Министерство образования и науки Российской Федерации
Томский государственный университет
систем управления и радиоэлектроники
Институт системной интеграции и безопасности
Центр технологий безопасности

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Издание пятое, переработанное и дополненное

Рекомендовано Сибирским региональным отделение вузов России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности

В-Спектр
Томск 2011

УДК 004:056

О 75

О 75 Основы защиты информации: учебное пособие. Изд. 5-е, перераб. и доп. – Томск: В-Спектр, 2011. – 244 с.
ISBN 978-5-91191-214-7

Составители:

Шелупанов А.А., д.т.н., профессор
Зайцев А.П., к.т.н., профессор
Мещеряков Р.В., к.т.н., доцент
Давыдова Е.М., к.т.н.
Зыков В.Д., к.т.н.
Конев А.А., к.т.н.
Новгородова Н.А.,
Праскурин Г.А.,
Сопов М.А.,
Колесник Е.В.,
Колесник Е.А.

Учебное пособие содержит изложение основ защиты информации в различных аспектах.

Предназначено для студентов и слушателей курсов для групп специальностей «Информационная безопасность», а также для курсов повышения квалификации сотрудников организаций и предприятий различных форм собственности.

УДК 004:056

Рецензенты: **С.С. Бондарчук**, д.ф.-м.н., профессор
Г.И. Афонин, к.ф.-м.н., с.н.с.

ISBN 978-5-91191-214-7

© ЦТБ ТУСУР, 2011

СОДЕРЖАНИЕ

Авторское предисловие 5
1. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6
1.1. Понятие информационной безопасности 6
1.2. Информационное право в теории государства и права 9
1.3. Информация как объект правового регулирования 12
1.4. Защита информации 19
1.5. Информация ограниченного доступа 21
1.6. Правовые основы использования организационных и технических средств защиты информации 29
1.7. Лицензирование деятельности в области защиты информации .. 31
1.8. Сертификация, стандартизация, аккредитация в информационной сфере 38
1.9. Шифровальные (криптографические) средства защиты информации 49
1.10. Электронная цифровая подпись (ЭЦП) 53
1.11. Юридическая ответственность за нарушение норм защиты информации 59
Список литературы 69
2. ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 72
2.1. Введение 72
2.2. Функции организационной составляющей системы защиты информации 72
2.3. Регламентация работы с информацией и её носителями 74
2.4. Регламентация действий при осуществлении информационных процессов 76
2.5. Регламентация работы с элементами системы защиты информации 83
3 БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ 91
3.1. Введение 91
3.2. Ресурсы операционной системы 91
3.3. Методы обеспечения информационной безопасности в операционных системах 92
3.4. Аутентификация в операционных системах 93
3.5. Разграничение доступа к защищаемым объектам 104
3.6. Аудит событий 109
Список литературы 111
4. БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ 112
4.1. Ведение в базы данных 112

4.2. Безопасность баз данных 127
Список литературы 146
5. БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ 147
5.1. Основные термины и определения 147
5.2. Классификация сетей 149
5.3. Типовая сеть крупной организации 150
5.4. Уровни информационной инфраструктуры корпоративной сети 152
5.5. Классификация угроз, уязвимостей, атак 153
5.6. Защитные механизмы и контрмеры 159
6. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 180
6.1. Терминология 180
6.2. Угрозы со стороны участников информационного обмена 181
6.3. Требования к криптосистемам 181
6.4. Основные алгоритмы шифрования 182
6.5. Симметричные криптосистемы 183
6.6. Криптографические хэш-функции 185
6.7. Ассиметричные криптосистемы (криптосистемы с открытым ключом) 186
6.8. Управление ключами 189
6.9. Криптоанализ и атаки на криптосистемы 192
6.10. Характеристики безопасности обеспечиваемые средствами криптографической защиты информации: 194
6.11. Удостоверяющий центр 195
7. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ 209
7.1. Общие понятия 209
7.2. Технические каналы утечки информации. Структура, классификация и основные характеристики 209
7.2. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 213
Список литературы 243

Авторское предисловие

В учебном пособии рассматриваются ключевые разделы курсов по защите информации, предусмотрены как теоретические разделы, так и практические, направленные на развитие навыков анализа информационной безопасности объектов, а также путей их совершенствования.

Главная цель настоящего учебного пособия дать обучаемым азы, основы информационной безопасности и защиты информации, определить основные направления развития этой области знаний. В рамках образовательной программы попытаться сформировать у них элементы «информационной культуры». Авторы не претендуют на собственную исключительность и глубинные научные исследования в области информационной безопасности. Не случайно, что и пособие имеет название «Основы защиты информации», а не, например, «Теоретические основы информационной безопасности». В этом случае нам пришлось бы основательно потрудиться над теоретическими обоснованиями многих утверждений. Наша цель куда более скромна – побудить интерес у обучаемых к серьезному и вдумчивому изучению проблем информационной безопасности.

Достаточно точно, конкретно и правильно представлены понятия, определения и положения в ряде основополагающих работах В.И. Ярочкина, В.А. Герасименко, А.А. Малюка, С.П. Расторгуева и др. Многие из них мы будем использовать в учебном пособии, в частности, практически полностью вошли разделы, связанные с информационными системами. В пособии приведен словарь основных терминов.

Учебное пособие основано на опыте преподавания на кафедре Комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа ряда специальных дисциплин, включенных в государственный образовательный стандарт по специальностям: 090102 – «Компьютерная безопасность», 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем», 090105 – «Информационная безопасность телекоммуникационных систем». Необходимо также отметить, что именно в ФГОСах третьего направления остались эти специальности.

Пособие рассчитано на широкий круг читателей и может использоваться как учебно-методические указания, поскольку практически в каждом разделе имеются примеры с указаниями.

Мы выражаем свою благодарность всем сотрудникам кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа, сотрудникам Института криптографии связи и информатики Академии ФСБ России за помощь, конструктивную критику, советы и активную поддержку нашего скромного труда.

Авторы

1. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятие информационной безопасности

В Доктрине информационной безопасности РФ дается определение информационной безопасности.

Под информационной безопасностью Российской Федерации понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

В основе понятия «информационная безопасность» лежит понятие «безопасность», которое нашло свое отражение в Законе РФ «О безопасности».

Безопасность – это состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз. К жизненно важным интересам закон относит совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Основные объекты безопасности – личность, ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная ценность.

Таким образом, информационная безопасность – состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие.

Под защищенностью понимается совокупность правовых, научно-технических, специальных, организационных мер, направленных на своевременное выявление, предупреждение и пресечение неправомерного получения и распространения защищаемой информации, осуществляемых органами законодательной, исполнительной и судебной власти, общественными и иными организациями и объединениями, гражданами, принимающими участие в обеспечении информационной безопасности, в соответствии с законодательством, регламентирующим отношения в информационной сфере.

Одним из важнейших аспектов информационной безопасности является определение и классификация возможных угроз безопасности. Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. В Законе РФ «О безопасности» и Доктрине информационной безопасности РФ угрозы подразделяются на внешние и внутренние.

К внешним источникам угроз информационной безопасности РФ относятся: деятельность иностранных разведывательных и информационных структур, международных террористических организаций, а также

обострения международной конкуренции за обладание информационными технологиями и ресурсами; увеличение технологического отрыва ведущих государств мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий.

К внутренним источникам угроз относятся: критическое состояние отечественных отраслей промышленности; неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, усиления влияния организационной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере; недостаточная координация деятельности федеральных органов власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ; недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика; недостаточное финансирование мероприятий по обеспечению информационной безопасности; отставание России от ведущих стран мира по уровню информатизации в жизненно важных сферах государственной деятельности и ряд других.

Источниками внешних угроз являются: недобросовестные конкуренты; преступные группировки и формирования; отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть: администрация предприятия; персонал; технические средства обеспечения производственной и трудовой деятельности.

Основные проблемы информационной безопасности связаны, прежде всего, с умышленными угрозами (действия людей), так как они являются основной причиной и движущей силой преступлений и правонарушений. В то же время средства вычислительной техники (прежде всего ЭВМ), встраиваясь в систему отношений по поддержанию информационной безопасности, оказывают на них определенное воздействие. В отдельных случаях ЭВМ функционируют как источники повышенной опасности, и тогда нарушение установленных правил их эксплуатации может привести к нарушению информационной безопасности.

Деятельность по обеспечению информационной безопасности строится на основе принципов сформулированных в Законе РФ «О безопасности». К ним относятся: законность; соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности.

Применительно к информационной безопасности можно выделить принципы обоснованности, своевременности и прогноза.

Принцип обоснованности заключается в установлении путем экспертной оценки целесообразного ограничения доступа к конкретной информации, выделении вероятных экономических и иных последствий этого акта, исходя из баланса жизненно важных интересов личности, общества, государства, разработки адекватных мер противодействия внешним и внутренним угрозам информационной безопасности.

Принцип своевременности защиты информационной сферы позволяет реализовать процедуру предварительного ограничения доступа к защищаемой информации, осуществлять ее защиту и заключается в установлении ограничений на распространение этой информации с момента ее получения, разработки или заблаговременно.

Принцип прогноза информационной безопасности заключается в выделении конкретных внешних и внутренних угроз для охраняемой информационной сферы и базируется на объективной, реальной оценке охраняемых объектов – информации, инфраструктуры, субъектов, связанных с созданием, преобразованием и потреблением информации; моделировании возможной противоправной деятельности, посягающей на информационную безопасность.

На рис. 1.1 представлены направления и цели защиты информации и их взаимосвязь.

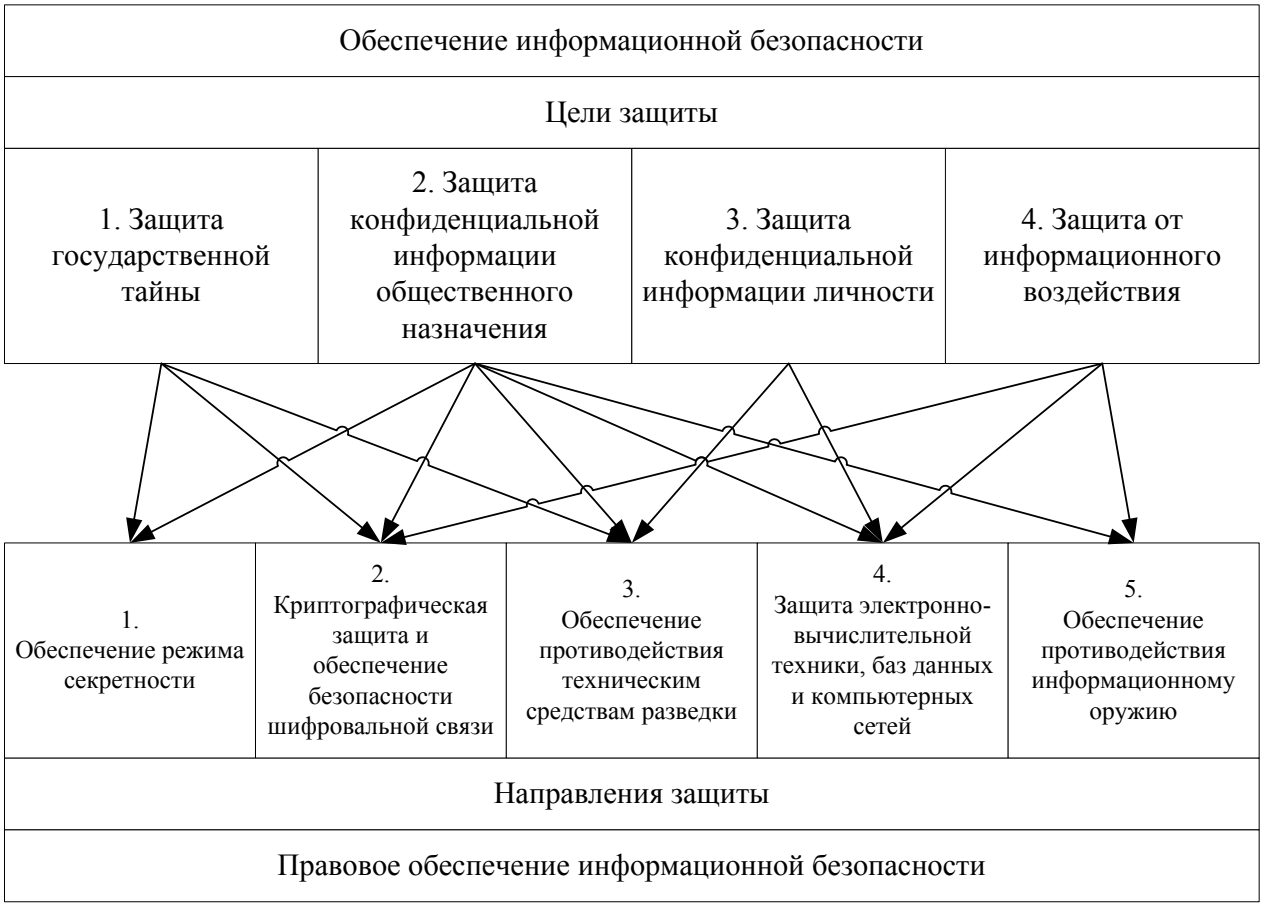


Рис. 1.1. Взаимосвязь целей и направлений защиты информации

Информационная безопасность в современных условиях стремительно приобретает все большую актуальность и значимость, является одним из приоритетных направлений обеспечения национальной безопасности России, а также международной безопасности, что требует теоретического осмысления основных положений информационной безопасности для совершенствования правовой базы и правоприменительной практики.

1.2. Информационное право в теории государства и права

Под правом понимается единая система норм, которая установлена или санкционирована государством, обязательная для всех членов общества.

Главное назначение права – обеспечение порядка в обществе с учетом интересов разных слоев и групп общества путем достижения согласия и компромисса.

Право состоит из отдельных правовых норм. Норма права – это установленное или санкционированное государством общеобязательное правило поведения общего характера, которое рассчитано на неопределенное число однотипных случаев и обращено ко всем и к каждому, оказавшимся в предусмотренной нормой жизненной ситуации.

Норма права представляет собой правило общего поведения, для которого характерна структура, представленная на рис. 1.2.



Рис. 1.2. Структура нормы права

Под формой (источником) права принято понимать способы придания официальной юридической силы правилу поведения и ее внешнее официальное выражение. Форма показывает, каким способом государство создает, фиксирует ту или иную норму права, в каком виде эта норма доводится до сознания людей (рис. 1.3).



Рис. 1.3. Формы (источники) права

Нормативно-правовой акт – это официальный, письменный документ, изданный органом государства, в пределах установленной компетенции, направленный на введение в действие правовых норм, на изменение существующих, либо их отмену.

Нормативно-правовые акты, в зависимости от их юридической силы, органа, который их принял, и способа принятия делятся на две большие группы: на законы и подзаконные акты. Классификация нормативно-правовых актов представлена на рис. 1.4.

