специалистов-оценщиков. Поэтому, учитывая особенности сегодняшней экономики, предлагается провести оценку информационных ресурсов поэтапно, в соответствии с планами развития информационного рынка в субъекте Российской Федерации и участия в нем органов (организаций) системы МВД России (рис. 1, блок 11). Оцененные информационные ресурсы должны быть в обязательном порядке, согласно требованию [11], приняты на баланс в финансово-хозяйственном подразделении органа (организации) МВД России (рис. 1, блок 12).

10. Далее (рис. 1, блок 13) комиссией по инвентаризации информационных ресурсов рассматриваются возможные ограничения и пути дальнейшего использования информационных ресурсов органа (организации) ОВД. По завершении работ руководителю органа (организации) системы МВД России представляется докладная записка по материалам инвентаризации информационных ресурсов и их перечень (таблица 2) на утверждение и производится закрепление информационных ресурсов за конкретными должностными лицами с целью их дальнейшего качественного ведения, поддержания. Должностное лицо, за кем закреплен информационный ресурс, должно отвечать и за его сохранность.

11. После проведения работ по инвентаризации информационных ресурсов в органе (организации) МВД России предлагается организовать систему контроля за их использованием (рис. 1, блок 14). Сюда необходимо включить мероприятия по периодической переоценке не законченных информационных ресурсов, в том числе и экономической их оценке, а также уточнение комплекса мероприятий по поддержанию, развитию, совершенствованию и защите информационных ресурсов органа (организации) системы МВД России.

Таким образом, в главе представлены методические рекомендации по работе с документами, содержащими информацию ограниченного распространения, в ОВД Российской Федерации: порядок обращения с документацией, содержащей служебную информацию ограниченного распространения, ПДн и коммерческую тайну; рекомендации по составлению перечня сведений конфиденциального характера; рекомендации по инвентаризации информационных ресурсов. Использование изложенных методических рекомендаций в профессионально-служебной деятельности субъектов информационных отношений ОВД в качестве руководства по защите информации ограниченного распространения позволит им соблюдать необходимые требования по работе с конфиденциальными документами и информационными ресурсами в соответствии с действующими нормативными правовыми актами, регламентирующими порядок и правила защиты информации ограниченного пользования на предприятиях и в государственных структурах, что в целом будет способствовать повышению эффективности деятельности правоохранительных органов по предупреждению, раскрытию и расследованию преступлений.

Контрольные вопросы по главе 1:

1. Что понимается под служебной информацией ограниченного распространения в системе МВД России?
2. Какими нормативными документами регламентируется порядок обращения со служебной информацией ограниченного распространения?
3. Какие документы относятся к основной служебной документации ограниченного распространения в МВД России?
4. Каков порядок регистрации, учета и хранения электронных документов в системе электронного документооборота МВД России?
5. Как определяются ПДн в международной и отечественной нормативной документации?
6. Перечислите основные требования по обработке и защите ПДн в соответствии с действующей нормативной документацией.
7. Что понимается под коммерческой и профессиональной тайной?
8. Приведите перечень сведений, которые не могут составлять коммерческую тайну.
9. Что относится к сведениям конфиденциального характера?
10. Что относится к информационным ресурсам информационно-вычислительных систем ОВД?
11. Какова процедура учета и регистрации информационных ресурсов в органах (организациях) системы МВД России?

Глава 2. Технические каналы утечки конфиденциальной информации, организационные и технические мероприятия по ее защите на объектах информатизации органов внутренних дел

2.1. Технические каналы утечки конфиденциальной информации, оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

Одним из наиболее мощных каналов поступления информации с ограниченным доступом в ОВД является реализация ими задачи по анализу оперативной обстановки в той местности, на которую распространяется юрисдикция конкретного органа. В их число попадают и персональные данные о гражданах, проживающих на данной территории, и сведения, составляющие коммерческую, профессиональную тайну субъектов предпринимательской и иной деятельности, а также сведения, составляющие государственную тайну, касающиеся специфики деятельности предприятий оборонного комплекса, войсковых частей, иных субъектов, работающих с такой информацией, которые расположены на данной территории.

Поэтому ОВД Российской Федерации разработали единый подход к организации технической защиты служебных сведений от утечки по техническим каналам, в том числе за счет побочных электромагнитных излучений и наводок (ПЭМИН) [19].

Основные надежды в вопросах обеспечения информационной безопасности специалисты связаны с внедрением интегральных подходов и технологий. Необходимым условием реализации интегрального подхода является блокирование всех технических каналов утечки и несанкционированного доступа к информации.

Под техническим каналом утечки информации понимают совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал [19]. Отсюда можно сделать вывод, что под техническим каналом утечки информации понимают способ получения с помощью технического средства разведки интересуемой информации об объекте.

Классификация технических каналов утечки информации приведена на рисунке 2.

Рисунок 2. Классификация технических каналов утечки информации

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку делятся на оптические, радиоэлектронные, акустические и материально-вещественные.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

К ОТСС относятся:

- технические средства автоматизированных систем (АС) управления, электронно-вычислительные машины и их отдельные элементы (средства вычислительной техники (СВТ));
- средства изготовления и размножения документов (СИРД);
- аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода;
- системы внутреннего телевидения; системы видеозаписи и видеовоспроизведения;
- системы оперативно-командной связи;
- системы внутренней автоматической телефонной связи, включая и соединительные линии перечисленного выше оборудования и т.д.

Вспомогательные технические средства и системы (ВТСС) –

технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в защищаемых помещениях (на них могут воздействовать электромагнитные и акустические поля опасного сигнала).

К ВТСС относятся:

- различного рода телефонные средства и системы;
- средства передачи данных в системе радиосвязи;
- системы охранной и пожарной сигнализации;
- средства оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- системы кондиционирования;
- системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);
- средства электронной оргтехники;
- средства и системы электрочасофикации;
- иные технические средства и системы.

Используя в своих интересах те или иные физические поля, злоумышленник создает определенную систему передачи информации. Для возникновения канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

В основе утечки лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных полей и материальных объектов.

Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России. Одним из основополагающих документов в рамках защиты от утечки по техническим каналам утечки является методический документ ФСТЭК России «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). В данном документе указано, что при ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

- акустическое излучение информативного речевого сигнала;
- электрические сигналы, возникающие при преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы контролируемой зоны (КЗ);
- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемого помещения (ЗП);
- несанкционированный доступ к обрабатываемой в АС информации и

несанкционированные действия с ней;

- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств;

- побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи информации;

- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации (закладочные устройства), модулированные информативным сигналом;

- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;

- прослушивание ведущихся телефонных и радиопереговоров;

- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств.

Можно заметить, что все каналы утечки информации, кроме последних двух, являются весьма специфическими, съем информации возможен только при использовании специального, часто очень дорогого оборудования. Поэтому важно понимать, что затраты на организацию защиты информации должны быть соразмерны величине ущерба, который может быть нанесен собственнику информационных ресурсов.

КЗ называют территорию, на которой исключено несанкционированное и неконтролируемое пребывание лиц и транспортных средств, которые могут быть потенциальными носителями средств перехвата информации. С изложенных выше позиций КЗ должна иметь определенные размеры, а положение ее границы на местности должно соответствовать условиям, исключающим возможность приема и регистрации опасных сигналов средствами перехвата информации. На практике используют два подхода к определению размеров КЗ. Первый из них предполагает нормативное установление, в зависимости от категории защищаемого объекта, таких размеров КЗ, при которых гарантированно исключается возможность ведения разведки ПЭМИН. Второй подход основан на учете состава технических средств передачи и обработки информации (ТСПИ) защищаемого объекта и расчете для каждого из них радиуса R2, так называемой «Зоны 2», т.е.

расстояния на котором отношение сигнал/помеха исключает возможность приема и регистрации средствами разведки ПЭМИН опасных сигналов различной физической природы [20] (рисунок 3).

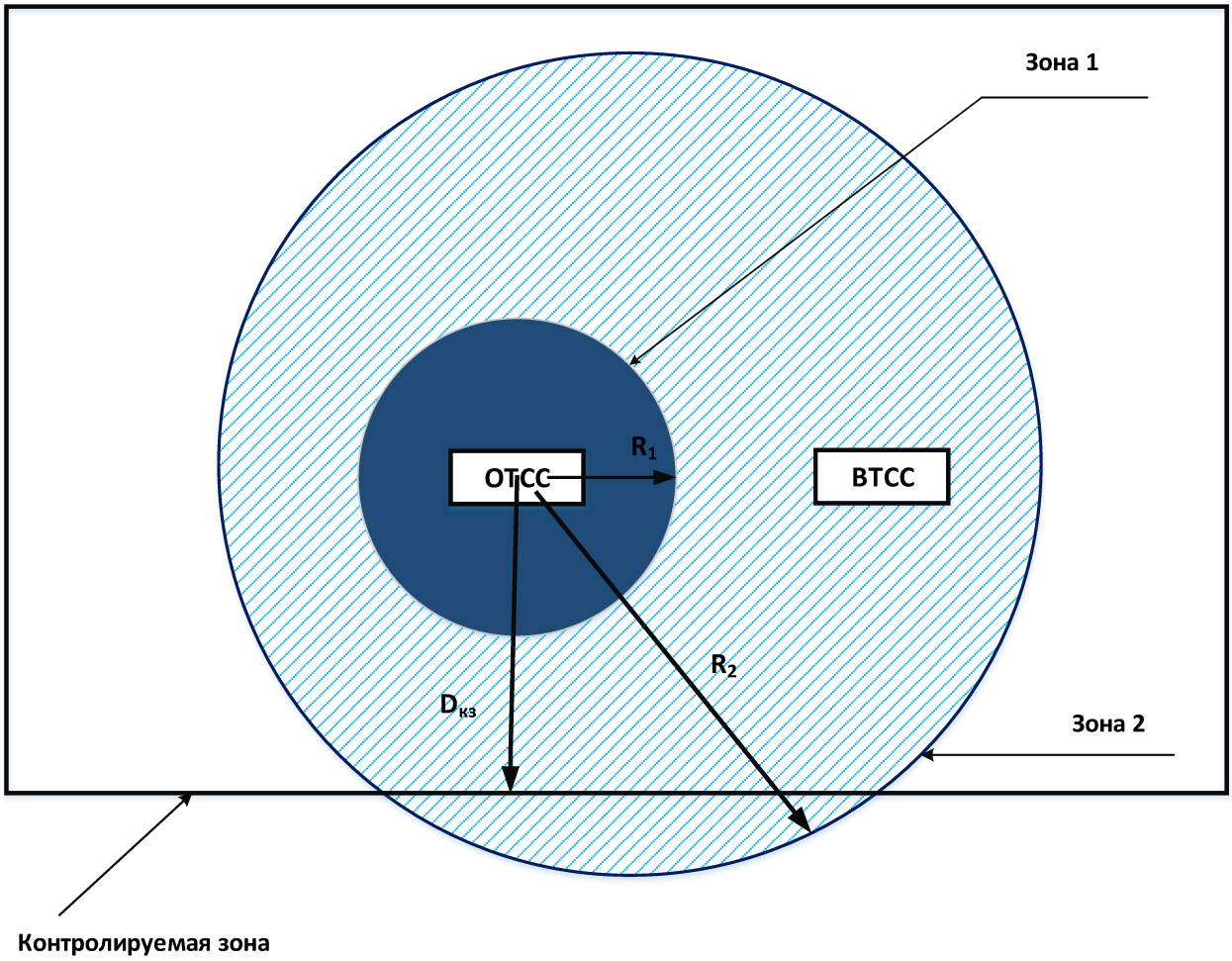

Рисунок 3. Схема уровней контролируемых зон. $D_{кз}$— расстояние от ОТСС до границы контролируемой зоны

Оба названных подхода дают максимальный, с точки зрения защиты информации, эффект при их реализации на этапах проектирования и строительства объектов, когда установленные или рассчитанные нормативы по размерам КЗ могут быть заложены в проектную и монтажную документацию, а ее границы на местности оборудованы соответствующими ограждениями и пропускными пунктами.

Однако на практике часто объекты защиты создаются не в специально построенных, а в приспособленных зданиях и сооружениях, имевших ранее другое предназначение. Это значительно усложняет, а иногда и вообще исключает, возможность установления КЗ требуемого размера, приводит к тому, что граница КЗ может проходить непосредственно на наружной стороне стен используемых зданий и сооружений. В этом случае необходимо принимать специальные меры, обеспечивающие доведение отношения опасного сигнала к помехам на границе КЗ до уровня, исключающего

возможность его приема и регистрации аппаратурой перехвата. Одной из наиболее действенных в этом отношении мер является пространственное зашумление объектов защиты за счет применения специальных генераторов шума различных диапазонов.

Вместе с тем даже при правильном организационном и техническом решении вопросов установления границ контролируемой зоны, существует реальная необходимость дифференцированного применения способов и мер защиты, особенно на комплексных объектах ТСПИ. Объективной предпосылкой для такой дифференциации являются принципиальные различия по конструкции и предназначению отдельных ТСПИ, как источников опасных сигналов (ОС), по причинам возникновения и формам проявления технических каналов утечки информации.

Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;
- при посещении учреждения (предприятия) посторонними лицами;
- за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

ПЭМИН – это паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники. В зависимости от среды распространения различают:

- электромагнитные каналы утечки информации, однородная среда распространения – эфир;
- электрические каналы утечки информации, неоднородная среда распространения – эфир и линии ВТСС, в том числе и проникновение их от ОТСС в отходящие линии.

В электромагнитных каналах утечки информации носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами.

Побочные электромагнитные излучения (ПЭМИ) – нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации.

Информативными ПЭМИ называются сигналы, представляющие собой ВЧ несущую, модулированную информацией, обрабатываемой на СВТ (например, изображением, выводимым на экран монитора, данными, обрабатываемыми на устройствах ввода-вывода и т.д.).

Неинформативными ПЭМИ называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ.

Основными причинами возникновения электромагнитных каналов утечки информации в технических средствах обработки информации (ТСОИ)

являются:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ (гетеродины, генераторы подмагничивания и стирания, задающие генераторы);
- модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Практически все компоненты СВТ во время работы являются источниками возникновения ПЭМИ:

- процессор, шина данных процессора и цепи питания;
- контроллеры и мост чипсета;
- модули памяти и шина данных;
- инверторы питания перечисленных выше устройств;
- HDD, SDD и шины IDE (ATA) и SATA;
- CD и шина IDE (ATA);
- видеокарта и шина AGP или E-PCI;
- COM порт и внешние подключения по нему;
- LTP порт и внешние подключения по нему;
- USB порт;
- VGA, HDMI, DVI и другие виды портов, предназначенные для подключения мониторов;
- беспроводные сетевые адаптеры IEEE 802 для локальных сетей.

Причинами возникновения электрических каналов утечки информации являются наводки информативных сигналов, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, емкостными и индуктивными связями.

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить на:

- наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными ПЭМИ ТСОИ (ПЭМИ – ток в проводнике);
- наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними емкостными и индуктивными связями («просачивание» информативных сигналов в цепи электропитания через блоки питания ТСОИ, ток – ток);
- наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ (ПЭМИ – ток в проводнике, ток – ток).

Информация в процессе обработки СВТ проходит через ряд режимов ее преобразования, передачи и отображения. Наиболее потенциально опасными

из них являются:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на машинный носитель информации (МНИ);
- чтение информации с МНИ;
- передача данных в каналы связи;
- вывод данных на печатающие устройства;
- записи данных от сканера на МНИ.

Возможность перехвата информации средствами перехвата ПЭМИН зависит о вида технического средства и составляет:

- мониторы с электронно-лучевой трубкой – десятки, сотни метров;
- жидкокристаллические мониторы – единицы, десятки метров;
-  – единицы метров;
- принтеры, сканеры, многофункциональное устройства – десятки метров;
- клавиатура – десятки, сотни метров;
- Flash-накопители, внешние HDD – без удлинителя – единицы, с удлинителем – десятки метров.

Указанные расстояния являются примерными и для конкретного объекта могут отличаться как в меньшую, так и в большую стороны.

Способы перехвата конфиденциальной информации, обрабатываемой техническими средствами:

1. Перехват ПЭМИ (магнитные и электрические антенны):

- перехват ПЭМИ, возникающих вследствие протекания по ТСОИ переменного электрического тока;
- перехват ПЭМИ, возникающих вследствие работы ВЧ-генераторов, входящих в состав ТСОИ;
- перехват ПЭМИ, возникающих вследствие паразитной генерации.

2. Перехват наводок информативных сигналов (широкополосные токосъемники и пробники):

- перехват наводок информационных сигналов в соединительных линиях ВТСС и посторонних проводников;
- перехват наводок информационных сигналов с линий электропитания ТСОИ;
- перехват наводок информационных сигналов с цепей заземления ТСОИ.

3. Перехват путем «высокочастотного облучение» ТСОИ (специальная аппаратура).

4. Перехват от внедренных в ТСОИ электронных устройств негласного съема информации.

Способами перехвата акустической речевой информации являются:

1. Перехват информации по прямому акустическому каналу утечки:

- запись речевой информации скрытно установленными портативными средствами звукозаписи;

- скрытая установка передающих закладных устройств с датчиками микрофонного типа;

- прослушивание (запись) разговоров направленными микрофонами.

2. Перехват информации по виброакустическому каналу утечки:

- скрытое прослушивание (запись) разговоров из смежных помещений с использованием электронных стетоскопов;

- скрытая установка в смежных помещениях передающих закладных устройств с датчиками контактного типа.

3. Перехват информации по прямому акустоэлетромагнитному каналу утечки:

- перехват ПЭМИ на частотах работы ВЧ-генераторов, входящих в состав ВТСС, обладающих «микрофонным эффектом»;

- ВЧ-облучение ВТСС, обладающих «микрофонным эффектом».

4. Перехват информации по акустоэлектрическому каналу утечки:

- подключение специальных НЧ-усилителей к соединительным линиям ВТСС, обладающих «микрофонным эффектом»;

- подключение аппаратуры «ВЧ-навязывания» к соединительным линиям ВТСС, обладающим «микрофонным эффектом».

5. Перехват информации по акустооптическому (лазерному) каналу утечки – облучение оконных стекол лазерными акустическими системами разведки.

Рассмотрим возможные каналы утечки информации в волоконно-оптических линиях связи (ВОЛС). ВОЛС имеют более высокую степень защищённости информации от несанкционированного доступа, чем какие-либо иные линии связи. Дело в том, что в оптическом волноводе электромагнитное излучение выходит за пределы волокна на расстояние не более длины волны (физический принцип распространения электромагнитной волны в световоде) при отсутствии внешнего воздействия на оптоволокно.

Неправомерное получение информации, ее искажение, уничтожение и блокирование возможны также в результате несанкционированного доступа к информации и негативных воздействий на нее в средствах вычислительной техники и автоматизированных системах.

Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее должно приводиться в Модели угроз безопасности информации, разрабатываемой в организации.

Для добывания конфиденциальных сведений могут использоваться:

- портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки ПЭМИН;

- автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

- компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

Угроза компьютерной разведки объектам защиты возможна в случае

подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь – глобальным, сетям.

Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий администрации (организации). Такая аппаратура маскируется и перевозится в чемоданах, портфелях, атташе-кейсах, упаковочных коробках и т.п.

Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.

Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

Несанкционированный доступ (НСД) к информации и специальные воздействия на нее могут осуществляться при ее обработке в отдельных СВТ, в локальных вычислительных сетях администрации, в региональных и глобальных телекоммуникационных системах [21].

Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
- просмотра информации с экранов дисплеев и других средств ее отображения.

Наиболее опасной является аппаратура портативной (возимой и носимой) разведки рабочих электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям организации территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри здании организации.

Оценка возможности НСД к информации в СВТ и АС осуществляется с использованием следующих руководящих документов ФСТЭК России:

- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- Руководящий документ «Автоматизированные системы. Защита от

несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации».

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в АС [21].

Доступ к информации как с территории России, так и из-за ее пределов, может позволить на основе анализа и статистической обработки получать сведения конфиденциального характера.

2.2. Организационные и технические мероприятия по защите конфиденциальной информации

Мероприятия по технической защите конфиденциальной информации являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ [22, 23]. Основные понятия предметной области «Защита информации» установлены стандартом ГОСТ Р 50922–96, а также в Руководящих документах ФСТЭК России (Приложение 3).

Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации – 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.

Для защиты информации в информационных системах могут быть сформулированы следующие принципы [24]:

1. Законность и обоснованность защиты.

Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.

2. Системность.

Системный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- при всех видах информационной деятельности и информационного

проявления;

- во всех структурных элементах;
- при всех режимах функционирования;
- на всех этапах жизненного цикла;
- с учетом взаимодействия объекта защиты с внешней средой.

С позиций системного подхода к защите информации предъявляются определенные требования:

- обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявления ее узких и слабых мест и противоправных действий;
- безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах экономической системы и на всех этапах технологического цикла обработки информации;
- планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции;
- защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам;
- эффективность защиты информации означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз;
- четкость определения полномочий определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;
- учет случаев и попыток несанкционированного доступа к конфиденциальной информации; обеспечение степени конфиденциальной информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

При обеспечении безопасности информационной системы необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и пути несанкционированного доступа к информации. Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз

безопасности.

2. Комплексность защиты.

Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

4. Непрерывность защиты.

Защита информации – это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

5. Разумная достаточность.

Создать абсолютно непреодолимую систему защиты принципиально невозможно: при достаточных времени и средствах можно преодолеть любую защиту. Следовательно, возможно достижение лишь некоторого приемлемого уровня безопасности. Высокоэффективная система защиты требует больших ресурсов (финансовых, материальных, вычислительных, временных) и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

6. Гибкость.

Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью.

7. Открытость алгоритмов и механизмов защиты.

Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты. Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна, необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

8. Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат обязательному учету и защите.

Режим защиты конфиденциальной информации устанавливается

собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации, при ее использовании в управлении экологически опасными объектами. В остальных случаях проводится добровольная сертификация.

Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении. Для сведений, составляющих служебную тайну не ниже требований, установленных «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации» (СТР-К) и государственными стандартами Российской Федерации.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией без принятия необходимых мер технической защиты информации не допускается.

Объектами защиты в подразделениях ОВД являются:

- средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки конфиденциальной информации – ОТСС;

- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует) – ВТСС;

- помещения (служебные кабинеты, актовые, конференц-залы и т.п.),

специально предназначенные для проведения конфиденциальных мероприятий, – защищаемые помещения (ЗП).

Ответственность за выполнение требований СТР-К возлагается на начальника ОВД, начальников подразделений, начальника отдела безопасности защиты конфиденциальной информации, а также на специалистов, допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

Непосредственное руководство работами по защите конфиденциальной информации осуществляет руководитель организации.

Защита конфиденциальной информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в соответствии со СТР-К в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации.

Защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе.

Защита информации на объекте информатизации достигается выполнением комплекса мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств [3, 25].

Разработка мер и обеспечение защиты конфиденциальной информации осуществляются подразделением по защите конфиденциальной информации (службой безопасности) или отдельными специалистами, назначаемыми руководителем организации для проведения таких работ [26, 27]. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности технические средства защиты. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России (Приложение 3).

Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя ОВД, эксплуатирующего объекты информатизации.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки) в

соответствии с нормативными документами ФСТЭК России.

2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП (далее – сотрудники), ответственными за безопасность информации.

3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

4. Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения.

5. Инструктирование сотрудников, работающих в ЗП, о правилах эксплуатации ЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

6. Проведение в ЗП обязательных визуальных (непосредственно перед совещаниями) и инструментальных (перед ответственными совещаниями и периодически раз в квартал) проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП.

7. Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре.

8. Оснащение телефонных аппаратов городской АТС, расположенных в ЗП, устройствами высокочастотной развязки подавления слабых сигналов, а также поддержание их в работоспособном состоянии. Для спаренных телефонов достаточно одного устройства на линию, выходящую за пределы ЗП. Оснащение телефонов городской АТС в ЗП первой группы (категории) и телефонов основных абонентов специальными шифраторами (скремблерами).

9. Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах.

10. Обеспечение требуемого уровня звукоизоляции входных дверей ЗП для чего:

- входные двери обиваются звукоизолирующим материалом (например, войлоком), обеспечивается плотное их прилегание без щелей и перекосов к дверной коробке;
- устанавливаются пороги;
- притворы уплотняются специальным шнуром по ГОСТ 10174-72 или пористой резиной;
- щели между дверной коробкой и стеной заделываются прокладками по ГОСТ 10174-72 «Прокладки уплотняющие пенополиуретановые»;
- двери ЗП первой и второй категории оснащаются тамбурами, внутренние отсеки тамбуров обиваются звукоизолирующим материалом (например, войлоком).

11. Обеспечение требуемого уровня звукоизоляции окон ЗП для чего:

- заделываются щели между оконными коробками и стенами;
- проводится регулярный осмотр оконных стекол, стекла, имеющие трещины и сколы, заменяются на новые, которые устанавливаются либо на

герметизирующую замазку, либо на виброизолирующую прокладку без щелей и перекосов;

- окна оснащаются сплошными шторами из плотной портьерной ткани или жалюзи;
- окна ЗП первой и второй категории оснащаются системой активного зашумления.

12. Демонтирование или заземление (с обеих сторон) лишних экранов кабеля.

13. Отключение при проведении совещаний в ЗП всех неиспользуемых электро- и радиоприборов от сетей питания и трансляции.

14. Выполнение перед проведением совещаний следующих условий:

- окна должны быть плотно закрыты и зашторены;
- двери плотно прикрыты;
- в ЗП первой и второй категории должны быть включены системы активного зашумления.

К основным мероприятиям по технической защите конфиденциальной информации в ОТСС и ВТСС относятся:

- размещение ВТСС (телефонных аппаратов, громкоговорителей и т.п.) за пределами зоны (зоны 1), в которой возможно создание электромагнитными излучениями работающих ОТСС наводок информативного сигнала на ВТСС. При невозможности выполнения этого требования для телефонных аппаратов их следует оснастить безразрывными розетками и отключать от телефонной сети на период обработки конфиденциальной информации;
- размещение за пределами зоны 1 «случайных распределенных антенн» (линий электропитания, сигнализации, телефонных сетей и т.п.), имеющих выход за границу контролируемой зоны. При невозможности выполнения этого требования для конкретной линии ее следует демонтировать (перенести), экранировать, заземлить с обеих сторон или зашунтировать емкостью;
- оборудование помещений, в которых эксплуатируются ОТСС, системой заземления, осуществляемой по схеме ветвящегося дерева, не имеющей замкнутых контуров. Заземлители должны располагаться в пределах контролируемой зоны на расстоянии от ее границы и от подземных коммуникаций (водопровода, кабелей и т.п.), имеющих выход за пределы контролируемой зоны, не менее требуемого нормативными документами. В противном случае необходимо использовать глубинные заземлители;
- обеспечение электропитания ОТСС от автономного источника питания, расположенного в пределах контролируемой зоны, (трансформаторной подстанции с заземленной нулевой точкой, системы «двигатель-генератор»), либо от городской сети электропитания с использованием развязывающих фильтров для подключения ОТСС к сети электропитания, обеспечивающих требуемое затухание.

При невозможности обеспечения контролируемой зоны заданных размеров рекомендуется одно из следующих мероприятий:

- проведение частичной экранировки помещения. В первую очередь

подлежат экранировке наиболее распространенные элементы: окна, двери, вентиляционные и другие отверстия в стенах, полу и потолке помещения. В случае необходимости, проводится экранировка стен, пола и потолка;

- применение систем электромагнитного пространственного зашумления (СПЗ) в районе размещения защищаемого ОТСС;
- применение средств линейного электромагнитного зашумления (СЛЗ) линий электропитания, радиотрансляции, заземления, связи.

Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются действующими государственными стандартами и другими нормативными и методическими документами ФСТЭК России.

Основными путями проникновения вирусов в АС могут являться:

- внешние носители информации, переносные (съемные) HDD, Flash Hard Drive, Zip Drive, магнитооптические (МО) и т.п.);
- оптические диски;
- электронная почта;
- файлы, получаемые из сети Internet/Intranet;
- ранее инфицированные рабочие станции;
- ранее инфицированные файл-серверы;
- ранее инфицированные серверы локальной вычислительной сети.

Организации антивирусной защиты информации на объектах информатизации достигается путем:

- внедрения средств антивирусной защиты информации;
- применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

Организация работ по антивирусной защите информации возлагается на руководителей структурных подразделений и должностных лиц, осуществляющих контроль за антивирусной защитой, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на руководителя подразделения по защите конфиденциальной информации (службы безопасности) организации.

Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации машинных носителей информации, информационных массивов, программных средств общего и специального назначения;
- периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе гибких магнитных дисков перед началом работы с ними на отсутствие

программных вирусов;

- внеплановая проверка магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

К использованию допускается только лицензированные антивирусные средства защиты. В связи с неопределенным порядком сертификации этих средств рекомендуется использовать только отечественные средства, а также средства, централизованно закупленные у разработчиков указанных средств, либо их официальных дилеров.

Установка средств антивирусного контроля на серверах и рабочих станциях осуществляется сотрудниками подразделения автоматизации в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС», которая определяет меры безопасности при вводе в эксплуатацию новых рабочих станций и серверов, а также при изменении конфигурации технических и программных средств существующих в АС компьютеров.

Порядок применения средств антивирусной защиты, учитывающий особенности объекта информатизации и выполняемых на данном объекте работ, определяется инструкцией по антивирусной защите конфиденциальной информации.

В разделе должны быть определены:

- должностные лица, ответственные за получение, рассылку, установку, поддержание в работоспособном состоянии и использование средств антивирусной защиты (назначаются приказом);
- должностные лица, осуществляющие контроль над организацией антивирусной защиты (назначаются приказом);
- порядок установки и применения средств антивирусной защиты;
- порядок ликвидации последствий воздействий программных вирусов.

В общем случае инструкция по антивирусной защите конфиденциальной информации должна включать в себя:

- инструкцию по защите конфиденциальной информации на рабочих станциях.
- инструкцию по защите конфиденциальной информации на почтовых серверах.
- инструкцию по защите конфиденциальной информации на файл-серверах.
- инструкцию по защите конфиденциальной информации на серверах локальной вычислительной сети.