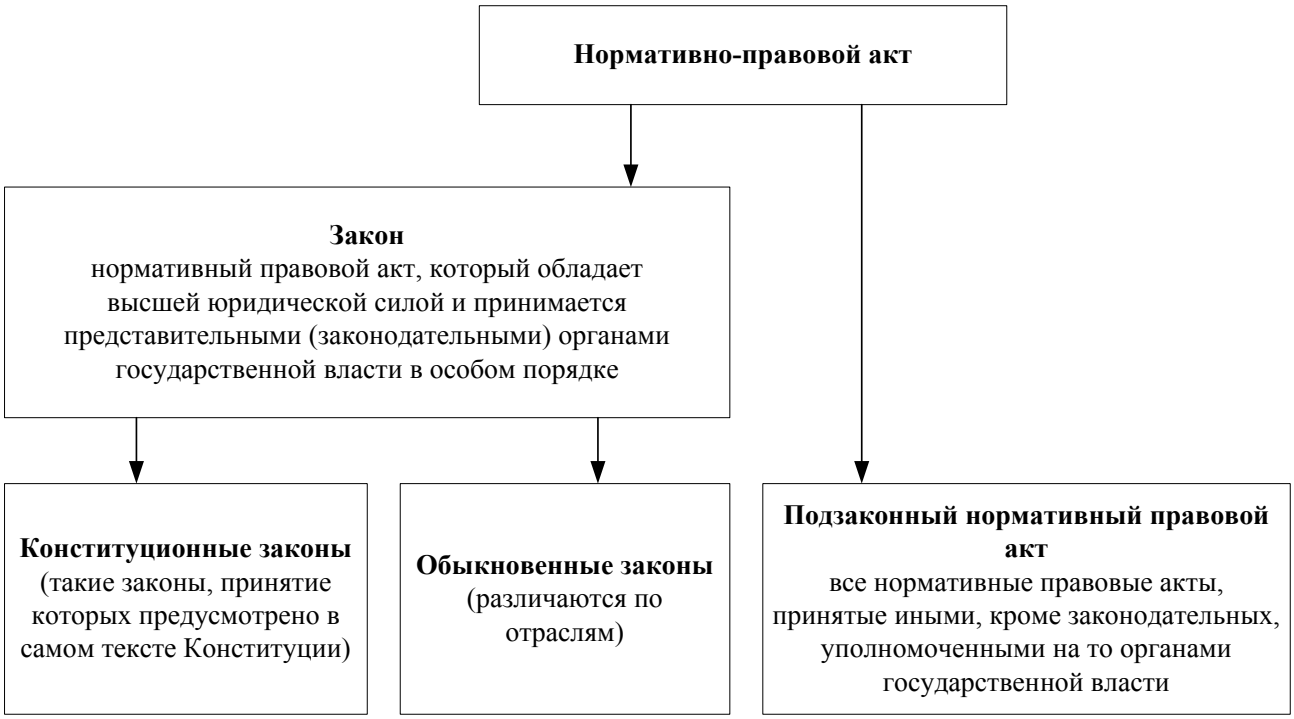


Рис. 1.4. Классификация нормативно-правовых актов

В юридической науке принято использовать понятие «структура правоотношения». Элементы этой структуры следующие:

– содержание правоотношения;

– субъекты правоотношения – те лица, которые могут быть их участниками. Основные участники правоотношений – физические лица и организации;

– объекты правоотношения – материальные и нематериальные блага, на которые направлены действия субъектов правоотношения.

Чтобы быть участником правоотношения, необходимо обладать определенными юридическими качествами (правосубъектностью): правоспособностью, дееспособностью и деликтоспособностью.

Система права означает внутреннюю организацию права, связи между его основными компонентами. Система права включает в себя четыре компонента: нормы права, правовые институты, суботрасли (подотрасли) и отрасли (рис. 1.5).



Рис. 1.5. Компоненты системы права

1.3. Информация как объект правового регулирования

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации, федеральных законах и других регулирующих отношения по использованию информации законах.

Согласно «Конституции Российской Федерации», человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства (ст. 2).

Государство, зафиксировав права и свободы человека и гражданина в «Конституции Российской Федерации» (гл. 2), обязуется через деятельность государственных, правоохранительных органов осуществлять их реализацию и защиту.

В «Конституции Российской Федерации» зафиксированы основные положения о правах и свободах человека и гражданина в информационной сфере, например:

– каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23, ч. 1);

– каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ст. 23, ч. 2);

– сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24, ч. 1);

– органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ст. 24, ч. 2);

– каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом (ст. 29, ч. 4);

– каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом (ст. 44, ч. 1).

– государственная защита прав и свобод человека и гражданина в Российской Федерации гарантируется (ст. 45).

Дальнейшее правовое регулирование этих отношений и их защита отражены в федеральных законах и иных нормативных актах.

В соответствия с федеральным законом «Об информации, информационных технологиях и о защите информации»:

– информация – сведения (сообщения, данные) независимо от формы их представления;

– информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

– информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

– доступ к информации – возможность получения информации и ее использования;

– предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

– распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Информация может являться объектом публичных, гражданских и иных правовых отношений.

Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

К основным требованиям к защищаемой информации относят:

– конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [4];

– доступность информации – состояние информации, когда она находится в то время, в том виде и том месте, когда она необходима;

– целостность информации – свойство, при выполнении которого информация сохраняет заранее определенный вид и качество.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Граждане (физические лица) и организации (юридические лица) (далее – организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законами.

Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое

положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

Информация в зависимости от категории доступа к ней подразделяется на:

– общедоступную информацию,

– информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном феде-

ральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Информационные системы включают в себя:

1) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными законами.

Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года N 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления – Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

Правительство Российской Федерации вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных государственных информационных систем.

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, федеральных законов и иных нормативных правовых актов Российской Федерации.

Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

1.4. Защита информации

Защита информации согласно закону «Об информации, информационных технологиях и о защите информации» представляет собой принятие правовых, организационных и технических мер, направленных на:

1) 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.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите инфор-

мации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Правонарушения в сфере информации, информационных технологий и защиты информации влекут за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

1.5. Информация ограниченного доступа

1.5.1. Правовой режим защиты государственной тайны

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Законодательство РФ о государственной тайне основывается на «Конституции Российской Федерации, законе «О безопасности» и включает закон «О государственной тайне», а также положение других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Согласно закону «О государственной тайне»:

– государственная тайна (ГТ)– защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

– носители сведений, составляющих государственную тайну,

– материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов сигналов, технических решений и процессов;

– система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях;

– допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;

– доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

– гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

– средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Согласно ст. 29 Конституции Российской Федерации, перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Перечень сведений, составляющих государственную тайну, содержится в законе «О государственной тайне»:

– сведения в военной области;

– сведения в области экономики, науки и техники;

– сведения в области внешней политики и экономики;

– сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные (ст. 12):

– о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

– об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

– о регистрационном номере;

– о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Степень секретности является показателем уровня важности и ценности информации для собственника, определяющий уровень ее защиты.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

– «секретно»;

– «совершенно секретно»;

– «особой важности».

Согласно постановлению Правительства РФ «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»:

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный инте-

ресам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с перечнем сведений, составляющих государственную тайну, «Перечень сведений, отнесенных к государственной тайне».

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Постановление Правительства РФ «Об утверждении правил разработки перечня сведений, отнесенных к государственной тайне» регламентирует правила разработки перечней сведений, отнесенных к государственной тайне.

Рассекречивание сведений и их носителей – снятие ранее введенных в предусмотренном законом «О государственной тайне» порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основаниями для рассекречивания сведений являются:

– взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;

– изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Постановление Правительства РФ определяет инструкцию о порядке допуска должностных лиц и граждан российской федерации к государственной тайне.

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться (ст. 24):

– права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

– права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

– права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие социальные гарантии:

– процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

– преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых «Конституцией Российской Федерации», федеральными конституционными законами и федеральными законами (ст. 30).

Органы государственной власти, наделенные в соответствии с законом полномочиями по распоряжению сведениями, составляющими государственную тайну, обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных их органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

1.5.2. Правовой режим защиты конфиденциальной информации

Согласно «Перечню сведений конфиденциального характера» к конфиденциальной информации относят:

1) Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональ-

ные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2) Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. N 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации.

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

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

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

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

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Защита коммерческой тайны устанавливается федеральным законом «О коммерческой тайне».

Согласно закону «О коммерческой тайне»:

– коммерческая тайна – 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;

– информация, составляющая коммерческую тайну (секрет производства), – 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 ценность 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;

– обладатель информации, составляющей коммерческую тайну, – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

– доступ к информации, составляющей коммерческую тайну, – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

– передача информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

– предоставление информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

– разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Термин **«служебная информация»** находит свое отражение в различных законодательных актах, например:

– служебная информация государственного служащего согласно «О государственной гражданской службе Российской Федерации»;

– служебная информация Правительства РФ согласно «О Правительстве Российской Федерации»;

– служебная информация муниципального служащего согласно «Об основах муниципальной службы в Российской Федерации»;

– служебная информация служащего Банка России согласно «О Центральном банке Российской Федерации (Банке России)»;

– служебная информация на рынке ценных бумаг согласно «О рынке ценных бумаг»;

– служебная информация сотрудника Федеральной службы безопасности согласно «О Федеральной службе безопасности»;

– и ряде других нормативно-правовых актов.

Таким образом, **служебная тайна –** это охраняемые законом конфиденциальные сведения о деятельности государственных органов, доступ к которым ограничен федеральным законом или в силу служебной необ-

ходимости, а также ставшие известными сведения в государственных органах и органах местного самоуправления только на законном основании и в силу исполнения их представителями служебных обязанностей, имеющие действительную или потенциальную ценность в силу неизвестности их третьим лицам, к ним нет свободного доступа на законном основании, обладатель сведений принимает меры к их конфиденциальности.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

В соответствии с признаком профессиональной принадлежности, из действующего законодательства можно выделить следующие виды **профессиональных тайн**:

- врачебная тайна,
- адвокатская тайна,
- банковская тайна,
- нотариальная тайна,
- тайна усыновления,
- тайна страхования,
- тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений,
- тайна связи,
- тайна совещания судей,
- тайна совещания присяжных заседателей,
- налоговая тайна
- и ряд других.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом «О персональных данных».

Согласно закону «О персональных данных»:

– **персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, соци-

альное, имущественное положение, образование, профессия, доходы, другая информация;

– оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

– обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

– распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

– использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

– блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

– уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

– конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

– общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Конституционное положение о недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (ст. 24) является одной из гарантий закрепленного в ст. 23 «Конституции Российской Федерации» права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Все это не противоречит ст. 12 «Всеобщей декларации прав человека» и ст. 8 «Европейской конвенции о защите прав человека и основных свобод». Согласно ст. 12 никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Согласно ст. 8 каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции; не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц.

Таким образом, **тайна частной жизни** – это охраняемые законом конфиденциальные сведения, составляющие личную, семейную тайну лица, тайну переписки, почтовых, телефонных переговоров и иных сообщений, незаконное собирание или распространение которых причиняет вред правам и законным интересам этого лица.

Государство призвано защищать частную жизнь лица от незаконного и необоснованного проникновения в нее со стороны, как государственных органов, органов местного самоуправления, так и негосударственных организаций, учреждений, а также отдельных граждан.

1.6. Правовые основы использования организационных и технических средств защиты информации

Согласно доктрине Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

– создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

– усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

– разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

– создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

– выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

– лицензирование деятельности в области защиты информации;

– сертификация средств защиты информации,

– стандартизация способов и средств защиты информации;

– совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

– контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;

– формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

– лицензирование деятельности организаций в области защиты информации;

– аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

– сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

– введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

– создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

1.7. Лицензирование деятельности в области защиты информации

Среди методов обеспечения безопасности информации, отмеченных в Доктрине информационной безопасности Российской Федерации, одно из важных мест занимают сертификация средств защиты информации и лицензирование деятельности в области защиты информации.

Согласно закону о «Лицензировании отдельных видов деятельности»:

– лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю;

– лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом;

– лицензирование – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании;

– лицензионные требования и условия – совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности;

– лицензирующие органы – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом;

– лицензиат – юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности;

– соискатель лицензии – юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности;

– реестр лицензий – совокупность данных о предоставлении лицензий, переоформлении документов, подтверждающих наличие лицензий, приостановлении и возобновлении действия лицензий и об аннулировании лицензий.

В целях обеспечения единства экономического пространства на территории Российской Федерации Правительство Российской Федерации в соответствии с определенными Президентом Российской Федерации основными направлениями внутренней политики государства:

– утверждает положения о лицензировании конкретных видов деятельности;

– определяет федеральные органы исполнительной власти, осуществляющие лицензирование конкретных видов деятельности;

– устанавливает виды деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов Российской Федерации.

Лицензирующие органы осуществляют следующие полномочия:

– предоставление лицензий;

– переоформление документов, подтверждающих наличие лицензий;

– приостановление действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий и возобновление действия лицензий;

– прекращение действия лицензий в случае, предусмотренных законом;

– ведение реестров лицензий, предоставление заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании;

– контроль за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий;

– обращение в суд с заявлениями об аннулировании лицензий.

Порядок осуществления полномочий лицензирующих органов устанавливается положениями о лицензировании конкретных видов деятельности.

Лицензирующие органы формируют открытые и общедоступные государственные информационные ресурсы, содержащие сведения из реестров лицензий, положения о лицензировании конкретных видов деятельности, а также технические регламенты и иные нормативные правовые акты Российской Федерации, устанавливающие обязательные требования к лицензируемым видам деятельности, за исключением случаев,

если в интересах сохранения государственной или служебной тайны свободный доступ к таким ресурсам в соответствии с законодательством Российской Федерации ограничен.

Вид деятельности, на осуществление которого предоставлена лицензия, может выполняться только получившим лицензию юридическим лицом или индивидуальным предпринимателем.

Срок действия лицензии не может быть менее чем пять лет. Срок действия лицензии по его окончании может быть продлен по заявлению лицензиата.

Продление срока действия лицензии осуществляется в порядке переоформления документа, подтверждающего наличие лицензии.

Положениями о лицензировании конкретных видов деятельности может быть предусмотрено бессрочное действие лицензии.

Для получения лицензии соискатель лицензии направляет или представляет в соответствующий лицензирующий орган заявление о предоставлении лицензии и копии документов, перечень которых определяется положением о лицензировании конкретного вида деятельности и которые свидетельствуют о наличии у соискателя лицензии возможности выполнения лицензионных требований и условий, в том числе документов, наличие которых при осуществлении лицензируемого вида деятельности предусмотрено федеральными законами.

Лицензирующий орган проводит проверку полноты и достоверности сведений о соискателе лицензии, содержащихся в представленных соискателем лицензии заявлении и документах, а также проверку возможности выполнения соискателем лицензии лицензионных требований и условий в порядке, предусмотренном законом.

Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий сорока пяти дней со дня поступления заявления о предоставлении лицензии и прилагаемых к нему документов. Указанное решение оформляется соответствующим актом лицензирующего органа.

Более короткие сроки принятия решения о предоставлении или об отказе в предоставлении лицензии могут устанавливаться положениями о лицензировании конкретных видов деятельности.

Лицензирующий орган обязан в указанный срок уведомить соискателя лицензии о принятии решения о предоставлении или об отказе в предоставлении лицензии.

Уведомление о предоставлении лицензии направляется (вручается) соискателю лицензии в письменной форме.

Основанием отказа в предоставлении лицензии является:

– наличие в документах, представленных соискателем лицензии, недостоверной или искаженной информации;

– несоответствие соискателя лицензии, принадлежащих ему или используемых им объектов лицензионным требованиям и условиям.

Соискатель лицензии имеет право обжаловать в порядке, установленном законодательством Российской Федерации, отказ лицензирующего органа в предоставлении лицензии или его бездействие.

В решении о предоставлении лицензии и в документе, подтверждающем наличие лицензии, указываются:

– наименование лицензирующего органа;

– полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование, и организационно-правовая форма юридического лица, место его нахождения, адреса мест осуществления лицензируемого вида деятельности, государственный регистрационный номер записи о создании юридического лица;

– фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, место его жительства, адреса мест осуществления лицензируемого вида деятельности, данные документа, удостоверяющего его личность, основной государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя;

– лицензируемый вид деятельности (с указанием выполняемых работ и оказываемых услуг при осуществлении видов деятельности, указанных в п. 2 ст. 17 Федерального закона «О лицензировании отдельных видов деятельности»);

– срок действия лицензии;

– идентификационный номер налогоплательщика;

– номер лицензии;

– дата принятия решения о предоставлении лицензии.

Документ, подтверждающий наличие лицензии, оформляется на бланке соответствующего лицензирующего органа – федерального органа исполнительной власти или органа исполнительной власти субъекта Российской Федерации по форме, утвержденной Правительством Российской Федерации, в двух экземплярах, один из которых направляется (вручается) соискателю лицензии, другой хранится в лицензионном деле лицензиата.

Лицензионный контроль проводится лицензирующим органом в целях проверки полноты и достоверности сведений о соискателе лицензии, содержащихся в представленных соискателем лицензии заявлении и документах, возможности выполнения им лицензионных требований и условий, а также проверки сведений о лицензиате и соблюдения им лицензионных требований и условий при осуществлении лицензируемого вида деятельности.