Состояние вопросов антивирусной защиты отражается в отчете о состоянии обеспечения информационной безопасности в администрации с обязательным указанием выявленных нарушений, вызванных заражением программными вирусами, описанием причин появления вирусов, характера и

последствий их воздействия и принятых мерах.

Организация антивирусной защиты информации должна быть направлена на предотвращение заражения отдельных компьютеров, рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения компьютерными вирусами.

Защита информации должна осуществляться посредством применения многоуровневой системы антивирусной защиты. Особое внимание необходимо уделить постоянному обновлению вирусных баз и непосредственно самих версий антивирусного программного обеспечения. Частота обновления антивирусных вирусных баз и версий антивирусных программ семейства:

- горячие обновления – выпускаются несколько раз в день нарастающим итогом;
- еженедельные дополнительные вирусные базы – один раз в неделю (обычно по понедельникам);
- новые версии программ – в среднем один раз в полтора-два месяца.

Конкретная система антивирусной защиты должна разрабатываться с учетом особенностей конкретных локальных вычислительных сетей и, в общем случае, должна включать в себя:

- антивирусную защиту рабочих станций;
- антивирусную защиту почтовых серверов;
- антивирусную защиту серверов;
- возможность автоматического обновления вирусных баз и версий.

Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

- входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения;
- входной антивирусный контроль всей информации, поступающей с электронной почтой;
- входной антивирусный контроль всей поступающей информации из сети Internet/Intranet;
- выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а также передача информации посредством электронной почты;
- периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;
- обязательная антивирусная проверка используемых в работе внешних носителей информации.
- постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;
- обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

- внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

- восстановление работоспособности программных и аппаратных средств, а также непосредственно информации в случае их повреждения компьютерными вирусами;

- порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта;

- вся поступающая в администрацию (организацию) информация, полученная по модемной связи, а также информации на магнитных носителях (программные средства общего и специального назначения, информационные массивы) подлежит обязательной проверке на наличие программных вирусов;

- о произведенной проверке и ее результатах делается отметка на сопроводительном письме (акте, аппаратном журнале и т.п.) пользователем, производившим проверку;

- при обнаружении на внешних носителях или в полученных файлах вредоносного программного обеспечения пользователи докладывают об этом в подразделение по защите конфиденциальной информации, и принимают меры по восстановлению работоспособности программных средств и данных;

- о факте обнаружения программных вирусов сообщается в органы, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов;

- перед отправкой массивов информации и программных средств осуществляется ее проверка на наличие программных вирусов. В тексте сопроводительного письма (аппаратном журнале, техническом журнале и т.п.) указывается, что проверка на наличие программных вирусов информации произведена;

- при обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на ПЭВМ, поставить в известность подразделение информационно-технической службы органа власти по защите конфиденциальной информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты;

- при функционировании ПЭВМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети;

- ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями подразделения информационно-технической службы органа власти по защите конфиденциальной информации;

- программные средства общего и специального назначения объекта информатизации, осуществляющие обработку служебной информации ограниченного распространения, подлежат обязательной переустановке с рабочих копий эталонных накопителей информации независимо от результатов по удалению выявленных программных вирусов имеющимися

средствами антивирусной защиты;

- при обнаружении программных вирусов, ликвидацию которых имеющимися средствами антивирусной защиты осуществить невозможно, ставится в известность разработчик антивирусных программ. Файлы с внедренными программными вирусами архивируются и представляются на дискетах с пометкой: «Осторожно! Программные вирусы!»;
- при наличии в организации возможности отправки электронной почты заархивированные зараженные файлы с сопроводительным документом направляются разработчику средств антивирусной защиты;
- восстановление работоспособности объекта информатизации в этих случаях производится путем полной переустановки программных средств с использованием рабочих копий эталонных дискет и резервных копий файлов с данными (которые должны регулярно обновляться).

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на системного администратора.

Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих: буквы в верхнем регистре и буквы в нижнем регистре, цифры, специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, *, % и т.п.).
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, имя учетной записи пользователя и т.д.), а также общепринятые сокращения;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.);
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Формирование личных паролей пользователей осуществляется централизованно. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

Полная плановая смена паролей пользователей должна проводиться регулярно. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры.

Хранение сотрудником значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором Touch Memory).

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности подразделения, периодический контроль – на специалиста по защите информации или ответственного сотрудника [25, 26].

2.3. Содержание и основы организации защиты конфиденциальной информации в автоматизированных системах от несанкционированного доступа

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах, наносят серьезный материальный и моральный урон многим органам, организациям и подразделениям системы МВД России, участвующим в процессах автоматизированного информационного взаимодействия [27].

Жизненно важные интересы этих органов, организаций и подразделений, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их безопасности, экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования или уничтожения.

Проблема защиты вычислительных систем становится еще более серьезной и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам.

В качестве возможных нежелательных воздействий на компьютерные системы должны рассматриваться: преднамеренные действия злоумышленников, ошибочные действия обслуживающего персонала и пользователей системы, проявления ошибок в ее программном обеспечении,

сбои и отказы оборудования, аварии и стихийные бедствия. Результаты анализа типовых угроз безопасности АС ОВД приведены в Приложении 4.

В качестве защищаемых объектов должны рассматриваться информация и все ее носители (отдельные компоненты и АС обработки информации в целом).

Обеспечение безопасности вычислительной системы предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также для попыток хищения, модификации, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов системы: оборудования, программного обеспечения, данных (информации) и ее персонала.

В этом смысле защита информации от НСД является только частью общей проблемы обеспечения безопасности компьютерных систем и защиты законных интересов субъектов информационных отношений, а сам термин НСД было бы правильнее трактовать не как «несанкционированный доступ» (к информации), а шире, – как «несанкционированные (неправомерные) действия», наносящие ущерб субъектам информационных отношений.

В соответствии с ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения» под АС обработки информации понимается организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения АС обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Под обработкой информации в АС понимается любая совокупность операций (прием, сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Субъекты по отношению к определенной информации могут выступать в качестве: источника информации; пользователя информации; владельцев информации; физических и юридических лиц, о которых собирается информация и т.д.

Будучи заинтересованным в обеспечении конфиденциальности, целостности и доступности информации субъект информационных отношений является уязвимым, то есть потенциально подверженным нанесению ему ущерба (прямого или косвенного, материального или морального) посредством воздействия на критичную для него информацию и ее носители

либо посредством неправомерного использования такой информации. Поэтому все субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности.

Поскольку ущерб субъектам информационных отношений может быть нанесен опосредованно, через определенную информацию и ее носители (в том числе АС обработки информации), то закономерно возникает заинтересованность субъектов в обеспечении безопасности этой информации и систем ее обработки и передачи. Иными словами, в качестве объектов, подлежащих защите в интересах обеспечения безопасности субъектов информационных отношений, должны рассматриваться: информация, ее носители и процессы ее обработки.

Однако уязвимыми в конечном счете являются именно заинтересованные в обеспечении определенных свойств информации и систем ее обработки субъекты (информация, равно как и средства ее обработки, не имеет своих интересов, которые можно было бы ущемить и нанести тем самым ущерб). В дальнейшем, говоря об обеспечении безопасности АС ОВД или циркулирующей в системе информации, всегда будем понимать под этим косвенное обеспечение безопасности субъектов, участвующих в процессах автоматизированного информационного взаимодействия [23].

В свете сказанного, термин «безопасность информации» нужно понимать, как защищенность информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Поскольку субъектам информационных отношений ущерб может быть нанесен также посредством воздействия на процессы и средства обработки критичной для них информации, то становится очевидной необходимость обеспечения защиты всей системы обработки и передачи данной информации от несанкционированного вмешательства в процесс ее функционирования, а также от попыток хищения, незаконной модификации и/или разрушения любых компонентов данной системы.

Поэтому под безопасностью АС обработки информации, эксплуатируемой на объекте информатизации ОВД (компьютерной системы), будем понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных и персонала) от подобного рода нежелательных для соответствующих субъектов информационных отношений воздействий [28].

Безопасность любого компонента (ресурса) АС ОВД складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента системы предполагает, что он может быть

модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

В свете приведенного выше подчеркнем, что конечной целью защиты АС ОВД и циркулирующей в ней информации является предотвращение или минимизация наносимого субъектам информационных отношений ущерба (прямого или косвенного, материального, морального или иного) посредством нежелательного воздействия на компоненты АС ОВД, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

Наибольшую сложность при решении вопросов обеспечения безопасности конкретных информационно-управляющих систем (информационных технологий) представляет задача определения реальных требований к уровням защиты критичной для субъектов информации, циркулирующей в АС ОВД. Ориентация на интересы субъектов информационных отношений дает ключ к решению данной задачи для общего случая.

Исторически сложившийся подход к классификации государственной информации (данных) по уровням требований к ее защищенности основан на рассмотрении и обеспечении только одного свойства информации – ее конфиденциальности (секретности). Требования же к обеспечению целостности и доступности информации, как правило, лишь косвенно фигурируют среди общих требований к системам обработки этих данных. Считается, что раз к информации имеет доступ только узкий круг доверенных лиц, то вероятность ее искажения (несанкционированного уничтожения) незначительна. Низкий уровень доверия к АС и предпочтение к бумажной информационной технологии еще больше усугубляют ограниченность данного подхода.

Если такой подход в какой-то степени оправдан в силу существующей приоритетности свойств безопасности важной государственной информации, то это вовсе не означает, что его механический перенос в другую предметную область (с другими субъектами и их интересами) будет иметь успех.

Во многих областях деятельности (предметных областях) доля конфиденциальной информации сравнительно мала. Для служебной и персональной информации, равно как и для коммерческой информации, не подлежащей засекречиванию, приоритетность свойств безопасности информации может быть иной [29]. Для открытой информации, ущерб от разглашения которой несущественен, важнейшими могут быть такие качества, как доступность, целостность или защищенность от неправомерного тиражирования.

Требования к системе защиты АС ОВД в целом (методам и средствам защиты) должны определяться, исходя из требований к защищенности

различных типов информационных пакетов, обрабатываемых в данных АС с учетом особенностей конкретных технологий их обработки и передачи (уязвимостей) [21].

Требования к уровню защищенности критичных свойств информационных пакетов различных типов (документов, справок, отчетов и т.п.) в конкретной предметной области должны устанавливаться ее владельцами (собственниками) или другими субъектами информационных отношений на основе анализа серьезности последствий нарушения каждого из свойств информации (типов информационных пакетов): доступности, целостности и конфиденциальности.

Прежде чем переходить к рассмотрению основных задач и подходов к построению систем защиты, призванных обеспечить надлежащий уровень безопасности субъектов информационных отношений, надо уточнить, от какого рода нежелательных воздействий необходимо защищать информацию и АС ее обработки и передачи на объектах информатизации ОВД.

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является определение, анализ и классификация возможных угроз безопасности АС ОВД (Приложение 4). Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты АС, эксплуатируемых на объектах информатизации ОВД.

Как показывает анализ, большинство современных АС ОВД в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных АС ОВД возможны все «традиционные» для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации. Кроме того, для них характерны и новые специфические каналы проникновения в систему и НСД к информации, наличие которых объясняется целым рядом их особенностей.

Перечислим основные особенности распределенных АС ОВД [3]:

- территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;
- широкий спектр используемых способов представления, хранения и передачи информации;
- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;
- абстрагирование владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе автоматизированной обработки информации

большого количества пользователей и персонала различных категорий;

- непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;
- отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД.

В общем случае АС ОВД состоят из следующих основных структурно-функциональных элементов:

- рабочих станций – отдельных ЭВМ или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места (АРМ) пользователей (абонентов, операторов);
- серверов или Host-машин (служб файлов, печати, баз данных и т.п.) не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;
- межсетевых мостов (шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) – элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;
- каналов связи (локальных, телефонных, с узлами коммутации и т.д.).

Рабочие станции являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей [6].

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей как серверы (Host-машины) и мосты. Первые – как концентраторы больших объемов информации, вторые – как элементы, в которых осуществляется преобразование (возможно через

открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, наличие возможностей по их надежной защите физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала сети, имеющих непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и преднамеренные воздействия злоумышленников на выделенные серверы и мосты можно считать маловероятными. В то же время, надо ожидать массированной атаки на серверы и мосты с использованием средств удаленного доступа. Здесь злоумышленники прежде всего могут искать возможности повлиять на работу различных подсистем серверов и мостов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Использоваться могут все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (каналы, как правило, слабо защищены от подключения) и применения высококлассных программ для преодоления системы защиты.

Конечно, сказанное выше не означает, что не будет попыток внедрения аппаратных и программных закладок в сами мосты и серверы, открывающих дополнительные широкие возможности по несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных. Возможные при этом угрозы подробно изложены ниже.

Под угрозой (в широком смысле) обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угрозой интересам субъектов информационных отношений на объекте информатизации ОВД будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты АС ОВД может прямо или косвенно привести к нанесению ущерба интересам данных субъектов [25].

В силу перечисленных выше особенностей современных АС, эксплуатируемых в защищенном исполнении на объектах инфоматизации ОВД, существует значительное число различных видов угроз безопасности субъектов информационных отношений.

Нарушением безопасности (или просто нарушением) будем называть реализацию угрозы безопасности.

Основными видами угроз безопасности АС ОВД и информации (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);

- сбои и отказы оборудования (технических средств) АС ОВД;

- последствия ошибок проектирования и разработки компонентов АС ОВД (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);

- ошибки эксплуатации (пользователей, операторов и другого персонала);

- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, террористов и т.п.).

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Непреднамеренные угрозы безопасности АС ОВД (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному отказу системы, либо к разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

- неправомерное отключение оборудования или изменение режимов работы устройств и программ;

- неумышленная порча носителей информации;

- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- заражение компьютера вирусами;

- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

- проектирование архитектуры системы, технологии обработки данных,

разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

- игнорирование организационных ограничений (установленных правил) при работе в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и осуществления НСД к информации:

- физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов АС ОВД (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
- внедрение агентов в число персонала системы (в том числе и в административную группу, отвечающую за безопасность);
- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых персональных ЭВМ);
- несанкционированное копирование носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- чтение остаточной информации из оперативной памяти и с внешних

запоминающих устройств;

- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

- вскрытие шифров криптозащиты информации;

- внедрение аппаратных спецвложений, программных «закладок» и «вирусов» («троянских коней» и «жучков»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

- незаконное подключение к линиям связи с целью работы «между строк» с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Каналы преднамеренной утечки конфиденциальной информации могут быть самыми разнообразными, например:

- установление злоумышленником дружеских контактов с сотрудниками ОВД;

- профессиональный анализ информации, имеющейся в открытой печати;

- поступление на работу в ОВД с целью получения открытого доступа к интересующей злоумышленников служебной информации;

- работа с информационными сетями;

- криминальный доступ к информации (кража документов, шантаж должностных лиц, подкуп).

Утечка информации может носить и непреднамеренный характер, например: случае неумышленного уничтожения документа; незнания сотрудником порядка работы с секретными документами; излишней

болтливости сотрудников, ведения ненужных кулуарных разговоров по служебным проблемам; работы с конфиденциальными документами в присутствии посторонних; неосторожного использования секретной информации в неслужебной переписке; самовольного копирования документов для большей комфортности в работе.

При движении конфиденциальных документов по инстанциям увеличивается число источников информации (сотрудников, баз данных, рабочих материалов и т.п.), обладающих ценными сведениями, и расширяются потенциальные возможности для утраты конфиденциальной информации, ее разглашения сотрудниками, утечки по техническим каналам, исчезновения носителя этой информации [27].

Каналы утраты конфиденциальной документированной информации имеются на всех стадиях и этапах движения документов, при выполнении любых процедур и операций. К ним относятся:

- кража (хищение) документа или отдельных его частей (листов, приложений, копий, схем, фотографий и др.), носителя чернового варианта документа или рабочих записей;
- несанкционированное копирование бумажных и документов, баз данных, фото-, видео-, аудиодокументов, запоминание злоумышленником или его сообщником текста документа;
- тайное или разрешенное ознакомление сотрудника ОВД с документом и сообщение информации злоумышленнику лично или по линиям связи, прочтение текста документа по телефону или переговорному устройству, разглашение информации с помощью мимики, жестов, условных сигналов;
- подмена документов, носителей и их отдельных частей с целью фальсификации или сокрытия факта утери, хищения;
- дистанционный просмотр документов и изображений дисплея с помощью технических средств визуальной разведки;
- ошибочные (умышленные или случайные) действия персонала при работе с документами (нарушение разрешительной системы доступа, обращения с документами, технологии их обработки и хранения);
- случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов;
- считывание данных в чужих массивах за счет использования остаточной информации на копировальной ленте, бумаге, дисках и дискетах;
- утечка информации по техническим каналам при обсуждении и диктовке текста документа, работе с компьютером и другой офисной техникой;
- гибель документов в условиях экстремальных ситуаций.

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные [28]. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо. Прямые каналы могут использоваться без

внесения изменений в компоненты системы или с изменениями компонентов.

По типу основного средства, используемого для реализации угрозы, все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

Классификация видов нарушений работоспособности АС ОВД и НСД к информации по объектам воздействия и способам нанесения ущерба безопасности приведена в таблице 3.

По способу получения информации потенциальные каналы доступа можно разделить на:

- физический;
- электромагнитный (перехват излучений);
- информационный (программно-математический).

Таблица 3

Основные способы нанесения ущерба объектам АС ОВД

Способы нанесения ущерба	Объекты воздействий			
	Оборудование	Программы	Данные	Персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкциониро-ванное использование ресурсов	Несанкциони-рованное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкциониро-ванное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности АС ОВД	Изменение режимов функционирова-ния, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использова-ние незаконных копий	Публикация без ведома авторов	

В соответствии с Руководящим документом ФСТЭК России «Защита от

несанкционированного доступа к информации. Термины и определения», НСД – это доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам АС ОВД, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также путем подключения к линиям связи.

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АС ОВД, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографированием) устройств отображения информации, прослушиванием переговоров персонала АС ОВД и пользователей.

Таким образом, специфика распределенных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

Уязвимыми являются буквально все основные структурно-функциональные элементы распределенных АС ОВД: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи.

Защищать компоненты АС ОВД необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов путей преднамеренного или случайного НСД к данным и вмешательства в процессы обработки и обмена информацией (в том числе управляющей согласованным функционированием различных компонентов сети и разграничением ответственности за преобразование и дальнейшую передачу информации).

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики – важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

По результатам проведенного анализа возможных угроз безопасности АС ОВД можно сформулировать перечень основных задач, которые должны решаться их системой компьютерной безопасности [21, 31]:

- управление доступом пользователей к ресурсам АС ОВД с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного (с превышением предоставленных

полномочий) доступа к ее информационным, программным и аппаратным ресурсам со стороны посторонних лиц, а также лиц из числа персонала организации (подразделения ОВД) и пользователей;

- защита данных, передаваемых по каналам связи;

- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;

- контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках НСД к ресурсам АС ОВД;

- контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;

- обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;

- управление средствами системы защиты.

Обычно различают внешнюю и внутреннюю безопасность компьютерных систем. Внешняя безопасность включает защиту АС от стихийных бедствий (пожар, наводнение и т.п.) и от проникновения в систему злоумышленников извне с целями хищения, получения доступа к информации или вывода системы из строя. В данном учебном пособии меры и методы защиты АС ОВД от стихийных бедствий и аварий, а также меры физической защиты (охраны и др.) не рассматриваются.

Все усилия по обеспечению внутренней безопасности АС ОВД фокусируются на создании надежных и удобных механизмов регламентации деятельности всех ее законных пользователей и обслуживающего персонала для принуждения их к безусловному соблюдению установленной в организации дисциплины доступа к ресурсам системы (в том числе к информации).

По способам осуществления все меры обеспечения безопасности АС ОВД подразделяются на:

1) правовые (законодательные). К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей (Приложения 5, 6);

2) морально-этические. К морально-этическим мерам противодействия относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти

нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний;

3) организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

- анализ и обобщение информации о новых ТСР, определение их возможностей и составление прогнозов их развития, выработка способов защиты информации от ТСР;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала системы;
- организацию охраны и надежного пропускного режима;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения, и т.п.;

4) физические и технические (аппаратурные и программные). Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС ОВД и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Законодательные и морально-этические меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение [31].

Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения и НСД к АС ОВД и информации. В некоторых случаях они являются единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Очевидно, что в организационных структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего надо решить правовые и организационные вопросы.

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем [32].

Организационные меры – это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако, это вовсе не означает, что систему защиты необходимо строить исключительно на их основе, как это часто пытаются сделать чиновники, далекие от технического прогресса. Этим мерам присущи серьезные недостатки, такие как:

- низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

- дополнительные неудобства, связанные с большим объемом рутинной формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений персонала и пользователей АС ОВД.

Рассмотрим известное утверждение о том, что создание абсолютной (то есть идеально надежной) системы защиты принципиально невозможно.

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора АС ОВД, администратора безопасности и т.п.). Вместе с самими средствами защиты эти люди образуют так называемое «ядро безопасности». В этом случае стойкость

системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер. Но даже имея совершенные законы и проводя оптимальную кадровую политику, все равно проблему защиты до конца решить не удастся. Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты. Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Защита информации в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, должна основываться на следующих основных принципах [28]:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- открытости алгоритмов и механизмов защиты;
- простоты применения защитных мер и средств.

Системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности АС ОВД.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонированно. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одной из наиболее укрепленных линий обороны призваны быть средства защиты, реализованные на уровне операционных систем в силу того, что операционная система – это как раз та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж обороны.

Защита информации – это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации на объекте информатизации ОВД.

Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы [21]. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов АС и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Естественно, что для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает владельцев АС ОВД от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее

преодоления (даже автору). Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей, имен и т.д.).

В Приказе ФСТЭК России от 11 февраля 2013 г. № 17 организационные и технические меры по защите информации от НСД разделены на группы воздействия [16]:

1) идентификация и аутентификация субъектов доступа и объектов доступа;
2) управление доступом субъектов доступа к объектам доступа;
3) ограничение программной среды;
4) защита машинных носителей информации;
5) регистрация событий безопасности;
6) антивирусная защита;
7) обнаружение (предотвращение) вторжений;
8) контроль (анализ) защищенности информации;
9) обеспечение целостности АС и информации;
10) обеспечение доступности информации;
11) защита среды виртуализации;
12) защита технических средств;
13) защита АС, ее средств, систем связи и передачи данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать:

- присвоение субъектам и объектам доступа уникального признака (идентификатора);
- сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов;
- проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности или аутентификация).

Идентификация и аутентификация (подтверждение подлинности) являются первым эшелоном защиты от несанкционированного доступа и необходимо понимать разницу между этими понятиями.

Идентификатор присваивается пользователю, процессу, действующему от имени какого-либо пользователя, или программно-аппаратному компоненту (субъекту) и позволяет назвать себя, т.е. сообщить свое «имя». Аутентификация позволяет убедиться, что субъект именно тот, за кого себя выдает. Пример идентификации и аутентификации – вход в домен Windows. В данном случае логин – это идентификатор, пароль – средство аутентификации. Знание пароля является залогом того, что субъект

действительно тот, за кого себя выдает.

Субъект может аутентифицироваться (подтвердить свою подлинность), предъявив одну из следующих сущностей:

- нечто, что он знает (например, пароль);
- нечто, чем он владеет (например, eToken);
- нечто, что есть часть его самого (например, отпечаток пальца).

Меры по управлению доступом должны обеспечивать:

- управление правами и привилегиями субъектов доступа;
- разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в АС ОВД правил разграничения доступа (ПРД);
- контроль за соблюдением этих правил.

Меры по ограничению программной среды должны обеспечивать:

- установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения;
- исключение возможности установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Защита машинных носителей информации должна исключать:

- возможность НСД к машинным носителям и хранящейся на них информации;
- несанкционированное использование машинных носителей.

Меры по регистрации событий безопасности должны обеспечивать:

- сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе;
- возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать:

- обнаружение в АС ОВД компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации;
- реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать:

- обнаружение действий в АС ОВД, направленных на преднамеренный НСД к информации, специальные воздействия на систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации;
- реагирование на эти действия.

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в АС ОВД, путем проведения мероприятий по анализу защищенности всей системы и тестированию ее системы защиты информации.

Меры по обеспечению целостности АС ОВД и информации должны обеспечивать:

- обнаружение фактов несанкционированного нарушения целостности АС ОВД и содержащейся в ней информации;

- возможность восстановления системы и содержащейся в ней информации.

Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в АС ОВД, в штатном режиме ее функционирования.

Меры по защите среды виртуализации должны исключать НСД к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать НСД к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование АС ОВД (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

Меры по защите АС ОВД, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии системы или ее отдельных сегментов с иными АС и информационно-телекоммуникационными сетями посредством применения архитектуры АС, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Средства защиты от НСД можно разделить на следующие группы [28]:

- технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки;

- программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.;

- смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности;

- организационные средства (мероприятия). К ним можно отнести

разработку документов, определяющих правила и процедуры, реализуемые для обеспечения защиты информации в АС ОВД, ограничение доступа в помещения, назначение полномочий по доступу и т.п.;

- криптографические средства – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы, аппаратные шифровальные (криптографические) средства, программно-аппаратные шифровальные (криптографические) средства.

Прежде чем выбирать средства защиты от НСД, необходимо определить перечень мер, которые они должны реализовывать. Перечень мер определяется на основе требований нормативных документов (базовый набор мер) и исходя из модели угроз конкретной АС ОВД.

После определения перечня мер, нужно выбрать средства защиты информации, которые эти меры реализуют. Необходимо учесть, требуется ли наличие сертификата у средства защиты информации. В приказе ФСТЭК России № 21 [15], например, нет однозначных требований по использованию сертифицированных средств защиты информации, – «применение средств защиты информации, прошедших установленным порядком процедуру оценки соответствия». Это значит, что для защиты персональных данных в негосударственных АС могут использоваться средств защиты информации, прошедшие сертификацию в добровольной системе сертификации или имеющие декларацию соответствия. А вот в государственных АС, к которым относятся и АС ОВД, все средств защиты информации должны быть сертифицированы. Соответственно, нужно выбирать средств защиты из Реестра сертифицированных средств защиты информации (Реестр), опубликованного на официальном сайте ФСТЭК России: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstven-nyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00.

При этом, несмотря на наличие в Реестре около 1000 сертифицированных средств защиты информации, большая часть из них была сертифицирована в единичном экземпляре или в составе маленькой партии, и недоступна для приобретения в настоящий момент. Поэтому реальный перечень сертифицированных средств защиты информации, которые можно использовать на практике, значительно меньше.

Сегодня сертификация средств защиты информации от НСД по линии ФСТЭК России проводится на соответствие одного или одновременно нескольких документов, основными из которых являются:

- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (РД СВТ);
- Требования к средствам антивирусной защиты (24 профиля защиты);
- Требования к средствам контроля съемных машинных носителей (10 профилей защиты);
- Требования к межсетевым экранам (5 типов межсетевых экранов);

- Требования к средствам доверенной загрузки (10 профилей защиты);
- Требования к системам обнаружения вторжений (12 профилей защиты);
- Руководящий документ «Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей».

В представленных документах средства защиты информации проранжированы по классам. В каждом документе введена своя шкала защищенности, где первый класс присваивается наиболее защищенным средствам защиты информации, точнее тем, которые проходили испытания по самым жестким условиям, и соответственно, с увеличением порядкового номера класса требования к испытаниям средств защиты информации смягчаются.

То есть недостаточно выбрать сертифицированное средство защиты информации, необходимо также правильно определить требуемый класс защищенности. Например, в [5] отмечено, что «для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия АС с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия АС с информационно-телекоммуникационными сетями международного информационного обмена».

Определившись с формальными признаками средства защиты информации (доступность на рынке, актуальность сертификата, наличие контроля недекларированных возможностей (при необходимости), класс защищенности), можно сосредоточиться на его функциональных характеристиках. Чтобы установить соответствие требуемых мер защиты и средства защиты необходимо внимательно изучить документацию на средство защиты информации, функциональные характеристики, область применения и ограничения.

Защита информации для лиц, допущенных к секретным работам, государственной тайне, осуществляется двумя способами: активным и пассивным.

Активный способ требует от сотрудников ОВД совершения активных действий по обеспечению режима секретности в подразделении, пассивный способ представляет собой форму нормативно-правовых актов, где сформулирован ряд запретов, необходимых для выработки специального поведения с целью недопущения утраты секретных сведений.

Активные действия предъявляют к сотрудникам ОВД с профессиональной точки зрения следующие требования: строгое соблюдение

правил по сохранению доверенной им тайны; пресечение попыток незаконного завладения секретными сведениями или действий, которые могут привести к утрате сведений; умение правильно определить гриф секретности сведений, составляющих государственную тайну; знание правил учета и хранения секретных документов; своевременное сообщение руководителю органа (подразделения) МВД России о выявленных каналах утечки секретной информации. При изменениях в своих анкетных данных, а также о внеслужебных связях с иностранными гражданами необходимо своевременно сообщать в отдел кадров, в обязательном порядке согласовывать с руководителем органа (подразделения) выезд в зарубежные страны по вопросам, не связанным со служебной деятельностью, а по возвращении из заграничной поездки информировать руководителя органа (подразделения) о возможных попытках получить секретную информацию, предпринятых со стороны иностранных граждан.

Пассивный способ включает в себя правила, которые нужно соблюдать при работе с секретными документами. Так, для составления совершенно секретных и секретных документов целесообразно пользоваться только специальными блокнотами с отрывными листами. Составляя документы, исполнители должны излагать в них минимальные секретные сведения и определять количество изготавливаемых копий в строгом соответствии с действительной служебной необходимостью и т.д.

Существуют отдельные ограничения в использовании технических средств при фиксации или передаче секретной информации. Например, запрещается вести секретные переговоры по телефону, телеграфу или радио, а также производить магнитофонные записи секретных совещаний без разрешения руководителя органа, организации, подразделения МВД России. Нельзя без соответствующего разрешения производить фото-, кино- и видеосъемку зданий, учреждений (предприятий) оборонного характера, секретных документов и специзделий. Также запрещено вносить фотоаппараты, кино-и видеокамеры, магнитофоны, радиоприемники и передатчики в служебные помещения, где производится работа с секретными документами.