К отношениям, связанным с проведением лицензирующим органом проверки возможности выполнения соискателем лицензии лицензионных требований и условий и проверки соблюдения лицензиатом указанных

требований и условий при осуществлении лицензируемого вида деятельности, применяются положения Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

Приостановление действия лицензии осуществляется лицензирующим органом в случае привлечения лицензиата за нарушение лицензионных требований и условий к административной ответственности в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

Действие лицензии возобновляется лицензирующим органом со дня, следующего за днем истечения срока административного приостановления деятельности лицензиата, или со дня, следующего за днем досрочного прекращения исполнения административного наказания в виде административного приостановления деятельности лицензиата.

Срок действия лицензии на время приостановления ее действия не продлевается.

В случае, если в установленный судьей срок лицензиат не устранил нарушение лицензионных требований и условий, повлекшее за собой административное приостановление деятельности лицензиата, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

Лицензия аннулируется решением суда на основании рассмотрения заявления лицензирующего органа.

Лицензирующие органы ведут реестры лицензий на виды деятельности, лицензирование которых они осуществляют.

Информация, содержащаяся в реестре лицензий, является открытой для ознакомления с ней физических и юридических лиц.

Информация, содержащаяся в реестре лицензий, в виде выписок о конкретных лицензиатах предоставляется физическим и юридическим лицам за плату. Размер платы за предоставление указанной информации составляет 100 рублей.

Информация из реестра лицензий органам государственной власти и органам местного самоуправления предоставляется бесплатно.

Срок предоставления информации из реестра лицензий не может превышать три дня со дня поступления соответствующего заявления.

Статья 17 закона «О лицензировании отдельных видов деятельности» определяет перечень видов деятельности, на осуществление которых требуются лицензии. Для информационной сферы это, например:

– деятельность по распространению шифровальных (криптографических) средств;

– деятельность по техническому обслуживанию шифровальных (криптографических) средств;

– предоставление услуг в области шифрования информации;

– разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации;

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

– деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин (программ для ЭВМ), баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование указанных объектов авторских и смежных прав в силу федерального закона или договора);

Таким образом, на перечисленные в ст. 17 виды деятельности обязательно требуются лицензии.

Должностные лица лицензирующих органов в случае ненадлежащего исполнения своих обязанностей при осуществлении лицензирования конкретных видов деятельности и в случае совершения противоправных действий (бездействия) несут ответственность в соответствии с законодательством Российской Федерации.

Постановление Правительства «Об организации лицензирования отдельных видов деятельности» в соответствии с федеральным законом «О лицензировании отдельных видов деятельности» определяет перечень федеральных органов исполнительной власти, осуществляющих лицензирование. Так для информационной сферы это:

– ФСТЭК России – деятельность по технической защите конфиденциальной информации;

– ФСТЭК России, ФСБ России – деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

– ФСБ России – разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность; деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); деятельность по распространению шифровальных (криптографических) средств; Деятельность по техническому обслуживанию шифровальных (криптографических) средств; предоставление услуг в области шифрования информации; разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин, баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование указанных объектов авторских и смежных прав в силу федерального закона или договора)

Согласно данным лицензируемых видов деятельности соответствующими органами разработаны соответствующие конкретные положения о лицензировании данных видов деятельности, например:

– Постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации»;

– Постановление Правительства РФ «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

– Постановление Правительства РФ «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;

– Постановление Правительства РФ «Об утверждении положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными

предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность»;

– Постановление Правительства РФ «Об утверждении положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

– Постановление Правительства РФ «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» (вместе с:

«Положением о лицензировании деятельности по распространению шифровальных (криптографических) средств»;

«Положением о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств»;

«Положением о лицензировании предоставления услуг в области шифрования информации»;

«Положением о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем»);

– и др.

1.8. Сертификация, стандартизация, аккредитация в информационной сфере

Согласно закону «О техническом регулировании»:

– аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия;

– безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее – безопасность) – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;

– декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов;

– декларация о соответствии – документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов;

– заявитель – физическое или юридическое лицо, которое для подтверждения соответствия принимает декларацию о соответствии или об-

ращается за получением сертификата соответствия, получает сертификат соответствия;

– знак обращения на рынке – обозначение, служащее для информирования приобретателей о соответствии выпускаемой в обращение продукции требованиям технических регламентов;

– знак соответствия – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту;

– идентификация продукции – установление тождественности характеристик продукции ее существенным признакам;

– контроль (надзор) за соблюдением требований технических регламентов – проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки;

– международный стандарт – стандарт, принятый международной организацией;

– национальный стандарт – стандарт, утвержденный национальным органом Российской Федерации по стандартизации;

– орган по сертификации – юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации;

– оценка соответствия – прямое или косвенное определение соблюдения требований, предъявляемых к объекту;

– подтверждение соответствия – документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

– продукция – результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях;

– сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

– сертификат соответствия – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

– система сертификации – совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;

– стандарт – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

– стандартизация – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг;

– техническое регулирование – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия;

– технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или межправительственным соглашением, заключенным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации);

– форма подтверждения соответствия – определенный порядок документального удостоверения соответствия продукции или иных объек-

тов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Законодательство Российской Федерации о техническом регулировании состоит из настоящего Федерального закона, принимаемых в соответствии с ним федеральных законов и иных нормативных правовых актов Российской Федерации.

Подтверждение соответствия осуществляется в целях:

– удостоверения соответствия продукции, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, работ, услуг или иных объектов техническим регламентам, стандартам, сводам правил, условиям договоров;

– содействия приобретателям в компетентном выборе продукции, работ, услуг;

– повышения конкурентоспособности продукции, работ, услуг на российском и международном рынках;

– создания условий для обеспечения свободного перемещения товаров по территории Российской Федерации, а также для осуществления международного экономического, научно-технического сотрудничества и международной торговли.

Подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер.

Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Обязательное подтверждение соответствия осуществляется в формах:

– принятия декларации о соответствии (далее – декларирование соответствия);

– обязательной сертификации.

Добровольное подтверждение соответствия осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации. Добровольное подтверждение соответствия может осуществляться для установления соответствия национальным стандартам, стандартам организаций, сводам правил, системам добровольной сертификации, условиям договоров.

Объектами добровольного подтверждения соответствия являются продукция, процессы производства, эксплуатации, хранения, перевозки, реализации и утилизации, работы и услуги, а также иные объекты, в отношении которых стандартами, системами добровольной сертификации и договорами устанавливаются требования.

Система добровольной сертификации может быть создана юридическим лицом и (или) индивидуальным предпринимателем или несколькими юридическими лицами и (или) индивидуальными предпринимателями.

Федеральный орган исполнительной власти по техническому регулированию ведет единый реестр зарегистрированных систем добровольной сертификации.

Объекты сертификации, сертифицированные в системе добровольной сертификации, могут маркироваться знаком соответствия системы добровольной сертификации. Порядок применения такого знака соответствия устанавливается правилами соответствующей системы добровольной сертификации.

Применение знака соответствия национальному стандарту осуществляется заявителем на добровольной основе любым удобным для заявителя способом в порядке, установленном национальным органом по стандартизации.

Объекты, соответствие которых не подтверждено в порядке, установленном настоящим Федеральным законом, не могут быть маркированы знаком соответствия.

Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента.

Объектом обязательного подтверждения соответствия может быть только продукция, выпускаемая в обращение на территории Российской Федерации.

Форма и схемы обязательного подтверждения соответствия могут устанавливаться только техническим регламентом с учетом степени риска недостижения целей технических регламентов.

Декларация о соответствии и сертификат соответствия имеют равную юридическую силу независимо от схем обязательного подтверждения соответствия и действуют на всей территории Российской Федерации.

Срок действия декларации о соответствии определяется техническим регламентом.

Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем. Схемы сертификации, применяемые для сертификации определенных видов продукции, устанавливаются соответствующим техническим регламентом.

Соответствие продукции требованиям технических регламентов подтверждается сертификатом соответствия, выдаваемым заявителю органом по сертификации.

Срок действия сертификата соответствия определяется соответствующим техническим регламентом.

Форма сертификата соответствия утверждается федеральным органом исполнительной власти по техническому регулированию.

Обязательная сертификация осуществляется органом по сертификации, аккредитованным в порядке, установленном Правительством Российской Федерации.

Федеральный орган исполнительной власти по техническому регулированию ведет единый реестр выданных сертификатов соответствия.

Порядок формирования и ведения единого реестра сертификатов соответствия, порядок предоставления содержащихся в указанном реестре сведений и оплаты за их предоставление, а также федеральный орган исполнительной власти, организующий формирование и ведение указанного реестра, определяется Правительством Российской Федерации.

Исследования (испытания) и измерения продукции при осуществлении обязательной сертификации проводятся аккредитованными испытательными лабораториями (центрами).

Аккредитованные испытательные лаборатории (центры) проводят исследования (испытания) и измерения продукции в пределах своей области аккредитации на условиях договоров с органами по сертификации. Органы по сертификации не вправе предоставлять аккредитованным испытательным лабораториям (центрам) сведения о заявителе.

Продукция, соответствие которой требованиям технических регламентов подтверждено в порядке, предусмотренном настоящим Федеральным законом, маркируется знаком обращения на рынке. Изображение знака обращения на рынке устанавливается Правительством Российской Федерации. Данный знак не является специальным защищенным знаком и наносится в информационных целях.

Маркировка знаком обращения на рынке осуществляется заявителем самостоятельно любым удобным для него способом.

Продукция, соответствие которой требованиям технических регламентов не подтверждено в порядке, установленном настоящим Федеральным законом, не может быть маркирована знаком обращения на рынке.

Государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, подведомственными им государственными учреждениями, уполномоченными на проведение государственного контроля (надзора) в соответствии с законодательством Российской Федерации (далее – органы государственного контроля (надзора)).

Государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется должностными лицами органов государственного контроля (надзора) в порядке, установленном законодательством Российской Федерации.

Государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется в отношении продукции или

связанных с требованиями к ней процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации исключительно в части соблюдения требований соответствующих технических регламентов.

В отношении продукции государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется исключительно на стадии обращения продукции.

За нарушение требований технических регламентов изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) несет ответственность в соответствии с законодательством Российской Федерации.

В случае неисполнения предписаний и решений органа государственного контроля (надзора) изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) несет ответственность в соответствии с законодательством Российской Федерации.

Орган по сертификации и должностное лицо органа по сертификации, нарушившие правила выполнения работ по сертификации, если такое нарушение повлекло за собой выпуск в обращение продукции, не соответствующей требованиям технических регламентов, несут ответственность в соответствии с законодательством Российской Федерации и договором о проведении работ по сертификации.

Аккредитованная испытательная лаборатория (центр), эксперты в соответствии с законодательством Российской Федерации и договором несут ответственность за недостоверность или необъективность результатов исследований (испытаний) и измерений.

Стандартизация осуществляется в целях:

– повышение уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества, объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера, повышение уровня экологической безопасности, безопасности жизни и здоровья животных и растений;

– обеспечение конкурентоспособности и качества продукции (работ, услуг), единства измерений, рационального использования ресурсов, взаимозаменяемости технических средств (машин и оборудования, их составных частей, комплектующих изделий и материалов), технической и информационной совместимости, сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных, проведения анализа характеристик продукции (работ, услуг), исполнения государственных заказов, добровольного подтверждения соответствия продукции (работ, услуг);

– содействие соблюдению требований технических регламентов;

– создание систем классификации и кодирования технико-экономической и социальной информации, систем каталогизации продукции (работ, услуг), систем обеспечения качества продукции (работ, услуг), систем поиска и передачи данных, содействие проведению работ по унификации.

Стандартизация осуществляется в соответствии с принципами:

– добровольного применения документов в области стандартизации;

– максимального учета при разработке стандартов законных интересов заинтересованных лиц;

– применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям либо Российская Федерация в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения;

– недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг в большей степени, чем это минимально необходимо для выполнения целей, указанных в ст. 11 Федерального закона «О техническом регулировании»;

– недопустимости установления таких стандартов, которые противоречат техническим регламентам;

– обеспечения условий для единообразного применения стандартов.

К документам в области стандартизации, используемым на территории Российской Федерации, относятся:

– национальные стандарты;

– правила стандартизации, нормы и рекомендации в области стандартизации;

– применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации;

– стандарты организаций;

– своды правил;

– международные стандарты, региональные стандарты, региональные своды правил, стандарты иностранных государств и своды правил иностранных государств, зарегистрированные в Федеральном информационном фонде технических регламентов и стандартов;

– надлежащим образом заверенные переводы на русский язык международных стандартов, региональных стандартов, региональных сводов правил, стандартов иностранных государств и сводов правил иностранных государств, принятые на учет национальным органом Российской Федерации по стандартизации.

Участники работ по стандартизации, а также национальные стандарты, общероссийские классификаторы технико-экономической и социальной информации, правила их разработки и применения, правила стандартизации, нормы и рекомендации в области стандартизации, своды правил образуют национальную систему стандартизации.

Национальные стандарты разрабатываются в порядке, установленном настоящим Федеральным законом. Национальные стандарты утверждаются национальным органом по стандартизации в соответствии с правилами стандартизации, нормами и рекомендациями в этой области.

Национальный стандарт применяется на добровольной основе равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, являющихся изготовителями, исполнителями, продавцами, приобретателями.

Применение национального стандарта подтверждается знаком соответствия национальному стандарту.

Общероссийские классификаторы технико-экономической и социальной информации (далее – общероссийские классификаторы) – нормативные документы, распределяющие технико-экономическую и социальную информацию в соответствии с ее классификацией (классами, группами, видами и другим) и являющиеся обязательными для применения при создании государственных информационных систем и информационных ресурсов и межведомственном обмене информацией.

Стандарты организаций, в том числе коммерческих, общественных, научных организаций, саморегулируемых организаций, объединений юридических лиц могут разрабатываться и утверждаться ими самостоятельно исходя из необходимости применения этих стандартов для целей, указанных в ст. 11 Федерального закона «О техническом регулировании», для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и разработок.

Национальный стандарт применяется на добровольной основе равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, являющихся изготовителями, исполнителями, продавцами, приобретателями.

Национальные стандарты и общероссийские классификаторы, а также информация об их разработке должны быть доступны заинтересованным лицам.

Официальное опубликование в установленном порядке национальных стандартов и общероссийских классификаторов осуществляется национальным органом по стандартизации. Порядок опубликования национальных стандартов и общероссийских классификаторов определяется уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

Технические регламенты, документы национальной системы стандартизации, международные стандарты, правила стандартизации, нормы стандартизации и рекомендации по стандартизации, национальные стандарты других государств и информация о международных договорах в области стандартизации и подтверждения соответствия и о правилах их применения составляют Федеральный информационный фонд технических регламентов и стандартов.

Федеральный информационный фонд технических регламентов и стандартов является государственным информационным ресурсом.

Порядок создания и ведения Федерального информационного фонда технических регламентов и стандартов, а также правила пользования этим фондом устанавливаются Правительством Российской Федерации.

В Российской Федерации в порядке и на условиях, которые установлены Правительством Российской Федерации, создается и функционирует единая информационная система, предназначенная для обеспечения заинтересованных лиц информацией о документах, входящих в состав Федерального информационного фонда технических регламентов и стандартов.

Заинтересованным лицам обеспечивается свободный доступ к создаваемым информационным ресурсам, за исключением случаев, если в интересах сохранения государственной, служебной или коммерческой тайны такой доступ должен быть ограничен.

Обозначение национального стандарта Российской Федерации состоит из индекса ГОСТ Р, регистрационного номера и отделенных тире двух последних цифр года утверждения. Например: ГОСТ Р 50314–92. С 2000 г. год утверждения указывается четырьмя цифрами. Например: ГОСТ 7.60–2003.

В настоящее время проводится работа по гармонизации межгосударственных и национальных стандартов с международными стандартами.

Россия активно сотрудничает с международными организациями по стандартизации – Международной электротехнической комиссией (МЭК), Международной организацией по стандартизации (ИСО), Международным союзом электросвязи (МСЭ) и др., – принимая участие в разработке международных стандартов и в обеспечении их применения в народном хозяйстве страны.