Таким образом, рассмотренные обязанности всесторонне и с достаточной полнотой регламентируют поведение сотрудников ОВД в ходе проведения секретных работ и обращения с документами, которые содержат сведения, охраняемые государством. Практика подтверждает, что твердое знание и неукоснительное соблюдение каждым сотрудником своих обязанностей служат залогом надлежащего обеспечения режима секретности и конспирации в деятельности ОВД и в значительной степени способствуют успешному решению стоящих перед ними задач.

В целях соблюдения режима секретности выработаны определенные принципы, которые должны неукоснительно соблюдаться в ОВД.

Принцип ограничения:

- к секретной информации допускается определенный круг лиц (каждый должен знать только то, что ему положено по функциональным

обязанностям; секретные документы могут читать только те, кому они адресованы);

- каждый документ разрабатывается в установленном количестве;
- устанавливается количество сведений, сосредоточенных в одном документе.

Принцип персональной ответственности: в любой момент времени за каждый документ отвечает и распоряжается им конкретный человек (тот, кто расписался за документ).

Принцип контроля и учета:

- все операции с документом (информацией) фиксируются в соответствующих журналах и карточках (разработка, размножение, передача из рук в руки, снятие копий и т.д.);
- документы выдаются только под роспись;
- осуществляется постоянный контроль за наличием, порядком хранения, учетом и обращением с документами.

Нарушение вышеперечисленных принципов создает предпосылки к утрате документов и утечке секретной информации. В отличие от денег и других материальных ценностей, документ необязательно похищать. Достаточно прочитать или перлюстрировать его (каким-либо образом снять копию содержания). Поэтому документы требуют особых, дополнительных мер защиты.

Весь личный состав подразделения ОВД, соприкасающийся с секретной информацией, предварительно проходит соответствующую проверку, профессиональную подготовку, сдает зачеты, дает подписку о неразглашении секретных сведений.

Защитные мероприятия в общем плане должны обеспечивать:

- предупреждение появления угрозы НСД к секретным материалам;
- выявление возможных направлений и степень нарастания опасности;
- обнаружение реальных действий по завладению информацией;
- пресечение разглашения, утечки сведений и НСД к ним;
- ликвидацию последствий неправомерного получения информации и ее использования преступниками (злоумышленником).

Обеспечение комплексных мер по соблюдению режима секретности предполагает проведение мероприятий, защищающих территорию, здания, помещения ОВД, технические средства и другие носители информации как в комплексе, так и по элементам: правовая защита (Конституция, законы, указы, постановления); организационная защита (подбор и расстановка кадров, режим и охрана, организация секретного делопроизводства); инженерно-техническая защита (физические средства, аппаратные средства, программные средства, криптографические средства) [28].

2.4. Обязанности и права должностных лиц по защите конфиденциальной информации, планирование и организация работ по технической защите конфиденциальной информации

Руководство технической защитой конфиденциальной информации в органе, организации, подразделении системы МВД России возлагается на его руководителя.

Руководители подразделений организуют и обеспечивают техническую защиту информации, циркулирующей в технических средствах и помещениях подчиненных им подразделений.

Начальник структурного подразделения по технической защите конфиденциальной информации осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю в организации [23].

Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

Руководители подразделений, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются заместителю начальника организации (через структурное подразделение по технической защите конфиденциальной информации).

Заместитель начальника органа (организации) МВД России имеет право привлекать к проведению работ по технической защите конфиденциальной информации на договорной основе предприятия, учреждения и организации, имеющие лицензии на соответствующие виды деятельности.

Планирование работ по технической защите конфиденциальной информации и контролю ее эффективности [25, 33]:

1. В целях развития и обеспечения деятельности системы защиты информации в органах, организациях, подразделениях системы МВД России необходимо проводить планирование работ по технической защите конфиденциальной информации и контролю ее эффективности. Проекты планов разрабатываются структурным подразделением (специалистом) по технической защите конфиденциальной информации совместно с подразделениями, выполняющими работы с этой информацией и утверждаются руководителем органа (организации).

2. Сроки разработки, представления и утверждения планов устанавливаются руководителем органа (организации). Планы работ рекомендуется разрабатывать на год. При необходимости разрабатываются целевые планы защиты наиболее важных работ, особо важных объектов информатизации, контроле эффективности мероприятий по защите информации, устранении недостатков и т.п.

В годовые планы по технической защите конфиденциальной информации и контролю включаются:

- мероприятия по выполнению приказов и распоряжений руководителя организации по вопросам технической защиты информации;

- подготовка проектов организационно-распорядительных документов по вопросам технической защиты информации в организации, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на АРМ, в ЗП;

- аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите конфиденциальной информации;

- проведение периодического контроля состояния технической защиты информации;

- мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

- мероприятия по совершенствованию системы технической защиты информации на объектах информатизации ОВД.

Целями годового плана по защите конфиденциальной информации могут быть:

1. Проведение анализа сведений, составляющих служебную тайну. При этом:

- установить места разработки, накопления и хранения документов, содержащих информацию, составляющую служебную тайну;

- выявить потенциальные каналы утечки таких сведений;

- оценить возможности по закрытию этих каналов;

- проанализировать соотношение затрат и преимуществ по использованию различных технологий, обеспечивающих защиту служебной тайны;

- назначить сотрудников, ответственных за каждый участок системы обеспечения безопасности.

2. Исключение несанкционированного распространения конфиденциальных секретов путем их утечки по техническим каналам, сотрудниками ОВД и другими носителями таких секретов.

3. Обеспечение деятельности системы защиты информации по следующим направлениям:

- работа с персоналом организации, в том числе путем проведения бесед при приеме на работу, инструктажа вновь принятых на работу по правилам и процедурам защиты служебной тайны и получения от них обязательств (контрактов) о неразглашении служебной информации, обучения сотрудников правилам сохранения служебных секретов, стимулирования соблюдения конфиденциальности, бесед с увольняющимися сотрудниками и получения от них подписок;

- организация работы с конфиденциальными документами на объектах информатизации ОВД, установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами и их

публикациями, контроль и учет технических носителей конфиденциальных сведений, засекречивание, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов;

- создание системы технической защиты информации;
- создание системы защиты информации от НСД к ней, обеспечение контроля за работой пользователей на персональных ЭВМ;
- защита служебной тайны в процессе заключения контрактов и договоров с взаимодействующими организациями (подразделениями), смежниками, поставщиками и т.д.;
- разработка памятки о сохранении сведений, составляющих служебную тайну, определение порядка ознакомления с «Перечнем сведений, составляющих служебную тайну» и присвоения документам грифа конфиденциальности;
- контроль сооружений и оборудования организации, обеспечение безопасности производственных и служебных помещений, охрана фото и копировального оборудования, контроль посещения организации.

Контроль выполнения планов и отчетность по ним возлагается на структурное подразделение по технической защите информации [31].

4. Организация работ по созданию и эксплуатации объектов информатизации и их средств защиты информации определяется в разрабатываемом «Положении о порядке организации и проведения работ по защите конфиденциальной информации» или в приложении к «Руководству по защите информации от утечки по техническим каналам на объекте» и должна предусматривать:

- порядок определения защищаемой информации;
- порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и средств защиты информации, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;
- ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации, за качество и научно-технический уровень разработки средств защиты информации.

5. Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты включают:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС ОВД или внешней среде (по необходимости);

- периодически проводимые (через определенное время) мероприятия;
- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

К разовым мероприятиям относят:

- общесистемные мероприятия по созданию научно-технических и методологических основ (концепций, руководств и других руководящих документов) по защите информации;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС ОВД (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);
- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т.п.);
- проведение спецпроверок, применяемых в АС ОВД средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам ПЭМИН;
- разработку и утверждение функциональных обязанностей должностных лиц подразделения информационной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов АС ОВД и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в АС ОВД, между участниками информационного обмена и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с применением электронной подписи;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- мероприятия по созданию системы защиты АС ОВД и созданию инфраструктуры;
- мероприятия по разработке правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями ОВД с использованием АС, а также используемых при их решении режимов обработки и доступа к данным; определение перечня файлов и баз данных, содержащих сведения, составляющие служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в АС ОВД; выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процесса обработки информации и

каналов доступа к ней; оценку возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);

- организацию надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
- организацию учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследований, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядка обновления используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);
- создание отделов защиты информации, или в случае небольших организаций и подразделений ОВД, объемов работ по защите информации, назначение штатных специалистов, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов АС обработки информации на объекте информатизации ОВД;
- определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС ОВД в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программном обеспечении и действиях персонала, стихийных бедствиях.

К периодически проводимым мероприятиям относят:

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;
- мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;
- периодическое осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты, в том числе с привлечением сторонних специалистов. На основе полученной в результате такого анализа информации принятие необходимых мер по совершенствованию системы защиты информации;
- мероприятия по пересмотру состава и построению системы защиты информации.

Мероприятия, проводимые по необходимости, включают:

- мероприятия, осуществляемые при кадровых изменениях в составе персонала АС ОВД;

- мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.);

- мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т.д.).

К постоянно проводимым мероприятиям относятся:

- мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС ОВД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т.п.);

- мероприятия по непрерывной поддержке функционирования и управлению используемыми средствами защиты;

- явный и скрытый контроль за работой персонала системы;

- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС ОВД;

- постоянно (силами отдела защиты информации и службы безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

Для планирования организации и обеспечения эффективного функционирования комплексной системы защиты информации в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, рекомендуется разрабатывать следующие группы организационно-распорядительных документов:

- документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в АС ОВД (план защиты информации в системе, план обеспечения непрерывной работы и восстановления информации и другие документы, разрабатываемые в ходе подготовки и проведения аттестационных испытаний);

- документы, определяющие ответственность взаимодействующих организаций (субъектов) при обмене электронными документами (договор об организации обмена электронными документами).

В план защиты информации в АС ОВД рекомендуется включать следующие сведения:

- описание защищаемой системы (основные характеристики защищаемого объекта): назначение АС ОВД , перечень решаемых ею задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в АС ОВД, и требований по обеспечению доступности, конфиденциальности, целостности этих категорий информации, список

пользователей и их полномочий по доступу к ресурсам системы и т.п.;

- цель защиты системы и пути обеспечения безопасности АС ОВД и циркулирующей в ней информации;

- перечень значимых угроз безопасности АС ОВД, от которых требуется защита и наиболее вероятных путей нанесения ущерба;

- основные требования к организации процесса функционирования АС на объектах информатизации ОВД и мерам обеспечения безопасности обрабатываемой информации;

- требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;

- основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности АС ОВД (особые обязанности должностных лиц АС).

В плане обеспечения непрерывной работы и восстановления информации рекомендуется отражать следующие вопросы:

- цель обеспечения непрерывности процесса функционирования АС ОВД, своевременность восстановления ее работоспособности и чем она достигается;

- перечень и классификация возможных кризисных ситуаций;

- требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т.п.);

- обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования АС ОВД.

Договор о порядке организации обмена электронными документами должен включать документы, в которых отражаются следующие вопросы:

- разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;

- определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;

- определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);

- определение порядка разрешения споров в случае возникновения конфликтов.

Организация работ по защите СВТ и АС ОВД от НСД к информации должна быть частью общей организации работ по безопасности информации.

Планирование и разработка мероприятий по защите должны проводиться одновременно с разработкой СВТ и АС и выполняться за счет финансовых и материально-технических средств (ресурсов), выделенных на их разработку.

2.5. Организация работ по созданию системы защиты конфиденциальной информации

Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в виде системы защиты информации во взаимосвязи с другими мерами по защите информации. Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применения (при необходимости) средств защиты по предотвращению утечки информации или воздействия на нее по техническим каналам за счет НСД к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств [28].

В СТР-К выделяются следующие стадии и этапы создания системы защиты информационного ресурса:

- предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания системы защиты информации (СЗИ) и технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации объекта информатизации, включающая разработку СЗИ в составе объекта информатизации;
- стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания СЗИ, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

На первой стадии по обследованию объекта информатизации:

- устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;
- определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам;
- определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;
- определяются условия расположения объектов информатизации относительно границ КЗ;
- определяются конфигурация и топология АС и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;

- определяются режимы обработки информации в АС в целом и в ее отдельных компонентах;
- определяется класс защищенности АС;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ. На основе действующих нормативных правовых актов и методических документов по защите конфиденциальной информации с учетом установленного класса защищенности АС задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

Перечень сведений конфиденциального характера составляется заказчиком объекта информатизации и утверждается его руководителем.

Аналитическое обоснование необходимости создания СЗИ должно содержать:
- информационную характеристику и организационную структуру объекта информатизации;
- характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;
- возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных средств защиты информации;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;
- ориентировочные сроки разработки и внедрения СЗИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с главным конструктором (должностным лицом, обеспечивающим научно-техническое руководство создания объекта информатизации), руководителем службы безопасности и утверждается руководителем организации-заказчика.

Техническое (частное техническое) задание на разработку СЗИ должно содержать:
- обоснование разработки;
- исходные данные создаваемого (модернизируемого) объекта

информатизации в техническом, программном, информационном и организационном аспектах;

- класс защищенности АС;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
- конкретизацию требований к СЗИ на основе действующих нормативно-методических документов и установленного класса защищенности АС;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;
- перечень подрядных организаций-исполнителей видов работ;
- перечень предъявляемой заказчику научно-технической продукции и документации.

Техническое (частное техническое) задание на разработку СЗИ подписывается разработчиком, согласовывается со службой безопасности организации-заказчика, подрядными организациями и утверждается заказчиком.

На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) объекта информатизации в соответствии с требованиями технического (частного технического) задания на разработку СЗИ;
- разработка раздела технического проекта на объект информатизации в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;
- закупка сертифицированных технических, программных и программно-технических (в том числе криптографических) средств защиты информации и их установка;
- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты

информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;

- организация охраны и физической защиты помещений объекта информатизации, исключающих НСД к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;

- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;

- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;

- выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

- разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

- выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

Задание на проектирование оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности организации – заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Мероприятия по защите информации от утечки по техническим каналам являются основным элементом проектных решений, закладываемых в соответствующие разделы проекта, и разрабатываются одновременно с ними.

На стадии проектирования и создания объекта информатизации оформляются также технический (техно-рабочий) проект и эксплуатационная документация СЗИ, состоящие из:

- пояснительной записки с изложением решений по комплексу организационных мер и программно-техническим (в том числе криптографическим) средствам обеспечения безопасности информации, состава средств защиты информации с указанием их соответствия требованиям технического задания;

- описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;

- плана организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации;

- технического паспорта объекта информатизации;

- инструкций и руководств по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для работников службы защиты информации.

На стадии ввода в действие объекта информатизации и СЗИ

осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком;
- аттестация объекта информатизации по требованиям безопасности информации.

На этой стадии оформляются:

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- предъявительский акт к проведению аттестационных испытаний;
- заключение по результатам аттестационных испытаний.