В случае, когда стандарты оформлены на основе аутентичного текста международного стандарта и содержат дополнительные требования, обо-

значение примененного международного стандарта приводится в скобках, например: ГОСТ 7.32–91 (ИСО 5966–82) и ГОСТ Р 50314–92 (ИСО 7944–84).

Государственные стандарты, например:

– ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России;

– ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Госстандарт России;

– ГОСТ Р 51188–98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России;

– ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России;

– ГОСТ Р ИСО 7498-1–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России;

– ГОСТ Р ИСО 7498-2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России;

– ГОСТ Р ИСО/МЭК 15408-1–2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель. Госстандарт России;

– ГОСТ Р ИСО/МЭК 15408-2–2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России;

– ГОСТ Р ИСО/МЭК 15408-3–2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России;

– ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества;

– ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

– ГОСТ 34.11–94. Информационная технология. Криптографическая защита информации. Функция хэширования;

– ГОСТ Р 52292–2004. Информационная технология. Электронный обмен информацией. Термины и определения;

– и др.

Согласно закону «Об информации, информационных технологиях и о защите информации» технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

Согласно закону о «О государственной тайне» технические средства: средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

1.9. Шифровальные (криптографические) средства защиты информации

Приказ ФСБ РФ «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Шифровальные (криптографические) средства защиты информации конфиденциального характера в настоящем Положении именуются средствами криптографической защиты информации (далее – СКЗИ). К СКЗИ относятся:

– средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

– средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

– средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи под-

линности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

– средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

– средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

– ключевые документы (независимо от вида носителя ключевой информации).

Требования Положения ПКЗ-2005 носят рекомендательный характер при разработке, производстве, реализации и эксплуатации:

– средств криптографической защиты информации, доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лиц, не являющихся государственными органами или организациями, выполняющими государственные заказы;

– средств криптографической защиты информации открытых и общедоступных государственных информационных ресурсов Российской Федерации;

– средств электронной цифровой подписи, предназначаемых для использования в электронном документообороте, информация которого не относится к информации конфиденциального характера;

– информационно-телекоммуникационных систем, реализующих функции криптографической защиты информации, не относящейся к информации конфиденциального характера.

Режим защиты информации путем использования СКЗИ устанавливается обладателем информации конфиденциального характера, собственником (владельцем) информационных ресурсов (информационных систем) или уполномоченными ими лицами на основании законодательства Российской Федерации.

При организации обмена информацией конфиденциального характера, участниками которого являются государственные органы и организации, выполняющие государственные заказы, необходимость криптографической защиты информации и выбор применяемых СКЗИ определяются государственными органами или организациями, выполняющими государственные заказы.

Необходимость криптографической защиты информации конфиденциального характера при ее обработке и хранении без передачи по каналам связи, а также выбор применяемых СКЗИ определяются обладателем или пользователем (потребителем) данной информации.

СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом Федеральным законом «О техническом регулировании».

Качество криптографической защиты информации конфиденциального характера, осуществляемой СКЗИ, обеспечивается реализацией требований по безопасности информации, предъявляемых к СКЗИ, ключевой системе СКЗИ, а также к сетям связи (системам), используемым СКЗИ с целью защиты информации при ее передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении (далее – сети (системы) конфиденциальной связи) и условиям размещения СКЗИ при их использовании (далее – требования по безопасности информации).

Для криптографической защиты информации конфиденциального характера должны использоваться СКЗИ, удовлетворяющие требованиям по безопасности информации, устанавливаемым в соответствии с законодательством Российской Федерации.

Реализация в конкретных образцах СКЗИ и сетях (системах) конфиденциальной связи требований по безопасности информации возлагается на разработчика СКЗИ.

Задание разработки СКЗИ для федеральных государственных нужд осуществляется государственным заказчиком по согласованию с ФСБ России.

Разработка СКЗИ в интересах негосударственных организаций может осуществляться по заказу конкретного потребителя информации конфиденциального характера или по инициативе разработчика СКЗИ. При этом в качестве заказчика СКЗИ может выступать любое лицо.

Производство СКЗИ осуществляется в соответствии с техническими условиями, согласованными с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

СКЗИ изготавливаются в полном соответствии с конструкцией и технологией изготовления опытных образцов СКЗИ, прошедших испытания на функционирование опытного образца СКЗИ в штатных режимах и имеющих положительное заключение экспертизы тематических исследований СКЗИ.

СКЗИ реализуются (распространяются) вместе с правилами пользования ими, согласованными с ФСБ России.

Реализация (распространение) СКЗИ и (или) РКД на них осуществляется юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами.

Приобретение РКД на СКЗИ (включая тиражирование программных СКЗИ) осуществляют юридические лица, являющиеся разработчиками и (или) изготовителями СКЗИ.

СКЗИ эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России.

СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров поэкземплярного учета СКЗИ и их опытных образцов определяет ФСБ России.

Организация поэкземплярного учета опытных образцов СКЗИ возлагается на разработчика СКЗИ.

Организация поэкземплярного учета изготовленных СКЗИ возлагается на изготовителя СКЗИ.

Организация поэкземплярного учета используемых СКЗИ возлагается на заказчика СКЗИ.

Организация централизованного (количественного) поэкземплярного учета опытных образцов СКЗИ, а также изготовленных и используемых СКЗИ осуществляется ФСБ России.

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, а также условий производства ключевых документов, осуществляется в соответствии с требованиями Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)».

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

– обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;

– собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;

ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

Контроль за соблюдением условий производства ключевых документов, указанных в технической, конструкторско-технологической и эксплуатационной документации к внешней системе изготовления ключей, осуществляется изготовителем ключевых документов, а также ФСБ России в рамках контроля за организацией и функционированием крипто-

графической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

С целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, обладатель, пользователь (потребитель) данной информации, установивший режим ее защиты с применением СКЗИ, а также собственник (владелец) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ, вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

1.10. Электронная цифровая подпись (ЭЦП)

Согласно Гражданскому Кодексу РФ: «Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон».

Единственной основой для регулирования порядка применения аналогов собственноручной подписи (АСП) является Гражданский Кодекс РФ, содержащий отсылочные нормы, либо к действующему закону, регулирующему порядок применения АСП, либо к договору сторон.

Регулирование порядка применения одного из видов АСП – ЭЦП осуществляется законом «Об электронной цифровой подписи». Необходимо отметить, что принятый закон «Об электронной подписи» частично изменяет понятия (в части ЭЦП), однако основные положения практически остались неизменными. Поэтому в настоящем пособии будем ориентироваться на действующий закон.

Регулирование порядка применения иных АСП, в том числе цифровой подписи – ЦП остается предметом договорного права, что непосредственно следует из текста ГК и закона об ЭЦП.

Большинство технологии цифровой подписи (ЦП) не являются технологией, регулирование которой предусмотрено законом об ЭЦП.

Согласно закону «Об ЭЦП»:

– электронный документ – документ, в котором информация представлена в электронно-цифровой форме;

– электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой

подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

– владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

– средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

– сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

– закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

– открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

– сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

– подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности элек-

тронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

– пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

– информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

– корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

– сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

– подтверждена подлинность электронной цифровой подписи в электронном документе;

– электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Создание ключей электронных цифровых подписей осуществляется для использования в:

– информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;

– корпоративной информационной системе в порядке, установленном в этой системе.

При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и

распространителей этих средств в соответствии с законодательством Российской Федерации.

Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.

Сертификат ключа подписи должен содержать следующие сведения:

– уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

– фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;

– открытый ключ электронной цифровой подписи;

– наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;

– наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

– сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр

должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Удостоверяющий центр:

– изготавливает сертификаты ключей подписей;

– создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

– приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;

– ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;

– проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;

– выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

– осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;

– может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

– вносить сертификат ключа подписи в реестр сертификатов ключей подписей;

– обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;

– приостанавливать действие сертификата ключа подписи по обращению его владельца;

– уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным

образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

– иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Владелец сертификата ключа подписи обязан:

– не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

– хранить в тайне закрытый ключ электронной цифровой подписи;

– немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

– по истечении срока его действия;

– при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

– в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

– по заявлению в письменной форме владельца сертификата ключа подписи;

– в иных установленных нормативными правовыми актами или соглашением сторон случаях.

Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

1.11. Юридическая ответственность за нарушение норм защиты информации

Ответственность, возлагаемая в случаях правонарушений в информационной сфере, формулируется в различных нормативных правовых актах. Конкретные нормы, устанавливающие ответственность за нарушения сосредоточены в основном в Уголовном Кодексе РФ и Кодексе об административных правонарушениях (КоАП).

Например, санкции за нарушение информационных правоотношений в УК РФ:

Ст. 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации –

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, –

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Ст. 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан –

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок от одного года до четырех лет.

3. Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, –

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Ст. 140. Отказ в предоставлении гражданину информации

Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление

гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, –

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет.

Ст. 146. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от трех до шести месяцев.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, –

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

– группой лиц по предварительному сговору или организованной группой;

– в особо крупном размере;

– лицом с использованием своего служебного положения, –

наказываются лишением свободы на срок до шести лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.

Примечание. Деяния, предусмотренные настоящей статьей, признаются совершенными в крупном размере, если стоимость экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав превышают пятьдесят тысяч рублей, а в особо крупном размере – двести пятьдесят тысяч рублей.

Ст. 147. Нарушение изобретательских и патентных прав

1. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до

официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб, –

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой, –

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

Ст. 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом –

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, –

наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, –

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, –

наказываются лишением свободы на срок до десяти лет.

Ст. 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей

1. Сокрытие или искажение информации о событиях, фактах или явлениях, создающих опасность для жизни или здоровья людей либо для окружающей среды, совершенные лицом, обязанным обеспечивать население и органы, уполномоченные на принятие мер по устранению такой опасности, указанной информацией, –

наказываются штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. Те же деяния, если они совершены лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, а равно главой органа местного самоуправления либо если в результате таких деяний причинен вред здоровью человека или наступили иные тяжкие последствия, –

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Глава 28. Преступления в сфере компьютерной информации (ст. 272, 273, 274)

Ст. 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), 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 до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное 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 ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными ра-

ботами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Ст. 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 до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, –

наказываются лишением свободы на срок от трех до семи лет.

Ст. 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе 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 до пяти лет, либо обязательными работами 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.

Ст. 275. Государственная измена

Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином Российской Федерации, –

наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет.

Ст. 276. Шпионаж

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Феде-

рации, если эти деяния совершены иностранным гражданином или лицом без гражданства, –

наказываются лишением свободы на срок от десяти до двадцати лет.

Ст. 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.

Ст. 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.

Например, санкции за нарушение информационных правоотношений в КоАП:

Глава 13. Административные правонарушения в области связи и информации

Ст. 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) –

влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

Ст. 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 трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

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 пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц – от десяти тысяч до двадцати тысяч рублей 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 двух тысяч до трех тысяч рублей; на юридических лиц – от пятнадцати тысяч до двадцати тысяч рублей.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, –

влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц – от двадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), –

влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от одной тысячи до одной тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц – от одной тысячи до одной тысячи пяти-

сот рублей; на юридических лиц – от десяти тысяч до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

Примечание. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности

Ст. 13.13. Незаконная деятельность в области защиты 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 пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц – от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц – от десяти тысяч до двадцати тысяч рублей 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 защиты 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 четырех тысяч до пяти тысяч рублей; на юридических лиц – от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Ст. 13.14. Разглашение информации с ограниченным доступом.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных ч. 1 ст. 14.33 настоящего Кодекса, –

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от четырех тысяч до пяти тысяч рублей.

Ст. 13.15. Злоупотребление свободой массовой информации.

1. Изготовление и (или) распространение теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также относящих-

ся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки информационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье, –

влечет наложение административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей с конфискацией предмета административного правонарушения; на должностных лиц – от четырех тысяч до пяти тысяч рублей с конфискацией предмета административного правонарушения; на юридических лиц – от сорока тысяч до пятидесяти тысяч рублей с конфискацией предмета административного правонарушения.

2. Распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года N 114-ФЗ «О противодействии экстремистской деятельности», без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена, –

влечет наложение административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей с конфискацией предмета административного правонарушения; на должностных лиц – от четырех тысяч до пяти тысяч рублей с конфискацией предмета административного правонарушения; на юридических лиц – от сорока тысяч до пятидесяти тысяч рублей с конфискацией предмета административного правонарушения.

Ст. 13.16. Воспрепятствование распространению продукции средства массовой информации.

Воспрепятствование осуществляемому на законном основании распространению продукции средства массовой информации либо установление незаконных ограничений на розничную продажу тиража периодического печатного издания –

влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

Ст. 13.17. Нарушение правил распространения обязательных сообщений.

Нарушение правил распространения обязательных сообщений –

влечет наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей.

Ст. 14.10. Незаконное использование товарного знака.

Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров –

влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч рублей с конфискацией предметов, содержащих незаконное воспроизведение товарного знака, знака обслуживания, наименования места происхождения товара; на должностных лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией предметов, содержащих незаконное воспроизведение товарного знака, знака обслуживания, наименования места происхождения товара; на юридических лиц – от тридцати тысяч до сорока тысяч рублей с конфискацией предметов, содержащих незаконное воспроизведение товарного знака, знака обслуживания, наименования места происхождения товара.

Список литературы

1. «О безопасности» от 05.03.1992 №2446-1.

2. «Доктрина информационной безопасности Российской Федерации» от 9 сентября 2000 г. № Пр-1895.

3. «О государственной тайне» от 21.07.1993 года № 5485-1.

4. «Об утверждении перечня сведений, отнесенных к государственной тайне». Указ Президента РФ от 30.11.95 №.

5. «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.

6. «О персональных данных» от 27.07.2006 № 152-ФЗ.

7. «Об электронной цифровой подписи». Федеральный закон от 10.01.2002 №1-ФЗ.

8. «Об электронной подписи». Федеральный закон от 06.04.2011 № 63-ФЗ.

9. «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)». Приказ ФСБ РФ от 09.02.2005 №66.

10. «О лицензировании отдельных видов деятельности» от 08.08.01 № 128-ФЗ.

11. «Об организации лицензирования отдельных видов деятельности». Постановление Правительства РФ от 26.01.2006 №45.

12. «Об утверждении формы документа, подтверждающего наличие лицензии». Постановление Правительства Российской Федерации от 11 апреля 2006 г. №208.

13. «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами». Постановление Правительства РФ от 29.12.2007 №957 (вместе с:

«Положением о лицензировании деятельности по распространению шифровальных (криптографических) средств»;

«Положением о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств»;

«Положением о лицензировании предоставления услуг в области шифрования информации»;

«Положением о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем»).

14. «О лицензировании деятельности по технической защите конфиденциальной информации». Постановление Правительства РФ от 15.08.2006 №504.

15. «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации». Постановление Правительства РФ от 31.08.2006 №532.

16. «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны». Постановление Правительства РФ от 15.04.1995 №333.

17. «Об утверждении положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность». Постановление Правительства РФ от 15.07.2002 №526 (в ред. Постановлений Правительства РФ от 14.06.2005 №376, от 26.01.2007 №50).

18. «Об утверждении положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». Постановление Правительства РФ от 22.10.2007 №689.

19. «О техническом регулировании» Федеральный закон от 27.12.2002 №184-ФЗ.

20. «Об утверждении правил по проведению сертификации в Российской Федерации». Постановление Госстандарта РФ от 10.05.2000 №26 (в ред. Изменения №1, утв. Постановлением Госстандарта РФ от 05.07.2002 №57).

21. «Об утверждении «Порядка проведения сертификации продукции в Российской Федерации». Постановление Госстандарта РФ от 21.09.1994 №15.

22. «О сертификации средств защиты информации». Постановление Правительства РФ от 26.06.1995 №608 (в ред. Постановлений Правительства РФ от 23.04.1996 №509, от 29.03.1999 №342, от 17.12.2004 №808).

23. «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия». Приказ ФСБ РФ от 13.11.1999 №564.

24. «Об особенности стандартизации оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, поставляемой вне оборонного заказа, а также процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения указанной продукции.». Постановление Правительства Российской Федерации от 17.10.2009 г. №822.

25. «О связи». Федеральный закон от 07.07.2003 №126-ФЗ.

26. «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ.

27. «Уголовный кодекс Российской Федерации» от 13.06.1996 №63-ФЗ.

28. «Кодекс Российской Федерации об административных правонарушениях» от 13.12.2001 №195-ФЗ.

2. ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Введение

В российских стандартах, связанных с защитой информации, введён ряд определений. Эти определения позволяют понять «что» и «как» нужно защищать. Чаще всего информационную безопасность рассматривают как состояние защищённости информации, при котором обеспечены её *конфиденциальность*, *доступность* и *целостность*. При этом под объектом защиты информации подразумевается *информация* или *носитель информации*, или *информационный процесс*, которые необходимо защищать. Определения каждого из объектов защиты приведены ниже.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационный процесс – процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Так как носителем информации может быть не только бумажный, но и электронный документ, то и сами информационные процессы будут осуществляться автоматизированно. Безопасность информации (при применении информационных технологий) – состояние защищённости информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность *автоматизированной информационной системы*, в которой она реализована.

Таким образом, при защите информации необходимо обеспечить конфиденциальность, целостность и доступность не только самой информации, но и её носителей, а также информационных процессов. Это связано с тем, что реализация угрозы носителю или информационному процессу, может привести к реализации угрозы самой информации. Например, уничтожение последней копии документа приведёт к уничтожению самой информации, а неработоспособность файлового сервера приведёт к недоступности данных.

2.2. Функции организационной составляющей системы защиты информации

Для обеспечения информационной безопасности организации необходимо построение системы защиты информации. Система защиты ин-

формации – совокупность *органов и (или) исполнителей*, используемой ими *техники защиты информации*, а также *объектов защиты информации*, организованная и функционирующая *по правилам и нормам*, установленным соответствующими документами в области защиты информации.

Организационное обеспечение информационной безопасности заключается в установлении правил и норм, а также в контроле их исполнения. Организационные меры обеспечения информационной безопасности – меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Функции организационной составляющей системы защиты информации:

– составление и регулярное обновление состава защищаемой информации предприятия, составление перечня защищаемых бумажных, электронных документов; регламентация обновления и ведения перечня защищаемой информации и её носителей;

– создание иерархической системы разграничения доступа персонала к защищаемой информации;

– формирование и организация деятельности службы безопасности и службы конфиденциальной документации, обеспечение деятельности этих служб нормативно-методическими документами по организации и технологии защиты информации;

– определение методов отбора персонала для работ с защищаемой информацией, методов воспитательной работы с персоналом, требований к обучению и инструктированию сотрудников;

– регламентация пропускного режима на территории, в здании и помещениях предприятия, предназначенных для обработки защищаемой информации;

– регламентация работы системы охраны территории, здания, помещений, оборудования, транспорта и персонала предприятия;

– регламентация контроля соблюдения сотрудниками порядка защиты информации;

– регламентация порядка защиты информации при проведении совещаний, заседаний, переговоров, приёме посетителей, работе с представителями рекламных агентств, средств массовой информации;

– регламентация организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны.

– регламентация действий персонала в экстремальных ситуациях;

– определение критериев и регламентация порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации (выявление угроз).

На основе перечисленных функций можно выделить несколько задача, решаемых в рамках организационного обеспечения информационной безопасности:

1. регламентация работы персонала с информацией и её носителями;
2. регламентация действий персонала при осуществлении информационных процессов;
3. регламентация работы с программно-техническими компонентами системы защиты информации;
4. регламентация деятельности по управлению системой защиты информации.

В данном разделе будут кратко описаны документы, позволяющие решать часть регламентационных задач.

2.3. Регламентация работы с информацией и её носителями

Правила работы с информацией и её носителями призваны запретить сотрудникам: разглашать информацию, копировать её на несанкционированные носители, работать с информацией в непредназначенных для этого местах или неразрешённым способом и т.д. Эти правила должны учитывать все типы носителей, используемых сотрудником при работе с информацией: электронные документы; бумажные документы; акустический сигнал.

Основные правила работы с информацией и её носителями включаются в трудовой договор или обязательство о неразглашении конфиденциальной информации. Более подробно правила работы должны быть расписаны в должностной инструкции сотрудника.

Обязательство (подписка, соглашение) о неразглашении конфиденциальной информации представляет собой правовой документ, которым претендент добровольно и письменно даёт согласие на ограничение его прав в отношении использования конфиденциальной информации. Одновременно в обязательстве претендент предупреждается об ответственности за разглашение этой информации. Функции обязательства может выполнять соответствующий раздел трудового договора.

При работе с конфиденциальной информацией сотрудникам запрещается:

– получать доступ к конфиденциальной информации, к которой у сотрудника нет допуска;

– передавать документы, содержащие конфиденциальную информацию другим сотрудникам и сторонним лицам без письменного разрешения руководителя;

– воспроизводить конфиденциальную информацию на неучтённых носителях информации (переписывать в записную книжку; копировать

электронный документ на собственный съёмный диск; фотографировать документы и т.д.);

– работать с документами, содержащими конфиденциальную информацию, за пределами выделенных помещений, а также выносить из здания организации документы без письменного разрешения руководителя;

– использовать конфиденциальную информацию в разговорах за пределами выделенных помещений (в частных беседах, на конференциях, выставках и т.п.);

– передавать информацию по незащищённым каналам связи.

Кроме запрета на распространение конфиденциальной информации, на сотрудника накладываются ограничения, связанные с распространением информации об информационных процессах, объектах защиты и системе защиты. Сотрудникам запрещается:

– разглашать сведения об используемых в организации информационных системах обработки конфиденциальной информации;

– разглашать коды и пароли, используемые сотрудником для доступа в информационные системы или помещения; передавать другим лицам ключи от помещений, сейфов, а также удостоверения и электронные идентификационные устройства (например, смарт-карты);

– разглашать сведения о составе находящихся у сотрудника документов и месте их хранения, а также о системе защиты информации и принципах работы её элементов.

Правила работы с носителями конфиденциальной информации:

– носители конфиденциальной информации необходимо хранить, применяя указанные руководителем средства защиты информации (сейфы, системы криптографической защиты и др.);

– извлекать из места хранения нужно только тот документ, который необходим для работы в данный момент;

– при работе с документом необходимо ограничить визуальный доступ к нему других сотрудников и посторонних лиц (ограничить зону видимости монитора, закрыть жалюзи на окнах; перевернуть документ лицевой стороной вниз в случае появления другого сотрудника и т.п.);

– при временном прекращении работы необходимо заблокировать доступ к носителю информации (убрать в сейф документы; закрыть помещение; заблокировать компьютер и т.п.).

Действия сотрудников по обеспечению безопасности носителей конфиденциальной информации должны быть согласованы со службой безопасности. Сотрудник обязан:

– немедленно предъявлять уполномоченному работнику все числящиеся за ним документы (на всех типах носителей) для проверки их наличия и комплектности;

– вести совместно с уполномоченным работником учёт находящихся у сотрудника конфиденциальных документов;

– ежедневно по окончании рабочего дня проверять наличие документов и сдавать их на хранение в соответствующий отдел службы безопасности;

– сдавать по описи работнику службы КД все материалы по окончании исполнения документа или работы над ним;

– сдавать по описи уполномоченному работнику все числящиеся за сотрудником документы при увольнении, уходе в отпуск, отъезде в командировку;

– немедленно сообщать своему непосредственному начальнику и в службу безопасности об утрате или недостаче документов, обнаружении лишних или неучтённых документов, отдельных листов.

2.4. Регламентация действий при осуществлении информационных процессов

Информационные процессы осуществляются в рамках каких-либо информационных систем. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и средств информатизации.

Таким образом, обеспечение безопасности информационных процессов можно рассматривать как обеспечение безопасности не только информации, но и обработки, передачи (и др. функций) информации, а также физической защиты средств информатизации.

При определении объектов, требующих защиты, необходимо составить Перечень конфиденциальной информации, включающий:

– наименование и тип (персональные данные, коммерческая тайна и т.п.) конфиденциальной информации;

– уровень конфиденциальной информации;

– срок действия ограничений на доступ или условие прекращения ограничений.

Для каждого типа конфиденциальной информации и уровня её конфиденциальности нужно определить особенности обработки информации на всех этапах жизненного цикла документов и информационные системы, участвующие в обработке.

2.4.1. Регламентация работы с объектами защиты

Перечень информационных систем должен включать: название информационной системы; тип и уровень конфиденциальности обрабатываемой информации. Описание самой информационной системы может включать информацию: о наличии выхода в Интернет; о возможных опе-

рациях с информацией; о наличии соединения с другими информационными системами и др.

Для каждой информационной системы необходимо определить круг лиц, работающих с этой системой, и их права доступа к обрабатываемой информации.

Разграничение доступа к информационным системам:

– определение ролей пользователей, работающих с информационной системой (администратор безопасности, администратор системы, оператор и др.);

– сопоставление ролей с должностями или конкретными сотрудниками.

Уровни разграничения доступа:

– классификация к информационным системам в рамках информационного пространства организации (базам данных; ресурсам рабочих станций; сетевым ресурсам; системе электронного документооборота; технологии бумажного документооборота и т.д.);

– классификация в рамках конкретной информационной системы (разграничение прав при доступе к таблицам, ячейкам баз данных; разграничение прав при доступе к аппаратным и файловым ресурсам операционной системы и сети; разграничение прав при доступе к различным приложениям в операционной системе и т.д.).

Положение о разграничении доступа к конкретной информационной системе должно включать:

– группы (роли) пользователей;

– тип доступа к информации.

Для представления текущего состояния разграничения доступа необходима следующая информация:

– ФИО сотрудника;

– группа пользователей, к которой относится сотрудник;

– должность сотрудника;

– подразделение, в котором работает сотрудник.

Каждая информационная система состоит не только из программной части, обеспечивающей автоматизацию функций обработки информации, но и из аппаратной. Поэтому на основании разграничения доступа к информационной системе, реализуется разграничение доступа в помещения, где установлены средства информатизации данной системы. Функциональная конфигурация и территориальное расположение должны быть представлены в документе с описанием информационной системы.

2.4.1. Рекомендации по созданию системы документооборота

Действия персонала должны быть регламентированы на каждом этапе жизненного цикла документа, т.е. должен быть регламентирован документооборот. Кроме того, должны быть сформулированы требования к

местам хранения и обработки документов, а также требования к осуществлению их доставки.

Документооборот как объект защиты – упорядоченная совокупность каналов санкционированного распространения защищаемой документированной информации между сотрудниками, которым разрешена работа с этой информацией.

Характеристики систем, учитываемые при организации документооборота:

– уровень конфиденциальности обрабатываемых данных;

– используемый способ передачи данных (сетевой протокол, шифрованный канал и др.) и его защищённость;

– форматы входных и выходных данных (бумажный документ, текстовый или графический файл и др.);

– формат хранения данных и его защищённость; тип носителя, используемого для хранения данных.

Рекомендации по реализации системы документооборота:

– внедрение автономной технологической системы для работы с конфиденциальными документами, не соприкасающейся с системой обработки открытых документов: системы защищённого электронного документооборота и отдела по работе с конфиденциальной документацией (КД); передача информации между сотрудниками должна проводиться только через эти системы;

– формирование изолированных подпотоков конфиденциальных документов в соответствии с уровнем конфиденциальности перемещаемых документов;

– регламентация перемещения документов с момента возникновения необходимости создания документа и до окончания работы с документом, отправки в другую организацию, передачи в архив, уничтожения;

– регламентация хранения носителей в централизованных хранилищах (архивах, серверах баз данных) и на рабочих местах сотрудников;

– введение персональной ответственности каждого сотрудника за сохранность носителя и конфиденциальность информации;

– разграничение доступа персонала к документам, делам, каталогам обмена, базам данных и в помещения, где хранятся документы;

– введение персональной ответственности должностных лиц за выдачу разрешения на доступ сотрудников к конфиденциальным сведениям и документам;

– регламентация порядка выдачи (возврата) документов, включая контроль их целостности;

– учёт документов и электронных носителей информации;

– периодический контроль наличия документов и электронных носителей информации, а также соблюдения правил работы с ними;

– регламентация копирования и тиражирования документов.

2.4.2. Регламентация работы с документами на разных этапах их жизненного цикла

Этапы жизненного цикла документа:

– создание документа;
– получение документа от сторонних лиц;
– хранение документа;
– выдача документа сотруднику и возврат документа;
– обработка документа (чтение или изменение документа);
– отправка документа сторонним лицам;
– уничтожение документа.

Для каждого этапа в нормативных документах организации должна быть указана следующая информация:

– должности сотрудников, имеющих право на осуществление данного этапа;
– при необходимости – должности сотрудников, санкционирующих выполнение данного этапа;
– формы учёта документов (журнала учёта конфиденциальных документов; журнала приёма/выдачи документов);
– порядок действий при осуществлении этапа.

Основная часть ответственности за бумажный документооборот возлагается на специальный отдел службы безопасности – отдел конфиденциальной документации (КД). В его полномочия входит осуществление всех этапов работы с документами, кроме периода от выдачи документа сотруднику до возврата этого документа.

Порядок создания документов:

– определение уровня конфиденциальности предполагаемого документа;
– учёт носителя будущего документа;
– составление текста;
– учёт подготовленного документа;
– издание документа.

На чистые носители конфиденциальной информации должны быть нанесены специальные реквизиты, позволяющие отличить конфиденциальные документы от общедоступных. Новый конфиденциальный документ может быть создан только с санкции уполномоченного руководителя.

На этапе создания документа используются журнал учёта чистых носителей и журнал учёта конфиденциальных документов. Журнал учёта конфиденциальных документов включает:

– учётный номер документа, гриф его конфиденциальности;

– дата создания документа;
– номер пункта Перечня конфиденциальной информации;
– название документа;
– количество листов документа;
– количество экземпляров документа;
– место постоянного хранения документа;
– отметки о включении документа в дело и об уничтожении документа.

Для организации хранения конфиденциальных документов могут использоваться централизованная или распределённая технологии.

Централизованная технология – хранение информации допускается только в одном хранилище (помещении архива, базе данных):

– при электронном документообороте сотрудник имеет право работать только с удалённой базой данных;
– при бумажном документообороте ознакомление с информацией происходит в специальном помещении хранилища.

Распределённая технология – хранение информации допускается не только в центральном хранилище, но и на рабочих местах сотрудников:

– при электронном документообороте данные могут быть сохранены локально на компьютере сотрудника;
– при бумажном документообороте сотрудник имеет право работать с документами на своём рабочем месте.

Требования к хранилищу конфиденциальных документов:

– хранилище должно опечатываться и сдаваться под сигнализацию;
– документы должны храниться в сейфах или запираемых шкафах;
– наличие комнаты для ознакомления сотрудников с документами с отсутствием возможности несанкционированного визуального ознакомления с информацией;
– отсутствие несанкционированных технических средств съёма информации.

Для распределённого хранения обязательным является наличие у сотрудника постоянного рабочего места. Кроме того, при бумажном документообороте на рабочих местах требуется наличие у сотрудника:

– личного сейфа (металлического шкафа);
– кейса для хранения и переноса конфиденциальных документов;
– номерной личной металлической печати.

При электронном документообороте требуется наличие у сотрудника:

– личного компьютера;
– установленных на компьютер средств шифрования;
– носителя, с записанными на него криптографическими ключами.

Правила передачи конфиденциальных документов сотрудникам:

– передача документов сотрудникам осуществляется работником отдела КД под роспись в журнале выдачи конфиденциальных документов;

– передача конфиденциальных документов осуществляется только сотрудникам, допущенным к данному документу, и только после проверки документа, удостоверяющего личность сотрудника;

– конфиденциальные документы перемещаются между руководителями или между руководителями и исполнителями только через отдел КД.

Обязанности работника службы КД при передаче документов:

– не допустить выдачу документа лицу, не имеющему права доступа к нему;

– в присутствии сотрудника проверить физическую сохранность документа, наличие всех приложений, листов и других частей документа;

– зафиксировать факт передачи документа в учётной форме под роспись сотрудника;

– знакомить сотрудника только с той частью документа, которая ему адресована;

– не разрешать сотрудникам при ознакомлении с документом делать выписки из текста;

– предотвращать любую возможность ознакомления с документом постороннего лица;

– обеспечить учёт документов, находящихся у сотрудников, контроль сохранности этих документов в рабочее и нерабочее время.