При положительных результатах аттестации на объект информатизации оформляется аттестат соответствия требованиям по безопасности информации.

Кроме вышеуказанной документации в организации оформляются приказы, указания и решения:

- о проектировании объекта информатизации, создании соответствующих подразделений разработки и назначении ответственных исполнителей;
- о формировании группы обследования и назначении ее руководителя;
- о заключении соответствующих договоров на проведение работ;
- о назначении лиц, ответственных за эксплуатацию объекта информатизации;
- о начале обработки в АС (обсуждения в защищаемом помещении) конфиденциальной информации.

Эксплуатация объекта информатизации осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией.

2.6. Контроль состояния технической защиты конфиденциальной информации, порядок аттестации объектов информатизации

В соответствии с ГОСТ Р 50922-96 «Защита информации. Термины и определения» контроль состояния защиты информации подразумевает под собой проверку соответствия организации и/или эффективности защиты информации. Контроль за эффективностью предусмотренных мер защиты возлагается на структурное подразделение по технической защите конфиденциальной информации.

Основными задачами контроля состояния технической защиты конфиденциальной информации являются: оценка уровня организации и эффективности принятых мер защиты, своевременное выявление и

предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации [31].

Выделяется несколько уровней контроля состояния технической защиты информации:

- межведомственный контроль – ФСТЭК России, ФСБ России, Роскомнадзор и др.;
- ведомственный контроль – вышестоящая ведомственная структура управления;
- объектовый контроль – служба безопасности органа (организации), также существует возможность привлечения внешней организации при условии наличия лицензии ФСТЭК России на осуществление данного вида деятельности.

Контроль состояния защиты информации должен осуществляться не реже одного раза в квартал, а также при ремонте и перед проведением особо важных мероприятий. Повседневный контроль состояния технической защиты информации осуществляется лицами, ответственными за эксплуатацию технических средств и помещений, а также непосредственными пользователями.

Контроль заключается в оценке [23]:

- инструментальной и визуальной проверки работоспособности применяемых средств защиты информации в соответствии с нормативно-технической документацией;
- выполнения требований нормативных и методических документов законодательства Российской Федерации по вопросам технической защиты информации, ФСТЭК России;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

Для объектов информатизации, требующих обязательной аттестации, контроль является частью аттестационных испытаний.

Методы технического контроля:

- инструментальный, заключающийся в проведении определенных измерений с помощью аппаратуры контроля с целью проверки эффективности защиты технической информации;
- инструментально-расчетный, заключающийся в проведении определенных измерений с помощью аппаратуры контроля и последующим расчетом контролируемых параметров на границе контролируемой зоны;
- расчетный метод, заключающийся в проведении определенных расчетов с использованием исходных данных по объекту разведки и технических средств разведки;
- экспертный, заключающийся в проведении проверок средства вычислительной техники на наличие подключений к сетям международного информационного обмена и обработки информации ограниченного доступа.

Результаты технического контроля оформляются в виде протокола, подписываются представителем органа контроля и представителем организации.

Что касается ПДн, государство в лице уполномоченных органов осуществляет контроль и надзор за соблюдением установленных законодательством мер. Федеральный закон от 27.07.2006 № 152[4] содержит самостоятельную главу, посвященную государственному контролю и надзору за обработкой ПДн, в которой имеется только одна статья, посвященная этой теме – ст. 23, согласно которой уполномоченный орган по защите прав субъектов ПДн обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки ПДн требованиям Федерального закона № 152 и принятых в соответствии с ним нормативных правовых актов. В настоящее время функции контроля за выполнением операторами установленных требований возложены на Роскомнадзор [13]. В соответствии с ч. 1.1 ст. 23 Федерального закона от 27.07.2006 № 152 порядок организации и проведения проверок юридических лиц и индивидуальных предпринимателей, являющихся операторами обработки ПДн, уполномоченным органом по защите прав субъектов ПДн, а порядок организации и осуществления государственного контроля и надзора за их обработкой иными лицами, являющимися операторами, устанавливается Правительством Российской Федерации.

При исполнении контрольных функций Роскомнадзор действует в соответствии с Постановлением Правительства Российской Федерации от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»[5] (которым утверждено Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций).

Помимо вышеизложенного, в соответствии с ч. 8 ст. 19 ФСТЭК России и ФСБ России в пределах своих полномочий (ФСБ России – в части использования криптографических средств защиты информации, ФСТЭК России – во всех остальных) вправе осуществлять контроль и надзор за выполнением организационных и технических мер при обработке ПДн в государственных информационных системах ПДн без права ознакомления с ПДн, обрабатываемыми в информационных системах ПДн. При этом ни ФСТЭК России, ни ФСБ России не наделены полномочиями по проведению контрольно-надзорных мероприятий в отношении операторов ПДн, не являющихся государственными или муниципальными органами.

Деятельность по аттестации объектов информатизации по требованиям безопасности информации осуществляет ФСТЭК России.

Согласно «Положению по аттестации объектов информатизации по требованиям безопасности информации» от 25 ноября 1994 года аттестация объектов информатизации представляет собой комплекс организационно-

[4] О персональных данных: федеральный закон от 27 июля 2006 года № 152-ФЗ (ред. от 24.04.2020) // СЗ РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

[5] О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: постановление Правительства РФ от 16.03.2009 № 228 (ред. от 16.05.2020) // Собрание законодательства РФ. – 27.07.2020. – № 701. – Ст. 1431.

технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России. Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности на период времени, разрешенный документом [33].

Аттестация должна проводится до начала обработки информации, подлежащей защите [34]. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите данной информации на конкретном объекте информатизации.

Проведение аттестации объектов информатизации состоит из нескольких этапов:

- подача и рассмотрение заявки на аттестацию (Приложение 7) – заявитель направляет заявление и необходимые исходные данные об объекте информатизации по установленной форме в управление ФСТЭК России по федеральному округу. Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации;
- предварительное ознакомление с аттестуемым объектом – в случае недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости), в специальных исследовательских центрах с помощью специальной контрольной аппаратуры и тестовых средств;
- разработка программы и методики аттестационных испытаний – по результатам рассмотрения заявки и анализа исходных данных определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации. Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации. Программа аттестационных испытаний согласовывается с заявителем;
- заключение договоров на аттестацию – этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением контрактов органа по аттестации с

привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации. Оплата работы членов аттестационной комиссии производится органом по аттестации в соответствии с заключенными трудовыми договорами за счет финансовых средств от заключаемых договоров на аттестацию объектов информатизации;

- проведение аттестационных испытаний объекта информатизации представляет собой многоэтапный процесс: осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации; определяется правильность категорирования объектов электронно-вычислительной техники и классификации АС, выбора и применения сертифицированных и несертифицированных средств и систем защиты информации; проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний; проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации; проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации; оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации. Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи аттестата и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя (Приложение 8). К заключению прилагаются протоколы испытаний, подписанные экспертами, подтверждают полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Заключение и протоколы испытаний подлежат утверждению органом по аттестации;

- оформление, регистрация и выдача «Аттестата соответствия» – документ оформляется и выдается заявителю после утверждения заключения по результатам аттестации. Регистрация аттестата осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору. Аттестат соответствия выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта

информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации. При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче аттестата соответствия. Но в случае несущественных замечаний аттестат может быть выдан после проверки их устранения. При этом может быть предложен срок повторной аттестации при условии устранения недостатков;

- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации – проводится ФСТЭК России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации – периодически в соответствии с планами работы по контролю и надзору. Существует возможность передачи некоторых из функций по контролю и надзору, осуществляемых ФСТЭК России, аккредитованным органам по аттестации. Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных и методических документов по безопасности информации, выявленных при контроле и надзоре, орган по аттестации может быть лишен лицензии на право проведения аттестации объектов информатизации.

При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и

надзор, может быть приостановлено или аннулировано действие аттестата соответствия, и информированием органа, ведущего сводную информационную базу аттестованных объектов информатики, и ФСТЭК России.

Решение об аннулировании действия аттестата принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных документов по безопасности информации, утвержденных ФСТЭК России, выявленных при контроле и надзоре и приведших к повторной аттестации, расходы по осуществлению контроля и надзора могут быть по решению Госарбитража взысканы с органа по аттестации. Повторная аттестация может быть также осуществлена за счет этого органа по аттестации.

Расходы по осуществлению надзора за обязательной аттестацией и эксплуатацией объектов, прошедших обязательную аттестацию, оплачиваются органом надзора из средств госбюджета, выделенных ему в этих целях;

- рассмотрение апелляций – при несогласии заявителя с отказом в выдаче аттестата он имеет право обратиться в вышестоящий орган по аттестации или непосредственно в ФСТЭК России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

2.7. Взаимодействие с предприятиями, учреждениями и организациями при проведении совместных работ с конфиденциальной информацией

Передача документов, подготовленных в системе МВД России, содержащих служебную информацию ограниченного распространения, в другие органы и организации осуществляется с письменного разрешения руководителя (начальника) или лица, его замещающего, органа, организации, подразделения системы МВД России, в котором данный документ находится, в объеме, необходимом указанным органам и организациям для выполнения конкретной задачи либо определенном договором на проведение совместных работ, при условии обеспечения ими защиты передаваемой служебной информации ограниченного распространения от НСД [27].

Поступившие в органы, организации, подразделения системы МВД России документы, содержащие служебную информацию ограниченного распространения, подготовленные в других органах и организациях, не подлежат передаче третьим лицам, не имеющим отношения к органам, организациям, подразделениям системы МВД России, без письменного разрешения должностного лица органа (организации), которым были введены ограничения на распространение данной информации.

Решение о передаче служебной информации ограниченного

распространения, образовавшейся в деятельности МВД России, другим государствам или международным организациям принимается руководством МВД России. Необходимым условием для передачи указанной информации является наличие письменных обязательств от принимающей стороны по ее защите.

Основанием для передачи служебной информации ограниченного распространения другим государствам или международным организациям служит официальный запрос, а также необходимость осуществления информационного обмена при взаимодействии в рамках заключенных договоров (соглашений), в том числе в ходе осуществления образовательной деятельности [5].

Передача служебной информации ограниченного распространения негосударственным организациям возможна только в рамках исполнения условий договоров, государственных контрактов в объеме, необходимом для их исполнения, либо в случаях, предусмотренных федеральными законами. Государственные контракты, договоры и дополнительные соглашения к ним, заключаемые между негосударственными организациями и органами, организациями, подразделениями системы МВД России, должны включать положения, регламентирующие порядок обращения со служебной информацией ограниченного распространения и ответственность за его нарушение.

Таким образом, в главе подробно рассмотрены понятие технического канала утечки конфиденциальной информации и его виды. Представлены нормативные документы, регламентирующие организационные и технические мероприятия по защите конфиденциальной информации на объектах информатизации ОВД. Сформулированы принципы защиты информации в АС. Отдельно подробно рассмотрены основы организации защиты конфиденциальной информации от НСД в АС. Раскрыты обязанности и права должностных лиц по защите конфиденциальной информации, рассмотрены планирование и организация работ по ее технической защите. Разобраны этапы планирования при создании системы защиты информации в АС ОВД, а также порядок аттестации и контроля объектов информатизации. Особое внимание уделено построению взаимодействия с предприятиями, учреждениями и организациями при проведении совместных работ с конфиденциальной информацией.

Контрольные вопросы по главе 2:

1. Что понимают под техническим каналом утечки информации?
2. Что относят к основным и к вспомогательным техническим средствам и системам?
3. Какие нормативные документы регламентируют требования по технической защите конфиденциальной информации?
4. Какие основные принципы сформулированы для обеспечения защиты информации в информационных системах?

5. Что является объектами защиты в подразделениях ОВД?

6. Какие виды информации подлежат защите?

7. Какие основные мероприятиям по технической защите конфиденциальной информации проводятся в защищаемых помещениях?

8. Как организуется антивирусная защита информации на объектах информатизации?

9. В чем заключаются организационные и технические требования использования паролей в информационных системах, возлагаемые на системного администратора?

10. Какие возможные нежелательные воздействия на компьютерные системы должны рассматриваться при организации в них защиты информации?

11. Совокупность каких взаимосвязанных компонентов понимается под АС обработки информации?

12. Какие элементы АС обработки информации нуждаются в особой защите и почему?

13. Какие выделяют основные виды угроз безопасности информации в АС ОВД?

14. Какие имеются каналы утраты конфиденциальной документированной информации на различных стадиях и этапах движения документов?

15. Как подразделяются меры обеспечения безопасности АС ОВД в соответствии со способом их реализации?

16. Кто осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю?

17. Как организуется планирование работ по технической защите конфиденциальной информации и контролю ее эффективности?

18. Какие выделяют стадии и этапы создания системы защиты информационного ресурса?

19. В чем заключается аналитическое обоснование необходимости создания средств защиты информации?

20. Что должно содержать техническое задание на разработку средств защиты информации?

21. Какие выделяют уровни контроля состояния технической защиты информации?

22. В какие сроки должен осуществляться контроль состояния защиты информации? В чем он заключается?

23. Кто осуществляет аттестацию объектов информатизации в соответствии с требованиями безопасности информации?

24. Из каких этапов состоит аттестация объектов информатизации?

25. Возможна ли передача документов, подготовленных в системе МВД России и содержащих служебную информацию ограниченного распространения, в другие органы и организации?

26. Что может являться основанием для передачи служебной информации ограниченного распространения другим государствам или международным организациям?

27. Возможна ли передача служебной информации ограниченного распространения негосударственным организациям?

Заключение

Предлагаемое учебное пособие может рассматриваться в качестве руководства по защите конфиденциальных документов и информационных ресурсов в ОВД Российской Федерации. В нем представлены методические рекомендации по работе с документацией, содержащей информацию ограниченного распространения, в ОВД: порядок обращения с документами, содержащими служебную информацию ограниченного распространения, персональные данные и коммерческую тайну; рекомендации по составлению перечня сведений конфиденциального характера; рекомендации по инвентаризации информационных ресурсов.

Подробно рассмотрены понятие технического канала утечки конфиденциальной информации и его виды. Представлены нормативные документы, регламентирующие организационные и технические мероприятия по защите конфиденциальной информации на объектах информатизации ОВД. Сформулированы принципы защиты информации в АС. Отдельно изложены основы организации защиты конфиденциальной информации от угроз НСД в АС. Раскрыты обязанности и права должностных лиц по защите конфиденциальной информации, рассмотрены планирование и организация работ по ее технической защите. Разобраны этапы планирования при создании системы защиты информации в АС ОВД, а также порядок аттестации и контроля объектов информатизации. Особое внимание уделено построению взаимодействия с предприятиями, учреждениями и организациями при проведении совместных работ с конфиденциальной информацией.

Использование изложенных сведений и представленных методических рекомендаций в профессионально-служебной деятельности субъектов информационных отношений ОВД позволит им соблюдать необходимые требования по работе с конфиденциальными документами и информационными ресурсами в соответствии с действующими нормативными правовыми актами, регламентирующими порядок и правила защиты информации ограниченного пользования на предприятиях и в государственных структурах, что в целом будет способствовать повышению эффективности деятельности правоохранительных органов по предупреждению, раскрытию и расследованию преступлений.

Учебное пособие рекомендуется для обучения курсантов, слушателей и адъюнктов образовательных организаций системы МВД России основам работы с конфиденциальной информацией. Материал, изложенный в пособии, может быть полезен профессорско-преподавательскому составу и сотрудникам ведомственных научных организаций, область научных интересов которых связана с методами, системами защиты информации и обеспечением информационной безопасности. Учебное пособие может заинтересовать студентов и аспирантов образовательных организаций гражданского профиля, а также научных работников, занимающихся проблемой повышения эффективности функционирования систем защиты

информации от несанкционированного доступа, эксплуатируемых на объектах информатизации различного назначения.

Список литературы

1. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02 июля 2021 г. № 400 // СПС «КонсультантПлюс» (дата обращения: 10.07.2021).
2. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).
3. Методы и средства повышения защищенности автоматизированных систем на основе задания требований к механизмам защиты: учеб. пособие / С.А. Змеев [и др.]; под общ. ред. д-ра техн. наук, проф. С.В. Скрыля и д-ра техн. наук, проф. Е.А. Рогозина. – Воронеж: Воронеж. ин-т МВД России, 2013. – 105 с.
4. Об утверждении перечня сведений конфиденциального характера: указ Президента Российской Федерации от 6 марта 1997 г. № 188 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).
5. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 // СПС «КонсультантПлюс» (дата обращения: 02.07.2020).
6. Организационно-технологическое управление процессами защиты информации от несанкционированного доступа в автоматизированных системах управления критических применений на основе использования программных средств защиты: учеб. пособие / Р.В. Беляев [и др.]. – Воронеж: ВУНЦ ВВС «ВВА», 2017. – 84 с.
7. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных: директива Европейского парламента и Совета Европейского союза от 24 октября 1995 г. № 95/46/ЕС // СПС «КонсультантПлюс» (дата обращения: 11.07.2020).
8. Методы и средства анализа и оценки защищенности автоматизированных систем специального назначения на основе требований к безопасности по ГОСТ Р ИСО/МЭК 15408-2-2013: монография / Е.А. Рогозин, [и др.]. – Воронеж: ВУНЦ ВВС «ВВА», 2020. – 96 с.
9. О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России: приказ МВД России от 9 ноября 2018 г. № 755 // СПС «КонсультантПлюс» (дата обращения: 11.07.2020).
10. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01 ноября 2012 г. № 1119 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).
11. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).
12. О мерах по обеспечению информационной безопасности Российской

Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента Российской Федерации от 17 марта 2008 г. № 351 // СПС «КонсультантПлюс» (дата обращения: 17.07.2020).

13. О персональных данных: федеральный закон от 27 июля 2006 года № 152-ФЗ // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

14. 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: приказ ФСБ России от 10 июля 2014 г. № 378 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

15. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18 февраля 2013 г. № 21 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

16. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. № 17 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

17. О коммерческой тайне: федеральный закон от 29 июля 2004 года № 98-ФЗ // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

18. О федеральной государственной информационной системе координации информатизации: постановление Правительства Российской Федерации от 14 ноября 2015 г. № 1235 // СПС «КонсультантПлюс» (дата обращения: 15.07.2020).

19. Вопросы Федеральной службы по техническому и экспортному контролю: указ Президента Российской Федерации от 16 августа 2004 г. № 1085 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

20. О связи: федеральный закон от 7 июля 2003 г. № 126-ФЗ // СПС «КонсультантПлюс» (дата обращения: 02.07.2020).

21. Дровникова И.Г. Формирование требований к системам защиты информации от несанкционированного доступа в автоматизированные системы органов внутренних дел на основе генетического алгоритма: монография / И.Г. Дровникова [и др.]. – [Электронный ресурс]. – Электр. дан. и прогр. – Воронеж: Воронеж. ин-т МВД России, 2019. – 128 с.

22.О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

23. Защита информации в экономических информационных системах (учебное пособие для студентов высших учебных заведений): учеб. пособие /

Е.А. Рогозин [и др.]. под общ. ред. д-ра техн. наук, проф. С.В. Скрыля и д-ра техн. наук, проф. Е.А. Рогозина. – Воронеж: ВЭПИ, 2011. – 207 с.

24. Методы и средства оценки защищенности автоматизированных систем органов внутренних дел: монография / И.Г. Дровникова [и др.]. – Воронеж: ВИ МВД России, 2017. – 88 с.

25. Защита конфиденциальных документов и информационных ресурсов в администрациях органов власти, учреждениях, организациях и на предприятиях: учеб. пособие / Р.В. Беляев [и др.]. – Воронеж: ВУНЦ ВВС «ВВА», 2019. – 251 с.

26. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при ее проектировании в системах электронного документооборота: монография / П.В. Зиновьев, И.И. Застрожнов, Е.А. Рогозин. – Воронеж: Воронеж. гос. техн. ун-т, 2015. – 106 с.

27. Методы и средства повышения защищенности автоматизированных систем: монография / А.А. Змеев [и др.]; под общ. ред. д-ра техн. наук, проф. С.В. Скрыля и д-ра техн. наук, проф. Е.А. Рогозина. — Воронеж: Воронеж. ин-т МВД России, 2013. – 108 с.

28. О защите физических лиц при автоматизированной обработке персональных данных: конвенция Совета Европы от 28 января 1981 г. // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

29. Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации: приказ МВД России от 2 января 2013 г. № 1 // СПС «КонсультантПлюс» (дата обращения: 11.07.2020).

30.Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации: приказ МВД России от 20 июня 2012 г. № 615 // СПС «КонсультантПлюс» (дата обращения: 11.07.2020).

31. О лицензировании отдельных видов деятельности: федеральный закон от 4 мая 2011 г. № 99-ФЗ // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

32. Об организации лицензирования отдельных видов деятельности: постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 // СПС «КонсультантПлюс» (дата обращения: 22.07.2020).

33. О лицензировании деятельности по технической защите конфиденциальной информации: постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

34. О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации: постановление Правительства Российской Федерации от 03 марта 2012 г. № 171 // СПС «КонсультантПлюс» (дата обращения: 02.07.2020).

35.Об обязательном экземпляре документов: Федеральный закон от 29.12.1994 № 77-ФЗ // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

36.Об электронной подписи: федеральный закон от 06.04.2011 г. № 63-ФЗ

// СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

37.О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных: федеральный закон от 19.12.2005 № 160-ФЗ // СПС «КонсультантПлюс» (дата обращения: 12.07.2020).

38.Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изм., внесенными Протоколом от 13.05.2004 № 14) // Бюллетень международных договоров. – май 2004 г. – № 14.

39.Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г. (ред. от 15.06.1999).

40.Постановление Правительства РФ от 21 марта 2012 г. № 211 (ред. от 15.04.2019) // СЗ РФ. – 2012. – № 45. – Ст. 6257.

Приложение 1

Термины и определения

Информатизация – организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем).

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи.

База данных – объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины.

Данные – информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

Информационная технология – приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами. Информационные ресурсы, созданные с участием средств федерального бюджета или бюджета субъекта Российской Федерации, являются государственными.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Пользователь (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Используемые сокращения

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
АТС – автоматическая телефонная станция;
ВОЛС – волоконно-оптические линии связи;
ВТСС – вспомогательные технические средства и системы;
ЗП – защищаемые помещения;
КЗ – контролируемая зона;
ЛВС – локальная вычислительная сеть;
МВД – министерство внутренних дел;
МНИ – машинный носитель информации;
МО – магнитооптические;
НИОКР – научно-исследовательская и опытно-конструкторская работа;
НСД – несанкционированный доступ;
ОВД – орган внутренних дел;
ОС – опасный сигнал;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПЭМИ – побочные электромагнитные излучения;
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средства вычислительной техники;
СИРД – средства изготовления и размножения документов;
СЛЗ – электромагнитное зашумление;
СПЗ – пространственное зашумление;
СТР-К – специальные требования и рекомендации по технической защите конфиденциальной информации;
ТСОИ – технические средства обработки информации;
ТСПИ – технические средства передачи и обработки информации;
ФЗ – федеральный закон;
ФСБ – федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю;
ЭВМ – электронно-вычислительная машина;
ЭМИ – электромагнитное излучение.

Приложение 2

Перечень
обязательных сведений о документах, используемых в целях учета и поиска документов в системах электронного документооборота федеральных органов исполнительной власти

Приложение
к Правилам делопроизводства
в федеральных органах
исполнительной власти
(в редакции постановления
Правительства Российской Федерации
от 26 апреля 2016 г. № 356)

С изменениями и дополнениями от:
7 сентября 2011 г., 26 апреля 2016 г.

1. Адресант (автор)
2. Адресат
3. Должность, фамилия и инициалы лица, подписавшего документ
4. Наименование вида документа
5. Дата документа
6. Регистрационный номер документа
7. Дата поступления документа
8. Регистрационный номер входящего документа
9. Сведения о связанных документах (наименование вида документа, дата, регистрационный номер, тип связи)
10. Заголовок к тексту (краткое содержание документа)
11. Индекс дела по номенклатуре дел
12. Сведения о переадресации документа
13. Количество листов основного документа
14. Отметка о приложении (количество приложений, общее количество листов приложений)
15. Указания по исполнению документа (исполнитель, поручение, дата исполнения)
16. Отметка о контроле
17. Гриф ограничения доступа
18. Сведения об электронной подписи
19. Проверка электронной подписи
20. Подразделение – ответственный исполнитель документа
21. Файлы электронного документа (количество файлов, имена файлов)

Приложение 3

Список стандартов, регламентирующих защиту данных

ГОСТ Р ИСО 15489-1-2019 Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 26 марта 2019 г. №101-ст);

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст);

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст);

ГОСТ Р 53112-2008 Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 530-ст)

ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст);

ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст);

ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. № 1340-ст);

ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст);

ГОСТ Р ИСО/МЭК 27002-2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 423-ст);

ГОСТ Р ИСО/МЭК 27003-2021. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации (утв. Приказом Федерального агентства по

техническому регулированию и метрологии от 19 мая 2021 г. № 387-ст);

ГОСТ Р ИСО/МЭК 27004-2021. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 388-ст);

ГОСТ Р ИСО/МЭК 27005-2010. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст);

ГОСТ Р ИСО/МЭК 27006-2020. Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 8 сентября 2020 г. №628-ст).

Приложение 4

Результаты анализа угроз безопасности в автоматизированных системах органов внутренних дел

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
1. Угроза безопасности: получение несанкционированного доступа к ресурсам АС ОВД Последствия: утрата, порча или модификация информации			
Защита информации от доступа несанкциониро-ванных пользователей. Обеспечение доступа к ресурсам АС ОВД только в соответствии с политикой безопасности. Управление АС ОВД авторизованным администратором в соответствии с принятой политикой и утвержденными требованиями по безопасности. Однозначное установление прав и полномочий пользователей	Контроль за доступом в АС ОВД посторонних лиц. Включение в АС ОВД механизмов, направленных на предотвращение несанкционирован-ного логического проникновения в нее пользователей и процессов. Обеспечение соответствия принятых мер и механизмов защиты требованиям руководящих и нормативных документов. Контроль состояния СЗИ НСД в АС ОВД со стороны администратора безопасности	Регламентация доступа к секретным работам и документам. Регламентация доступа к техническим и программным средствам АС ОВД. Идентификация и проверка подлинности субъектов доступа. Идентификация терминалов, узлов сети, внешних устройств ЭВМ по их логическим адресам. Идентификация программ, каталогов, томов, файлов. Управление потоками информации;	1. Определение объектов защиты и субъектов доступа, их уровней конфиденциаль-ности. Формирование матрицы разграничения доступа. 2. Организация допускной работы. 3. Организация конфиденциальног о делопроизводства. Определение учитываемых носителей информации, ведение журналов их учета. 4. Определение ответственности пользователей за нарушение безопасности информации. 5. Создание структуры подразделения

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
АС ОВД		Учет носителей информации ограниченного доступа. Наличие администратора безопасности, ответственного за ведение, нормальное функционирова-ние и контроль работы системы защиты информации (СЗИ) от НСД	защиты государственной тайны (ПЗГТ), назначение администратора безопасности. Регламентация действий администратора безопасности. 6. Создание СЗИ от НСД, включающей в себя комплекс технологических, организационных, технических и программных мер и средств защиты на этапах подготовки, обработки, передачи и хранения электронных документов. 7. Использование в составе АС ОВД сертифицированны х средств защиты информации соответствующего класса защищенности. 8. Разработка организационно-распорядительных документов: инструкций, положений и т.п. 9. Настройка

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			администратором безопасности механизмов защиты. 10. Определение правил и порядка технического обслуживания и ремонта программно-аппаратных средств АС ОВД
2. Угроза безопасности: пользователю может быть отказано в возможности доступа к ресурсам АС ОВД **Последствия: снижение продуктивности работы**			
Гарантия доступности ресурсов АС ОВД авторизованным пользователям	Информация должна быть доступна для использования, когда это необходимо. Пользователи АС ОВД должны обладать всеми санкционированными полномочиями по доступу к информации	Осуществление начальной идентификации и аутентификации (первоначальная установка паролей). Разблокировка АС ОВД специальным программным обеспечением	1. Определение допустимых характеристик надежности, производительности, качества функционирования АС ОВД. Организация контроля за их стабильностью. 2. Определение процедур по допуску пользователей к работе в АС ОВД. 3. Определение процедур восстановления работоспособности АС ОВД. 4. Дублирование информации на различных типах носителей.

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			5. Исключение необоснованных ограничений на доступ к информации и ресурсам АС ОВД
3. Угроза безопасности: события, относящиеся к безопасности, могут быть не зарегистрированы или могут оказаться не связанными с соответствующими пользователями **Последствия: невозможность проведения расследований и идентификации нарушителя**			
Учет и регистрация действий пользователей и событий АС ОВД	Создание механизмов учета и регистрации действий в АС ОВД. Осуществление аудита системы безопасности, включающего распознавание, регистрацию, хранение и анализ информации, относящейся к системе защиты АС ОВД. Протоколирование результирующих записей аудита.	Регистрация: - входа/выхода субъектов доступа в систему/ из системы; - загрузки и инициализации операционной системы и ее программного останова; - выдачи печатных документов на «твердую» копию; - попыток доступа программных средств к защищаемым файлам	1. Определение системных событий, которые должны трактоваться как признаки НСД. 2. Определение перечня штатных механизмов регистрации, входящих в состав операционной системы, сертифицированной СЗИ, а также организационных мер, которые будут использоваться для контроля системных событий и регистрации выдачи печатных документов на «твердую» копию и записи информации на съемные магнитные

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			носители информации. 3. Определение регламентов контроля за системными событиями, периодов и правил архивирования и уничтожения системных журналов. 4. Сигнализация попыток НСД, осуществление блокировки персональной ЭВМ при попытке НСД. 5. Определение регламентов действий администратора безопасности при выявлении фактов НСД
4. Угроза безопасности: фальсификация механизмов защиты (их			

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
подделка) **Последствия: изменение контрольных и опознавательных данных; изменение или приведение в не безопасное состояние механизмов защиты**			
Исключение несанкциониро-ванного доступа к элементам программного обеспечения, обеспечивающим функционирование СЗИ в АС ОВД	В АС ОВД должны быть реализованы механизмы и применены программно-аппаратные средства исключения НСД к элементам программного обеспечения, обеспечивающим функционирование СЗИ	Ограничение и контроль за доступом к АС ОВД. Ограничение и контроль за доступом к ресурсам АС ОВД. Создание замкнутой программной среды, ограниченной перечнем программ, разрешенных для запуска в системе. Контроль и анализ атак на средства защиты. Защита от модификации программного обеспечения.	1. Определение правил инсталляции нового программного обеспечения в АС ОВД. Регламентация правил его установки и настройки. 2. Регламентирование технологических процессов подготовки, ввода и обработки электронных документов. 3. Разработка перечня мероприятий, проводимых в случае компрометации СЗИ от НСД, включающий немедленное удаление из системы действующих значений паролей, ключей шифрования и кодов аутентификации. 4. Организация учета внесения

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			изменений в программное обеспечение АС ОВД и СЗИ от НСД. 5. Организация контроля за действиями программистов в процессе модификации программного обеспечения. 6. Организация контроля за действиями пользователей в целях исключения возможности модификации программного обеспечения. 7. Учет эталонных копий программного обеспечения и СЗИ от НСД, регламентирование доступа к эталонным копиям
5. Угроза безопасности: компрометация статусной информации о системе защиты в случае аварии АС ОВД **Последствия: компрометация механизмов защиты**			
Гарантия корректности выполнения всех функций безопасности и сохранения состояние	Функции защиты должны претворяться в жизнь для любой деятельности по защите в любой момент	Самотестирование (вычисление контрольных сумм для программного обеспечения и СЗИ от НСД,	1. Тестирование целостности СЗИ путем подсчета контрольных сумм при каждой инициализации АС ОВД.