Обязанности работника службы КД при возврате документов:

– проверить соответствие документа учётной форме и его комплектность;

– проверить документ на предмет возможной подмены листов или их порчи;

– проставить росписи о возврате в учётной карточке документа и внутренней описи документов, находящихся у сотрудника.

При обмене информацией со сторонними организациями необходимо учитывать как документы, отправляемые в другие организации, так и документы, приходящие в организацию.

Действия при получении документов из другой организации:

– приём, учёт и первичная обработка поступивших пакетов, конвертов и др.;

– учёт поступивших документов, находившихся в пакетах, и формирование базы данных по документам;

– предварительное рассмотрение и распределение поступивших документов.

Действия при отправке документов в другую организацию:

– получение документа от исполнителя или с другого участка службы КД (инвентарного, архивного и др.);

– получение разрешения руководителя подразделения на отправку документа;

– учёт отправляемых документов;

– пакетирование документов;

– отправление пакетов (конвертов) адресату.

Используемые учётные формы: журналы учёта поступивших и отправленных конфиденциальных документов; журнал учёта предоставленных другим организациям конфиденциальных документов.

Для отправки электронных документов в другие организации используется электронная почта. Положение об использовании электронной почты включает следующие разделы:

– право собственности предприятия на все сообщения электронной почты (в том числе на их просмотр уполномоченными лицами без ведома сотрудника);

– ограничение использования ЭП служебными обязанностями (в том числе ограничения, связанные с моральными и правовыми нормами);

– запрет на пересылку конфиденциальной информации организации;

– использование защищённых каналов связи при санкционированной отправке конфиденциальной информации;

– запрет на изменение даты/времени на компьютере.

– виды взысканий за несоблюдение требований.

В нормативном документе, регламентирующем снятие ограничений на доступ к конфиденциальному документу, должна быть приведена следующая информация:

– возможные причины досрочного снятия ограничений на доступ к носителям конфиденциальной информации (решение первого руководителя организации; письменные ходатайства подразделений, в ведении которых находится эта информация, или их правопреемников, окончание срока конфиденциальности и др.). При этом разглашение (опубликование в средствах массовой информации и т.п.) конфиденциальной информации не является основанием для автоматического снятия ограничений на доступ к ней;

– порядок созыва экспертной комиссии и порядок рассмотрения ею вопросов по снятию ограничений на доступ;

– о снятии ограничений на доступ к информации извещаются другие организации, которым эта информация передавалась.

Схема уничтожения конфиденциальных документов:

– получение разрешения уполномоченного лица на уничтожение;

– подготовка документов, дел и носителей информации к уничтожению; систематизация носителей по способу уничтожения;

– оформление акта на уничтожение;

– уничтожение документов в соответствии с актом;

– отметка об уничтожении документа в журнале учёта конфиденциальных документов.

В Акт уничтожения документов каждый уничтожаемый документ включается отдельной строкой с указанием количества экземпляров и листов.

2.5. Регламентация работы с элементами системы защиты информации

2.5.1. Регламентация работы с программно-техническими элементами системы защиты

Все программно-технические средства защиты, используемые в организации, должны быть учтены. Документ, содержащий описание всех средств защиты (Перечень средств защиты), должен включать:

– название, модель или версию;

– сферу применения;

– информацию о лицензии и сертификате;

– информацию о технической документации (перечень документов и место их хранения);

– информацию о сотруднике, ответственном за средство защиты и др.

Для каждого средства защиты должны быть задокументированы эталонные настройки и режимы работы. С заданной периодичностью должен проводиться контроль соответствия текущих настроек эталонным, а также контроль активности средства защиты. При этом должны быть описаны действия в случае аварийных ситуаций – сбоев, нарушении целостности настроек, стихийных бедствиях и др. Должно быть документировано разграничение доступа к настройкам средства защиты и к изменению его состава, а также правила и методы аутентификации.

Для средств защиты, использующих аутентификацию для пропуска на защищаемый объект санкционированных сотрудников, необходимы нормативные документы, описывающие требования к процессу и средствам аутентификации.

Инструкция по организации парольной защиты должна включать:

– требования к стойкости пароля;

– метод формирования новых паролей – самими сотрудниками или централизованно (работниками службы безопасности с дальнейшей передачей сотрудникам);

– требования к передаче и хранению паролей (при централизованном методе);

– действия работников службы безопасности при приёме и увольнении сотрудника (например, при создании новой учётной записи установка временного пароля, который сотрудник должен будет сменить при первом входе в систему);

– условия, приводящие к внеплановой смене пароля (разглашение пароля), и предпринимаемые действия;

– ответственные за контроль соблюдения требований.

Положение о внесении изменений в списки пользователей должно включать:

– список должностных лиц, имеющих право подавать заявки на создание новых учётных записей в каждой автоматизированной информационной системе;

– список должностных лиц, ответственных за создание учётных записей;

– ограничения, накладываемые на присвоение пользователям идентификаторов;

– описание процедуры регистрации и назначения прав пользователя, включая оформление заявки на внесение изменений в списки пользователей (обязательно указывается основание для создания учётной записи, например, трудовой договор).

Для различных средств защиты могут использоваться разные способы аутентификации, проводиться разные действия при вводе аутентификационных данных, поэтому необходимы:

– инструкции по работе с используемыми факторами аутентификации (по парольной защите, работе со смарт-картами и др.);

– инструкции по вводу аутентификационных данных в программное обеспечение (ОС, базы данных, веб-сайты и т.д.).

Изменение состава и настроек рубежа защиты (аппаратуры, программного обеспечения, настроек безопасности и т.д.) регламентируется Инструкцией по модификации автоматизированных систем и рабочих станций. Инструкция включает:

– список должностных лиц, имеющих право подавать заявки на модификацию автоматизированной информационной системы;

– список должностных лиц, ответственных за модификацию;

– перечисление возможных видов модификации;

– описание процедуры подачи заявки на модификацию и её выполнения;

– требования к обязательной предварительной проверке новых компонент, а также к проверке работоспособности системы в целом и средств защиты после модификации системы;

– описание процедуры модификации в случае аварийной ситуации.

Должны быть представлены формы: заявки на модификацию; журнала учёта модификаций; журнала учёта аварийных ситуаций.

Одним из средств контроля целостности средств защиты и системы в целом является антивирусная защита. Инструкция по организации антивирусной защиты должна включать:

– периодичность обновления антивирусной базы;

– периодичность проверки системы на наличие вредоносных программ;

– описание процедуры проверки на вирусы подключаемых к системе съёмных носителей, а также при получении файлов из внешних сетей;

– действия сотрудников при обнаружении вируса;

– действия работников службы безопасности при обнаружении вируса (вплоть до служебного расследования).

Для физической защиты объектов (зданий помещений) необходима регламентация пропускного и внутриобъектового режима.

Пропускной режим – совокупность мероприятий и правил, исключающих возможность несанкционированного проникновения лиц, проезда транспортных средств, проноса (провоза) имущества на территорию и с территорий зданий.

Внутриобъектовый режим – совокупность мероприятий и правил, выполняемых работниками организации, командированными лицами и посетителями, находящимися на охраняемой территории зданий, в соответствии с требованиями служебного распорядка и пожарной безопасности.

Основной документ – Инструкция по пропускному и внутриобъектовому режиму. Инструкция состоит из нескольких разделов, перечисленных ниже.

1. Общие положения.

– Нормативные документы, на основании которых составлялась инструкция.

– Определение пропускного и внутриобъектного режима и основные решаемые задачи.

– Подразделения, на которые возлагается руководство пропускным режимом, практическое его осуществление.

– Санкции к нарушителям пропускного режима.

2. Порядок пропуска лиц в здания.

– Перечисление всех контрольно-пропускных пунктов (КПП) организации и их назначения, их описание, расположение и установление единой нумерации.

– Требования к оборудованию КПП средствами защиты.

– Установление порядка прохода сотрудников и посетителей на территорию объекта и в категорированные подразделения.

– Требования к обеспечению КПП необходимым набором документов (журнал посещений, списки допущенных лиц).

– Определение прав и основных обязанностей контролёров КПП.

3. Виды пропусков, порядок их оформления.

– Виды пропусков, их количество и статус (удостоверения, временные, разовые, на автотранспорт).

– Описание пропусков.

– Порядок оформления и выдачи пропусков.

– Замена и перерегистрация пропусков.

– Мероприятия при утере пропуска сотрудником, увольнения сотрудника и т.п.

– Правила оформления документов на вывоз (вынос) материальных ценностей с территории объекта.

4. Порядок открытия дверей запасных выходов из зданий.

5. Порядок допуска на территорию объекта (с объекта) служебного, личного автотранспорта сотрудников и автотранспорта сторонних организаций.

6. Меры по обеспечению и контролю внутриобъектового режима.

– Действия при установке и снятии помещений с сигнализации.

– Регламентация видеонаблюдения.

– Регламентация противопожарной безопасности.

– Регламентация проведения совещаний и переговоров.

2.5.2. Регламентация работы с персоналом

При регламентации работы персонала основным является составление должностных инструкций. Должностные инструкции позволяют ограничить круг конфиденциальной информации, к которой необходимо предоставить сотруднику доступ. При этом доступ может быть предоставлен и сотрудникам сторонней организации. Кроме того, должностные инструкции позволяют сформулировать требования к сотруднику, принимаемому на конкретную должность. Требования могут касаться как профессиональных навыков работы сотрудника, так и его технических навыков и моральных качеств.

Работа с персоналом состоит из нескольких этапов: приём на работу; определение конфиденциальных документов, к которым сотрудник будет иметь доступ; текущая работа с персоналом, включая осуществление контроля работы сотрудников; регламентация действий сотрудников во время экстремальных ситуаций; увольнение сотрудника.

В ходе приёма на работу сотрудник должен подписать несколько документов: письменное согласие на использование его персональных данных; трудовой договор с разделом, посвящённым работе с конфиденциальной информацией, или обязательство о неразглашении; документ о прохождении первоначального обучения работе с конфиденциальной информацией и средствами защиты.

Согласие на использование персональных данных может применяться не только при приёме на работу, но и при работе с клиентами или партнёрами. Информация, содержащаяся в письменном согласии:

– фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва;

– для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется.

При приёме на работу в определённой должности сотрудник получает доступ к разрешённым для этой должности конфиденциальным документам. Список разрешённых к ознакомлению документов может изменяться. Таким образом, предоставление доступа сотруднику к конфиденциальным документам происходит:

– при вступлении в должность, предусматривающую ознакомление с конфиденциальной информацией (основание – приказ о при приёме на работу или переводе на другую должность);

– при необходимости ознакомления с дополнительными документами в рамках служебных обязанностей (основание – приказ о допуске к конфиденциальной информации с резолюцией уполномоченного лица).

При необходимости предоставления доступа к конфиденциальным документам других организаций необходимо заключение Соглашения по неразглашению переданной информации. Соглашение по неразглашению переданной информации должна включать следующее:

– раскрытие конфиденциальной информации организации партнёрам или клиентам возможно только в объёме, необходимом для реализа-

ции задач организации, а также при условии принятия ими на себя обязательств по неразглашению и исключению неправомерного использования полученных сведений (принимать решение о передаче может только руководитель организации);

– конфиденциальная информация партнёров или клиентов, переданная организации, и в отношении которой взято обязательство о неразглашении, подлежит защите наравне с конфиденциальной информацией самой организации.

Регламентация текущей работы с персоналом включает в себя определение:

– периодичности и порядка обучения и систематического инструктирования сотрудников по вопросам защиты информации;

– порядка проведения регулярной воспитательной работы с персоналом, работающим с конфиденциальной информацией и документами;

– периодичности и порядка контроля выполнения сотрудниками требований по защите конфиденциальной информации;

– действий по контролю степени осведомлённости сотрудников в области конфиденциальных работ организации;

– процедуры проведения служебных расследований по фактам утечки информации и нарушений персоналом требований по защите информации.

Контроль действий пользователя при работе с информацией, а также при изменении состава средств защиты и их настройке. Нормативная основа – Регламент контроля использования технических средств обработки и передачи информации включает:

– список должностных лиц, осуществляющих контроль;

– перечень технических средств, которые могут подвергаться контролю;

– возможные режимы контроля – автоматический и ручной; причины перехода от автоматического к ручному режиму;

– информацию, фиксируемую при осуществлении контроля в автоматическом режиме;

– описание действий сотрудника, которые могут быть заблокированы средствами автоматического контроля, в случае нарушения каких-либо правил;

– периодичность проверки журналов автоматического контроля работниками службы безопасности;

– действия сотрудников службы безопасности в случае выявления несанкционированных действий сотрудника.

Контроль выполнения регламентов работы с документами поводится на основе сравнения текущего состава и состояния конфиденциальных

документов с составом, указанным в учётных формах. Таким образом, целью проверки наличия документов, дел и носителей конфиденциальной информации является установление реального соответствия документов записям в учётных формах, сохранности, целостности и комплектности. Подобные проверки позволяют своевременно выявлять факты утраты конфиденциальных документов и контролировать правильность выполнения процедур и операций по их учёту, хранению и использованию.

Виды проверок:

– регламентированные, обязательные проверки наличия документов, дел и носителей информации (ежедневно, ежеквартально и по окончании календарного года);

– нерегламентированные проверки (при смене руководителей подразделений или направлений деятельности фирмы, увольнении сотрудников, после завершения экстремальной ситуации, при выявлении факта возможной утраты информации и в других случаях).

Схема проверки наличия документов:

– определение набора сверяемых документов (выданные конкретному сотруднику; по определённому направлению; все конфиденциальные документы);

– проверка в отделе КД;

– проверка на рабочих местах исполнителей;

– оформление и анализ результатов проверки.

По результатам проверки составляется Акт проверки наличия и состояния документов и дел. Нарушения, отмечаемые в Акте:

– отсутствие конфиденциального документа, дела или носителя информации у сотрудника (или в отделе КД), которому они были выданы;

– обнаружение в базе данных компьютера сотрудника (в службе КД) или на съёмном носителе неучтённой или несанкционированно сохранённой копии электронного документа.

Регламентация действий сотрудников в экстремальных ситуациях заключается в составлении аварийного плана. Структура аварийного плана:

– определение аварийных ситуаций;

– классификация объектов по приоритетам реагирования и восстановления;

– предварительные меры для каждого объекта (резервирование или обеспечение отказоустойчивости объектов; составление алгоритма быстрой замены объекта; распределение обязанностей по оперативной и восстановительной деятельности и оповещение о них сотрудников; составление инструкций для сотрудников);

– информация о сотруднике, ответственном за действия во время аварийной ситуации (ФИО; должность; номер телефона);

– мероприятия для каждого объекта, проводимые во время аварии (идентификация типа события; информирование ответственных лиц; проверка готовности к выполнению);

– мероприятия для каждого объекта, проводимые при возвращении к производственной деятельности – восстановление работоспособности объектов в порядке приоритетности.

Порядок действий при увольнении сотрудника:

– написание сотрудником заявления об увольнении с подробным раскрытием причины и, желательно, указанием места предполагаемой работы (уведомление службы безопасности является обязательным);

– приём отделом КД от увольняющегося сотрудника всех числящихся за ним документов, баз данных, носителей информации, материалов, с которыми он работал, проверка их комплектности;

– сдача сотрудником пропуска, средств аутентификации, всех ключей и печатей. При наличии кодового замка, использовавшегося сотрудником, – изменение кода;

– проведение работником службы безопасности беседы с сотрудником с целью напоминания ему об обязательстве о неразглашении конфиденциальной информации, об ответственности за разглашение.

3. БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

3.1. Введение

При работе с вычислительными системами операционные системы являются основным связующим звеном между пользователями и ресурсами. Именно операционная система организует доступ к хранящимся данным, предоставляет пользователю устройства ввода-вывода для управления данными. Как следствие, основным рубежом защиты при локальной работе с данными пользователя становится операционная система.

Задачи операционных систем в рамках информационной безопасности:

- обеспечение конфиденциальности обрабатываемых данных;
- обеспечение целостности обрабатываемых данных;
- подотчётность ресурсов системы.

К задачам, прежде всего, относятся те, которые обеспечивают безопасность информации во время работы пользователя с системой. Во время хранения или передачи данных механизмы защиты операционной системы не могут применяться, т.к. сама система отключена или данные выходят за её пределы. В таких случаях необходимо применение других методов защиты, например, криптографических.

Механизмы, отвечающие за безопасность данных, реализованы на различных уровнях операционной системы. На самом низком уровне, частично реализованном аппаратно: выполнение кода в разных режимах работы процессора (пользовательском и привилегированном), поддержка RAID-массивов, защита ячеек оперативной памяти, включая предотвращение выполнения данных. На более высоком уровне – защита виртуального адресного пространства процессов от вмешательства других процессов и др. Все эти механизмы работают прозрачно для пользователя, т.к. управление ими берёт на себя операционная система. В этом разделе будут рассматриваться только прикладные механизмы безопасности операционных систем, в управлении которыми необходимо участие человека.

3.2. Ресурсы операционной системы

В начале рассмотрения методов обеспечения безопасности операционных систем необходимо определить защищаемые объекты и тех, от кого их нужно защищать. Субъектом доступа в операционных системах принято считать пользователя или процесс, выполняемый от его имени.

Если говорить об обеспечении конфиденциальности и целостности информации, то надо учитывать объекты, к которым субъект может осуществить доступ. Это файлы, устройства и порты ввода-вывода.

В качестве защищаемых объектов будут рассматриваться только локальные ресурсы. Общая классификация защищаемых объектов представлена на рис. 3.1.

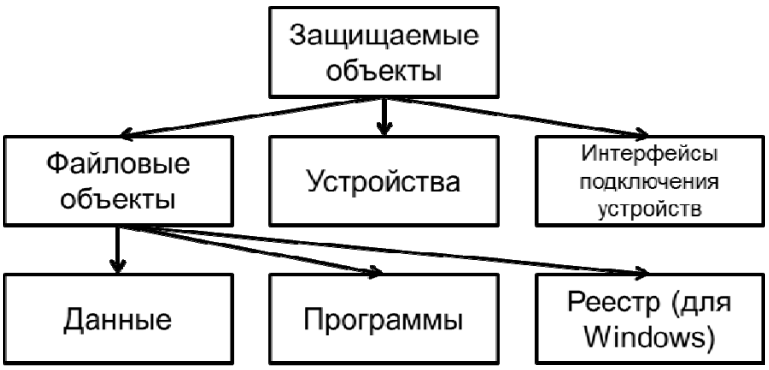


Рис. 3.1. Классификация защищаемых объектов

Файловые объекты подразделяются на:

– файлы с данными (файлы и каталоги);

– исполняемые файлы (программы);

– файлы с настройками операционной системы (для семейства Windows NT – реестр).

Реестр в данном случае рассматривается не как совокупность файлов на диске, а как хранилище настроек, обладающее иерархической структурой каталогов.

Под интерфейсами подключения устройств подразумеваются порты ввода-вывода – USB-порт, LTP-порт и др.

Устройства можно классифицировать на:

– жёсткие диски;

– устройства с отчуждаемыми носителями информации (CD-, DVD-привод, кардридер и др.);

– съёмные носители информации (USB-накопители, CD-, DVD-диски и др.);

– остальные устройства ввода-вывода (принтеры, WiFi-адаптеры и др.).

3.3. Методы обеспечения информационной безопасности в операционных системах

В России существуют документы, описывающие требования к механизмам защиты, которые могут быть реализованы в операционных системах. На основе этих документов проводится сертификация программных продуктов. Документы, содержащие требования, применимые к операционным системам:

– Руководящий документ Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации.

Показатели защищенности от несанкционированного доступа к информации» от 30 марта 1992 г..

– Руководящий документ Гостехкомиссии «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» от 19.06.2002.

В указанных документах выделены следующие группы требований к механизмам обеспечения безопасности операционных систем:

– идентификация и аутентификация;
– управление доступом;
– аудит безопасности.

Идентификация – это процедура распознавания субъекта по его уникальному в данной системе идентификатору. В процессе регистрации субъект предъявляет свой идентификатор системе, и она проверяет его наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные субъекты относятся к нелегальным.

Аутентификация – процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Субъект должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.).

Авторизация – процедура предоставления субъекту определённых прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.

Управление доступом – функции, ограничивающие доступ к информации или средствам обработки информации только авторизованным лицам или приложениям.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Журнал аудита – запись в хронологическом порядке действий системы, содержащая достаточно сведений для того, чтобы реконструировать, проанализировать и проверить последовательность сред и действий, окружающих каждое событие или ведущих к каждому событию по ходу операции от её начала до выдачи окончательных результатов.

3.4. Аутентификация в операционных системах

3.4.1. Функциональное назначение аутентификации

Основная цель этапа аутентификации заключается в предоставлении доступа к работе с операционной системой, программным обеспечением,

оборудованием, данными только санкционированным на эти действия пользователям.

При этом аутентификация может происходить не только с целью получения доступа к операционной системе и её ресурсам для работы с ними, но и для настройки параметров, влияющих на безопасность. Возможность изменения настроек, связанных с безопасностью, должна предоставляться только выделенным пользователям – администраторам. У прикладных пользователей права по отношению к системе должны быть ограничены.

Необходимость прохождения аутентификации может возникнуть на разных этапах работы пользователя с операционной системой. Эти этапы – загрузка системы, функционирование (работа с ресурсами) и возврат к функционированию в случае блокировки.

Функциональное назначение аутентификации при работе прикладных пользователей схематично представлено на рис. 3.2.

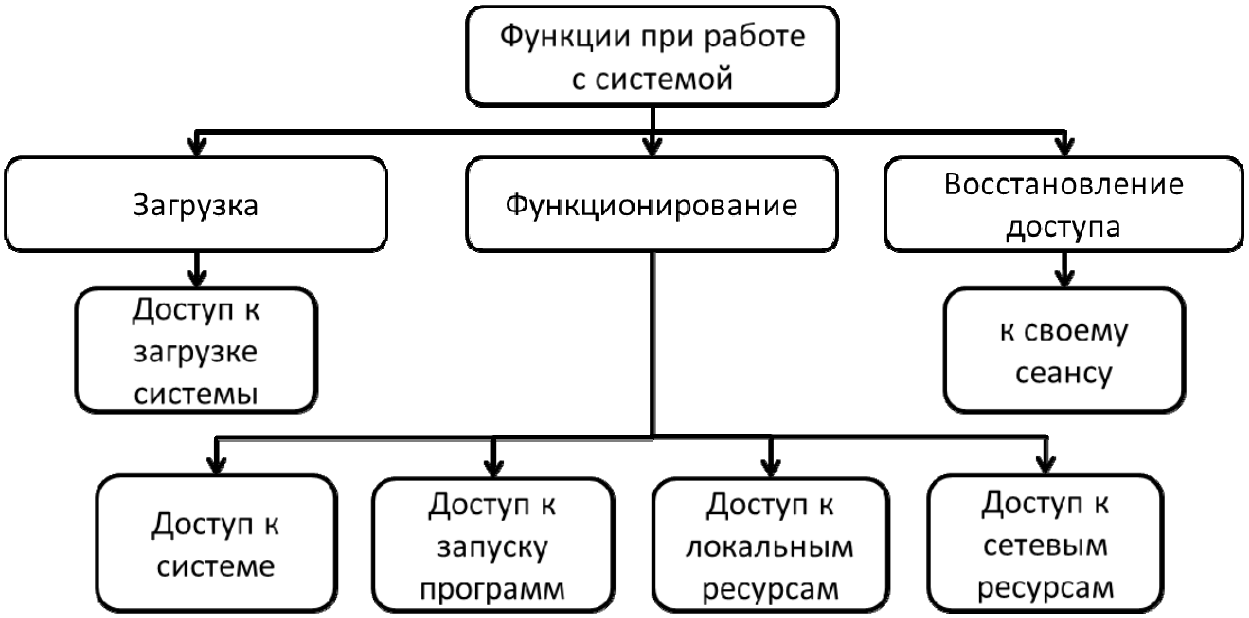


Рис. 3.2. Функции аутентификации по контролю доступа при работе с операционной системой

На этапе загрузки аутентификация может потребоваться во время начальной инициализации аппаратного обеспечения, осуществляемой базовой системой ввода-вывода (BIOS). Кроме BIOS, аналогичные функции предоставляют дополнительные средства защиты – аппаратные модули доверенной загрузки (например, Аккорд-АМДЗ, Криптон-Замок).

Во время функционирования операционной системы аутентификация может использоваться:

- для входа в систему с правами указанной учётной записи;
- для запуска программного обеспечения;
- для получения доступа к локальным и сетевым ресурсам.

При запуске программ или обращении к ресурсам операционная система осуществляет прозрачную аутентификацию, используя данные, предоставленные пользователем при входе в систему. Возможна и другая ситуация, когда необходимых для аутентификации данных в операционной системе нет. Например, когда запускаемое программное обеспечение поддерживает собственную базу учётных записей (системы электронного документооборота, системы управления базами данных и др.). В этом случае пользователь должен использовать аутентификатор, отличный от используемого для входа в операционную систему. Это относится и к файлам, зашифрованным при помощи дополнительного программного обеспечения, и к сетевым ресурсам, расположенным в другом домене, и т.п.

Одно из требований к операционным системам предусматривает наличие возможности блокирования интерактивного сеанса: в случае длительного бездействия пользователя; по инициативе самого пользователя. Тогда для восстановления собственного сеанса пользователю необходимо будет пройти процедуру аутентификации.

Кроме случаев, когда с процедурой аутентификации сталкивается прикладной пользователь, необходимо рассмотреть функции по контролю доступа к параметрам системы. Фактически, эти функции сводятся к использованию аутентификации при настройке этапов работы операционной системы – загрузки, функционирования (рис. 3.3).

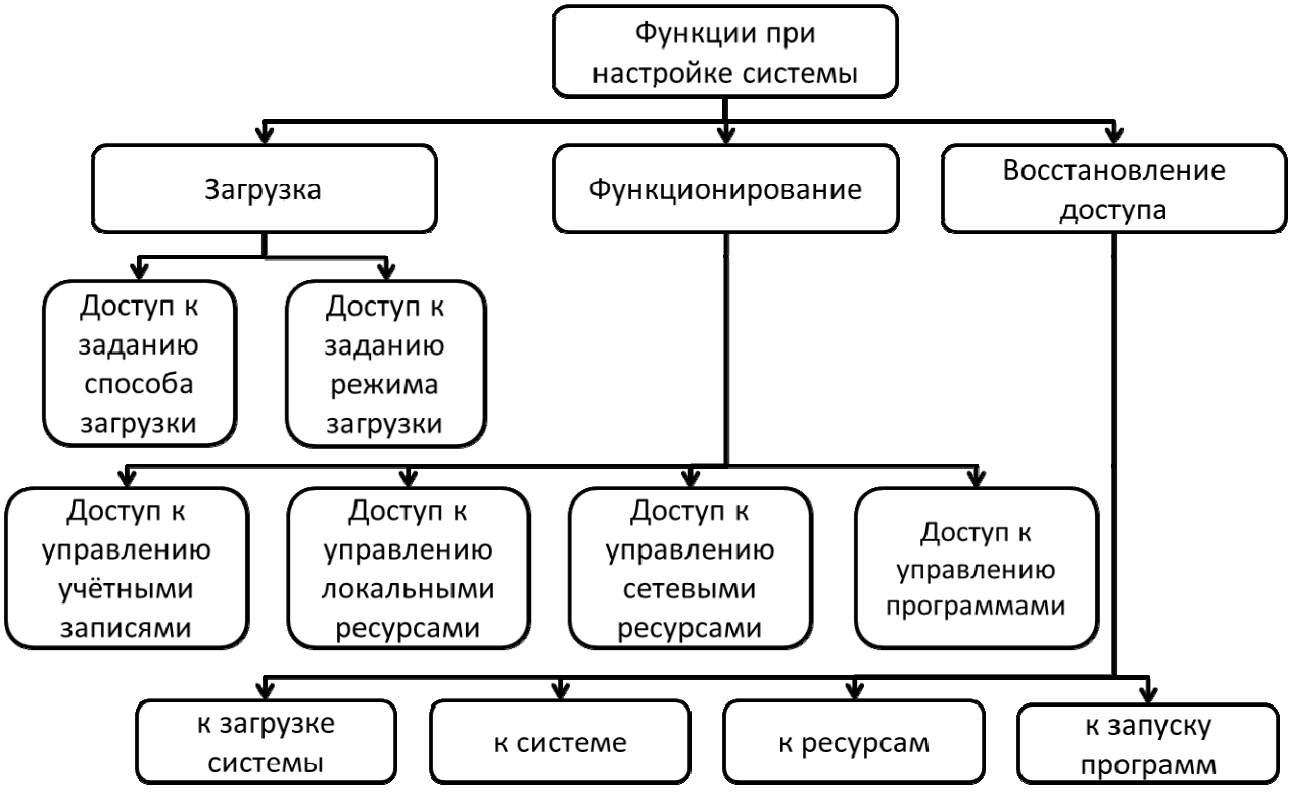


Рис. 3.3. Функции аутентификации по контролю доступа при настройке операционной системы

Настройка загрузки включает аутентификацию:

– при задании способа загрузки – с какого носителя должна загружаться система, нужна ли аутентификации при загрузке системы;

– при задании режима загрузки (например, при загрузке в безопасном режиме).

Аутентификация с правами администратора также должна применяться для получения доступа к управлению учётными записями пользователей (добавление, удаление, блокировка и т.п.) и настройкам разграничения доступа к ресурсам.

Для затруднения действий злоумышленника по подбору аутентификатора в операционных системах используется блокировка учётной записи пользователя при заданном количестве неуспешных попыток аутентификации. При достижении заданного значения неуспешных попыток система блокирует учётную запись или место входа (например, рабочую станцию). Восстановить доступ к системе может только уполномоченный пользователь, с правами которого необходимо аутентифицироваться.

Ещё одна процедура, для которой необходимо наличие аутентификатора – изменение аутентификационных данных. В операционных системах каждый пользователь должен иметь возможность изменять свои данные, а данные других пользователей – уполномоченный администратор. При этом администратор может только изменять аутентификационные данные, но не может их просматривать.

3.4.2. Методы аутентификации

Операционные системы поддерживают различные методы аутентификации, но в требованиях по защите информации всё чаще указывается на необходимость внедрения двухфакторной аутентификации. Под двухфакторной (многофакторной) аутентификацией подразумевают аутентификацию, в процессе которой используется два (несколько) различных типов аутентификационных факторов.

Фактор аутентификации – определённый вид информации, предъявляемый субъектом системе при его аутентификации.

Факторы аутентификации:

– что-либо, известное пользователю;

– что-либо, имеющееся у пользователя;

– что-либо, чем является сам пользователь.

Метод аутентификации – специфика использования определенного типа аутентификационных факторов в процедуре аутентификации.

Примеры методов аутентификации при использовании различных факторов приведены в табл. 3.1.

Таблица 3.1

Методы аутентификации

Фактор	Методы
Что-либо, известное пользователю	Использование пароля, ключевой фразы и т. д.
Что-либо, имеющееся у пользователя	Использование смарт-карт, токенов, дискет и т.д.
Что-либо, чем является сам пользователь	Использование биометрических характеристик

Таким образом, примерами двухфакторной аутентификации будут являться:

– отпечаток пальца и пароль;

– карта с магнитной полосой и PIN-код и т.д.

3.4.3. Аутентификация на основе паролей

Наиболее простой в реализации и поэтому широко используемой является аутентификация на основе пароля, который пользователь запоминает и предъявляет системе вместе со своим идентификатором. Модуль, ответственный за аутентификацию:

– ищет в базе данных паролей запись, соответствующую введённому идентификатору;

– сравнивает предоставленный пользователем пароль с паролем, хранящимся в найденной записи;

– при совпадении – предоставляет пользователю доступ.

Если введённый идентификатор не обнаружен в базе, то в доступе отказывается. Схема аутентификации с использованием пароля представлена на рис. 3.4.

- Секретная последовательность символов, известная пользователю.