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
безопасности в случае сбоев АС ОВД и прерывания обслуживания	функционирования АС ОВД	проверка целостности баз данных). Синхронизация процессов защиты аппаратно-программных средств. Наличие средств восстановления программного обеспечения и СЗИ от НСД	2. Определение мероприятий по восстановлению работоспособности АС ОВД. 3. Определение регламентов проведения контроля работоспособности средств восстановления
6. Угроза безопасности: АС ОВД может быть инсталлирована с некорректной системой защиты Последствия: система защиты может быть изменена или приведена в небезопасное состояние			
Обеспечение инсталляции, управления, администрирования и использования АС ОВД способами, которые устанавливаются системой безопасности АС ОВД	Обеспечение гарантий корректности инсталляции программного обеспечения АС ОВД и СЗИ от НСД	Отказ от использования программного обеспечения, полученного некорректными способами. Ограничение круга лиц, имеющих полномочия по инсталляции программного обеспечения.	1. Использование лицензионных версий программного обеспечения. 2. Использование сертифицированной СЗИ от НСД. 3. Проведение инсталляции программного обеспечения АС ОВД и СЗИ от НСД только специально выделенными и обученными специалистами. 4. Проведение инсталляции программного обеспечения АС ОВД и СЗИ от

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			НСД только под контролем администратора безопасности АС. 5. Регистрация и учет всех действий по инсталляции и деинсталляции программного обеспечения
7. Угроза безопасности: АС ОВД может оказаться предметом физического воздействия **Последствия: АС ОВД не сможет корректно выполнять функции безопасности**			
Обеспечение защиты АС ОВД от физического воздействия. Исключение связей с другими системами или пользователями, неопределенным и системой безопасности информационных технологий	Обеспечение физической целостности аппаратных, программных средств, хранящихся данных и их носителей. Работа аппаратно-программных средств АС ОВД только в локально-автономном режиме	АС ОВД должна размещаться в помещениях, в которые невозможен несанкциониро-ванный физический доступ посторонних лиц. Программно-аппаратные средства АС ОВД должны быть защищены конструктивно от неавторизованного изменения потенциальным злоумышленником. АС ОВД не должна иметь	1. Должна осуществляться физическая охрана АС ОВД (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещена АС ОВД с помощью технических средств охраны и специального персонала, использование строгого пропускного режима. 2. Применение специального оборудование помещений АС ОВД.

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
		физических связей с другими информационными технологиями	3. Все подключения периферийных устройств (принтера, электронного тахометра, сканера, переносного компьютера и т.п.) должны находиться в пределах возможности контроля за доступом к ним со стороны ответственного сотрудника ПЗГТ
8. Угроза безопасности: неправильное администрирование и ошибки работы пользователей **Последствия: возникновение ошибок безопасности**			
Контроль состояния СЗИ от НСД	Контроль корректности настроек функций защиты	Проведение периодического анализа уязвимости системы защиты	1. Периодическое тестирование функция СЗИ от НСД при изменении программной среды и персонала АС ОВД с помощью тест-программ, имитирующих попытки НСД. 2. Определение контрольных точек и регламентов проведения анализа уязвимости АС ОВД

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
9. Угроза безопасности: воздействие специальных программных вирусов Последствия: нарушение работоспособности АС ОВД, искажение, нарушение целостности, модификация программного обеспечения и данных			
Обеспечение защиты от воздействия разрушающих программных средств	Осуществление антивирусного контроля. Восстановление файлов	Определение регламентов антивирусного контроля и процедур восстановления файлов	Применение актуальных на текущий момент времени средств диагностики и восстановления
10. Угроза безопасности: перехват техническими средствами разведки побочных электромагнитных излучений аппаратных средств АС ОВД Последствия: восстановление или раскрытие содержания информации, обрабатываемой и отображаемой на элементах АС ОВД			
Защита от распространения ПЭМИ за пределы контролируемой зоны	Применение средств защиты, не нарушающих функционирование АС ОВД по целевому назначению	Локализация ПЭМИ в пределах контролируемой зоны	1. Проведение специальных исследований на ПЭМИ элементов физической архитектуры технических средств АС ОВД. 2. Выбор, обоснование применение сертифицирова-нных средст специальной защить
11. Угроза безопасности: перехват техническими средствами разведки опасных сигналов от аппаратных средств АС ОВД Последствия: восстановление или раскрытие содержания информации, обрабатываемой и отображаемой на элементах АС ОВД			
Предотвращение утечки информации по цепям электропитания	Применение средств защиты, не нарушающих функционирование АС ОВД по целевому назначению	Локализация опасных сигналов в пределах контролируемой зоны	1. Создание выделенной подсети электропитания технических средств АС ОВД. 2. Применение

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			источников бесперебойного питания и/или сетевых фильтров. 3. Высокочастотное зашумление линий выделенной подсети электропитания
12. Угроза безопасности: перехват техническими средствами разведки опасных сигналов от аппаратных средств АС ОВД Последствия: восстановление или раскрытие содержания информации, обрабатываемой и отображаемой на элементах АС ОВД			
Предотвращение утечки информации по цепям заземления	Применение средств защиты, не нарушающих функционирование АС ОВД по целевому назначению	Локализация опасных сигналов в пределах контролируемой зоны	1. Создание специализированного контура заземления технических средств АС ОВД в пределах контролируемой зоны. 2. Обеспечение соответствия конструктивных элементов контура заземления требованиям нормативных документов. 3. Доведение величины сопротивления заземления до уровня величины, не превышающей 4 Ом. Паспортизация

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
			системы заземления. Организация проведения периодических инструментальных проверок (не реже 2 раз в год)
13. Угроза безопасности: наличие в АС ОВД специально внедренных электронных устройств перехвата информации Последствия: раскрытие содержания информации, обрабатываемой в АС ОВД			
Предотвращение утечки информации за пределы контролируемой зоны через специально внедренные электронные устройства	Систематический контроль параметров излучений технических средств АС ОВД	Гарантия отсутствия специально внедренных устройств в технические средства АС ОВД	1. Использование в АС ОВД технических средств, прошедших специальные лабораторные проверки на наличие внедренных электронных устройств. 2. Регламентация порядка и правил изменения физической архитектуры технических средств в АС ОВД
14. Угроза безопасности: наличие в программном обеспечении АС ОВД не декларированных возможностей			

Задачи безопасности	Функциональные требования	Требования безопасности	Мероприятия по реализации требований безопасности
Последствия: модификация информации, нарушение целостности информации или ее утрата; блокирование работоспособности АС ОВД			
Предотвращение утечки информации за счет наличия в программном обеспечении не декларированных возможностей	Исключение несанкционированной инсталляции любых программных средств	Применение только лицензионных и сертифицированных программных средств	Контроль наличия лицензий и сертификатов на применяемые и планируемые к применению программные средства

Приложение 5

Выписки из Уголовного кодекса Российской Федерации

Глава 28. Преступления в сфере компьютерной информации.

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), в системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершённое группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода, осуждённого за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системе ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или

заниматься определенной деятельностью на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Глава 29. Преступления против основ конституционного строя и безопасности государства.

Статья 283. Разглашение государственной тайны.

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены – наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 284. Утрата документов, содержащих государственную тайну.

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, – наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Выписки из Кодекса Российской Федерации об административных правонарушениях

Статья 23.45. Органы, осуществляющие контроль за обеспечением защиты государственной тайны.

1. Органы, осуществляющие контроль за обеспечением защиты государственной тайны, рассматривают дела об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.12, частью 2 статьи 13.13 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

5) руководитель федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители;

6) руководители подразделений федеральных органов исполнительной власти, уполномоченных в области противодействия техническим разведкам и технической защиты информации, осуществляющих лицензирование видов деятельности, которые связаны с использованием и защитой сведений, составляющих государственную тайну.

Статья 23.46. Органы, осуществляющие государственный контроль в области обращения и зашиты информации.

1. Органы, осуществляющие государственный контроль в области обращения и защиты информации, рассматривают дела об административных правонарушениях.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

п.2 руководитель федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители – об административных правонарушениях, предусмотренных статьей 13. б, частями 1 и 2 статьи 13.12, частью 1 статьи 13.13 настоящего Кодекса.

Статья 13.6. Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи.

Использование на сетях связи несертифицированных средств связи либо предоставление несертифицированных услуг связи, если законом предусмотрена их обязательная сертификация – влечет наложение административного штрафа на граждан в размере от пятнадцати до двадцати минимальных размеров оплаты труда с конфискацией несертифицированных средств связи либо без таковой; на должностных лиц – от тридцати до сорока минимальных размеров оплаты труда с конфискацией несертифицированных средств связи либо без таковой; на юридических лиц – от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств связи либо без таковой.

Статья 13.12. Нарушение правил защиты информации.

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), – влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда: на должностных лиц – от пяти до десяти минимальных размеров оплаты труда; на юридических лиц – от пятидесяти до ста минимальных размеров оплаты труда.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну) – влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных

средств защиты информации или без таковой; на должностных лиц – от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц – от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, – влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц – от ста пятидесяти до двухсот минимальных размеров оплаты труда.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, – влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц – от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации составляющей государственную тайну, или без таковой.

Статья 13.13. Незаконная деятельность в области зашиты информации.

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна) – влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц – от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц – от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для зашиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии – влечет наложение административного штрафа на должностных лиц в размере от сорока до пятидесяти минимальных размеров оплаты труда; на юридических лиц – от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Приложение 6

Выписки из Трудового кодекса Российской Федерации

Глава 14. Защита персональных данных работника.

Статья 65. Документы, предъявляемые при заключении трудового договора.

При заключении трудового договора лицо, поступающее на работу, предъявляет работодателю: паспорт или иной документ, удостоверяющий личность; трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства; страховое свидетельство государственного пенсионного страхования; документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу; документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки.

В отдельных случаях с учетом специфики работы настоящим Кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных настоящим Кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

При заключении трудового договора впервые трудовая книжка и страховое свидетельство государственного пенсионного страхования оформляются работодателем.

Статья 85. Понятие персональных данных работника. Обработка персональных данных работника.

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Обработка персональных данных работника – получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты.

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

1) обработка персональных данных работника может осуществляться

исключительно в целях обеспечения соблюдения законов и иных нормативных правовых «фактов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения:

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом;

8) работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области:

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Статья 87. Хранение и использование персональных данных работников.

Порядок хранения и использования персональных данных работников в организации устанавливается работодателем с соблюдением требований

настоящего Кодекса.

Статья 88. Передача персональных данных работника.

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;

разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций

Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

полную информацию об их персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом:

определение своих представителей для защиты своих персональных данных;

доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных

персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение 7

Кому: _____
(наименование органа по аттестации
и его адрес)

ЗАЯВКА
на проведение аттестации объекта информатизации

1. (наименование заявителя) просит провести аттестацию (наименование объекта информатизации) на соответствие требованиям по безопасности информации:_____2.
Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.
3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.
4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.
5. Дополнительные условия или сведения для договора:
   5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период _____
   5.2. Аттестационные испытания объекта информатики предлагаю провести в период _____
   5.3. Испытания несертифицированных средств и систем информатизации (наименование средств и систем) предусмотрено провести в испытательных центрах (лабораториях) (наименование испытательных центров) в период _____ (или предлагается провести непосредственно на аттестуемом объекте в период _____).

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)

Приложение
к форме «Заявки...»

Исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов:

1. Полное и точное наименование объекта информатизации и его назначение.

2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия)).

3. Организационная структура объекта информатизации.

4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).

5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

8. Наличие и характер взаимодействия с другими объектами информатизации.

9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.

10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому

объекту информатизации, влияющие на безопасность информации.

Приложение 8

«УТВЕРЖДАЮ»
(должность руководителя органа по аттестации)
м.п. Ф.И.О.
«___» _____ 20__ г.

АТТЕСТАТ СООТВЕТСТВИЯ
(указывается полное наименование объекта информатизации)
ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ ____

Действителен до «___» _____ 20__ г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что: (приводится полное наименование объекта информатизации) _____ категории _____ класса соответствует требованиям нормативной и методической документации по безопасности информации.

Состав комплекса технических средств объекта информатизации (с указанием заводских номеров, модели, изготовителя, номеров сертификатов), схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов) прилагаются.

2. Организационная структура, уровень подготовки специалистов, нормативное, методическое обеспечение и техническая оснащенность службы безопасности информации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищенности объекта информатизации в процессе эксплуатации в соответствии с установленными требованиями аттестационных испытаний, утвержденными «____» _____ 20__ г.

3. Аттестация объекта информатизации выполнена в соответствии с программой и методиками __ г. № _____.

4. С учетом результатов аттестационных испытаний на объекте информатизации разрешается обработка (указывается высшая степень секретности, конфиденциальности) информации.

5. При эксплуатации объекта информатизации запрещается: (указываются ограничения, которые могут повлиять на эффективность мер и средств защиты информации).

6. Контроль за эффективностью реализованных мер и средств защиты возлагается на службу безопасности информации.

7. Подробные результаты аттестационных испытаний приведены в заключении аттестационной комиссии (№ ____ «___» _____20__ г.) и

протоколах испытаний.

8. «Аттестат соответствия» выдан на _____ года, в течение которых должна быть обеспечена неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации,
могущих повлиять на характеристики, указанные в п. 9.

9. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации.

9.1. _____

9.2. _____

Руководитель аттестационной комиссии

(должность с указанием наименования предприятия)

Ф.И.О.

«____» _____ 20__ г.

Отметки органа надзора:

_____

Примечание. Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.