- Устройство для ввода пароля (клавиатура, сенсорный экран и пр.).

- Программный модуль для ввода пароля и сравнения его с хранящимся в базе значением.

- Запись в базе включает в себя пару (*ID*, *K*), где *ID* – идентификатор пользователя; *K* – пароль пользователя.

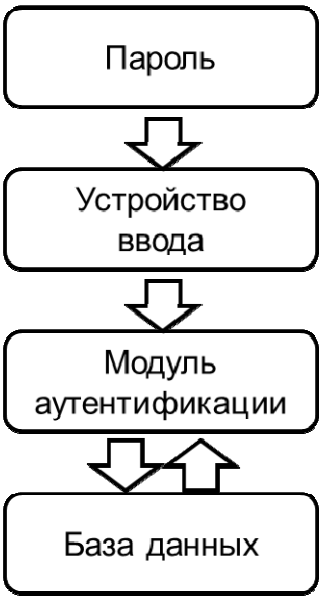


Рис. 3.4. Схема аутентификации с использованием пароля

В современных системах пароли хранятся в хэшированном виде, т.е. по хранящемуся значению сложно вычислить исходный пароль. Таким образом, модуль аутентификации хэширует введённые данные и сравнивает полученный хэш с хранящимся в базе.

Из-за того, что пароль позволяет получить доступ к защищаемой системе, он является основным объектам атак злоумышленников. Угрозы, возникающие по отношению к паролям, можно разделить на несколько групп.

Первая группа включает в себя угрозы от злоумышленников, находящихся за пределами контролируемой зоны:

– внедрение в систему вредоносных программ, позволяющих осуществлять атаки на пароль и передавать информацию злоумышленнику;

– анализ сетевого трафика для поиска пакетов с аутентификационной информацией, генерируемых при удалённом входе в систему;

– разглашение пользователем своего пароля по собственной инициативе или вследствие использования злоумышленником методов «социальной инженерии».

«Социальная инженерия» – набор психологических приёмов злоумышленника, направленных на выведывание у пользователей системы их аутентификационных данных.

Во вторую группу входят угрозы, осуществляемые при наличии доступа в помещение, но без доступа к самим операционным системам:

– визуальный съём пароля при вводе;

– хищение хранящегося в легкодоступном месте (под клавиатурой, в незапертых ящиках стола) материального носителя с записанным паролем;

– копирование базы с паролями за счёт загрузки под другой операционной системой.

Во время работы операционной системы запрещён любой доступ пользователя к файлу, в котором хранится база паролей. Но при наличии возможности изменения способа загрузки (в BIOS) злоумышленник может загрузить другую операционную систему с собственного носителя и свободно скопировать файл с базой или заменить его на собственный.

Третья группа – угрозы, реализуемые при наличии доступа в операционную систему. Эти угрозы направлены на получение злоумышленником прав администратора системы:

– внедрение вредоносных программ (эксплойты), позволяющих повысить права сеанса за счёт ошибок в операционной системе;

– внедрение в систему вредоносных программ (снифферы клавиатуры), перехватывающих все нажатия клавиш клавиатуры и передающих эти данные злоумышленнику.

Четвёртая группа – это угрозы, связанные с наличием у злоумышленника базы паролей. Так как в современных операционных системах пароли не хранятся в открытом виде, то угрозы следующие:

– взлом алгоритма шифрования паролей;

– подбор паролей.

При использовании хэширования базы паролей основным методом является подбор пароля, т.к. алгоритм уже известен, но обратное преобразование (хэша в пароль) практически не осуществимо. Основные методы подбора паролей – полный перебор и атака по словарю. Специальная программа для взлома паролей генерирует предполагаемое значение пароля, хэширует его и сравнивает с хранящимся в базе. Каждое значение пароля генерируется либо случайно, либо берётся из словаря.

Отталкиваясь от этих методов, сформулированы следующие требования к паролям для увеличения их стойкости:

– ограничение на минимальную длину пароля;

– использование при задании пароля нескольких типов символов (цифры, буквы различных регистров, специальные символы);

– запрет задания простых паролей, состоящих из значимых слов (имени, логина и др.) или дат;

– ограничение срока действия пароля (должен быть меньше ориентировочного времени подбора пароля заданной сложности);

– запрет использования старого пароля при задании нового (ведение истории паролей);

– ограничение на число неверно введённых значений пароля.

Увеличение стойкости пароля, наряду с преимуществами, имеет серьёзный недостаток – пароль становится трудно запоминаемым для пользователя. В итоге пользователь пытается записать где-нибудь пароль, что упрощает задачу злоумышленника.

Усиливает проблему необходимость работы с несколькими программами, требующими аутентификации. Иногда количество паролей, требующих запоминания, переваливает за десяток. В таком случае возможно применение технологии однократного входа (SSO – Single Sign-on), когда пользователь, вводя один пароль, получает доступ ко всем ресурсам.

Данная технология подразумевает наличие дополнительной базы для хранения паролей пользователя ко всем используемым ресурсам. Для доступа к хранимым паролям используется мастер-пароль. Если мастер-пароль введён правильно, то при обращении пользователя к ресурсам аутентификация проходит автоматически.

Преимущества технологии SSO:

– пользователю не нужно запоминать несколько паролей, поэтому может быть выбран более стойкий мастер-пароль;

– на аутентификацию пользователь затрачивает меньше времени.

Недостатки технологии SSO:

– необходимо защищать базу для хранения паролей;

– в случае взлома мастер-пароля злоумышленник получает доступ ко всем ресурсам, к которым имеет доступ пользователь.

3.4.4. Аутентификация при помощи физического объекта

Аутентификация при помощи физического объекта основана на предъявлении системе определённого устройства, которое пользователь не может передавать другим лицам.

Примерами подобных устройств являются: USB-ключи (token), пластиковые карты, смарт-карты (пластиковые карты со встроенным процессором), TouchMemory.

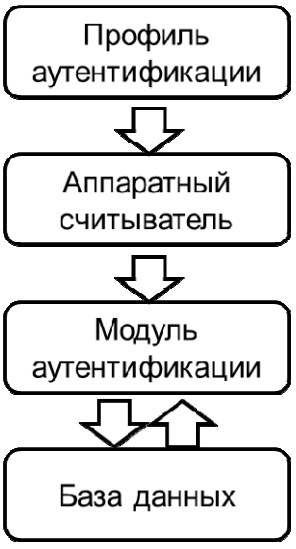
Физические объекты чаще всего используются при двухфакторной аутентификации. Кроме наличия объекта, для доступа к его содержимому необходимо знать пароль. Тогда в случае кражи (утери) устройства злоумышленнику требуется ещё и знание пароля. Фактически, этот пароль будет являться мастер-паролем для доступа ко всей информации, сохранённой на устройстве.

На устройствах может храниться статический код доступа (TouchMemory) или профиль, включающий аутентификационные данные, которые могут быть изменены. Применительно ко входу в операционную систему, профиль содержит имя учётной записи и пароль пользователя, а также название домена или рабочей станции, где существует данная учётная запись. Кроме того, некоторые устройства могут использоваться для хранения сертификатов.

Для увеличения защищённости хранимой на устройстве информации производители используют аппаратное (token) шифрование или шифрование с использованием встроенного в устройство программного обеспечения (смарт-карты).

Любому устройству для связи с системой необходим аппаратный считыватель, который может быть как стандартным – USB-порт, так и специализированным – считыватель для смарт-карт.

Схема аутентификации при использовании физического объекта приведена на рис. 3.5.



- Профиль аутентификации – запись на физическом объекте, в которой хранится информация для входа.
- Аппаратный считыватель – интерфейс между физическим объектом и системой.
- Модуль аутентификации самостоятельно считывает данные из профиля и сравнивает их данными, хранящимися в базе.
- Модуль аутентификации при двухфакторной аутентификации дополнительно делает запрос пароля на доступ к содержимому устройства.

Рис. 3.5. Схема аутентификации при использовании физического объекта

Наличие на устройстве профиля аутентификации приводит к тому, что данные, находящиеся в этом профиле, пользователь запоминать не должен. И даже возможна ситуация, когда пользователь просто не будет знать свой пароль для входа в операционную систему – ему будет достаточно запомнить пароль для получения доступа к содержимому самого устройства. Таким образом, пользователь не сможет разгласить свой пароль для входа в систему или записать его куда-либо. В то же время, пароль на устройство можно сделать достаточно простым (по аналогии с PIN-кодом к пластиковым или sim-картам).

При реализации технологии SSO с использованием физических объектов удаётся нейтрализовать основные недостатки данной технологии. В таком случае профили аутентификации будут храниться на самом устройстве, а не в базе данных программного обеспечения. Кроме того, если злоумышленник узнает мастер-пароль, то он всё равно не сможет воспользоваться никакими ресурсами, т.к. у него не будет самого устройства.

Преимущества аутентификации при помощи физического объекта:

– возможность использования случайных паролей произвольной длины для аутентификации в операционных системах и программных приложениях;

– отсутствие необходимости запоминания сложных паролей;

– возможность хранения паролей за пределами системы при использовании технологии SSO

Недостатки аутентификации при помощи физического объекта:

– необходимость дополнительных затрат на покупку устройств и аппаратных считывателей;

– необходимость учёта выдачи устройств пользователям;

– возможность утери или выхода из строя устройства.

3.4.5. Биометрическая аутентификация

Биометрическая аутентификация основана на предъявлении системе уникальных характеристик самого человека.

Методы биометрической аутентификации классифицируются на статические (физиологические) и динамические (поведенческие).

Статические методы основываются на физиологической характеристике человека, т.е. уникальной характеристике, данной ему от рождения и неотъемлемой от него. У взрослого человека данные характеристики являются практически неизменными (за исключением травм, порезов и т.п.).

Динамические методы основываются на поведенческой характеристике человека, т.е. построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия. Эти характеристики подвержены сильному влиянию психофизиологического состояния человека – эмоциональное состояние, усталость и т.д.

Примеры методов биометрической аутентификации приведены на рис. 3.6.

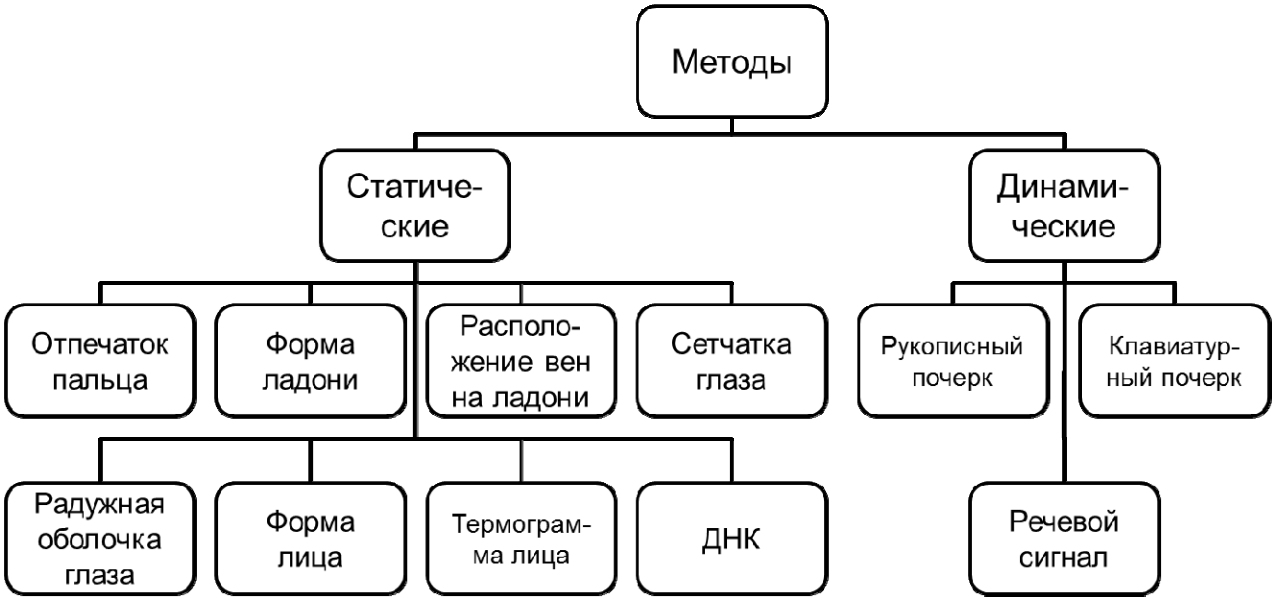


Рис. 3.6. Методы биометрической аутентификации

Состав систем биометрической аутентификации:

– аппаратная часть, позволяющая регистрировать «образ» уникальной характеристики человека (сканер отпечатка пальца, видеокамера, микрофон);

– программная часть, позволяющая из «образа» выделять параметры, совокупность значений которых уникально для человека.

Регистрирующее устройство для разных биометрических методов может быть как стандартным – веб-камера (форма лица) или микрофон (речевой сигнал), так и специализированным – сканер отпечатка пальца, инфракрасная камера (термограмма лица).

Основой систем биометрической аутентификации является совокупность параметров, позволяющих идентифицировать человека. Например, для идентификации по форме лица – размер некоторых частей лица (глаза, нос, рот и др.) и расстояние между ними, для клавиатурного почерка – скорость набора ключевого слова и длительность нажатия клавиш. В разных алгоритмах совокупности параметров могут различаться.

Решение о предоставлении доступа пользователя принимается после сравнения определённых на основе «образа» значений искомых параметров с эталонными значениями данного пользователя.

При сравнении значений, полученных при аутентификации, с эталонными редко происходит полное совпадение, поэтому доступ предоставляется при достижении заданного в системе порога.

Таким образом, этап регистрации пользователя при применении биометрических систем заключается в первоначальном определении значений параметров. Эти значения будут являться эталонными, и созданный

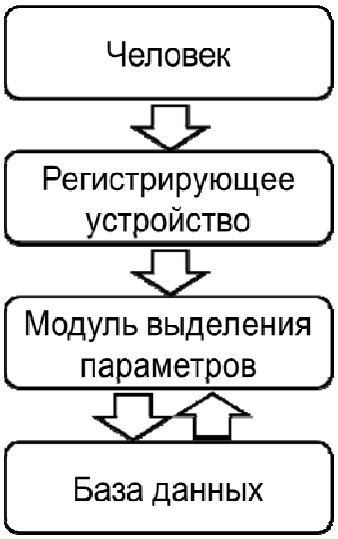
шаблон будет храниться в базе данных. При создании шаблона «образы» могут сниматься несколько раз, а полученные значения параметров усредняться.

Схема биометрической аутентификации приведена на рис. 3.7.

Режимы работы биометрических систем:

– верификация – пользователь вводит имя своей учётной записи, после чего система сравнивает полученные значения с шаблоном данной учётной записи;

– идентификация – система сравнивает полученные значения с шаблонами всех пользователей, хранящимися в базе, выбирая наиболее близкий.



• Уникальная биометрическая характеристика человека.

• Регистрирующее устройство, снимающее «образ» характеристики.

• Определение значений параметров, уникальных для человека, и сравнение их с эталонными.

• База данных для хранения значений эталонных параметров.

Рис. 3.7. Схема биометрической аутентификации

Качество работы биометрических систем определяется на основе количества ошибок первого и второго рода. Ошибка первого рода (ложная тревога) происходит, когда санкционированному пользователю система отказывает в доступе. Ошибка второго рода (пропуск цели) происходит, когда доступ предоставляется несанкционированному пользователю.

Преимущества биометрической аутентификации:

– в отличие от физических объектов и паролей, пользователь не может потерять или забыть средство аутентификации;

– поведенческие характеристики неотделимы от человека, что усложняет их использование злоумышленником.

Недостатки биометрической аутентификации:

– изменение некоторых характеристик со временем (голос, клавиатурный почерк);

– возможность изменения поведенческих характеристик при различном эмоциональном или физическом состоянии;

– не все биометрические методы применимы (например, анализ крови) или правильно воспринимаются пользователем (отпечаток пальца);

– не все методы теоретически гарантируют уникальность.

3.5. Разграничение доступа к защищаемым объектам

Задачи механизмов разграничения доступа:

– у прикладного пользователя не должно быть возможности работы с информацией, устройствами ввода-вывода, каналами связи, к которым ему запрещён доступ;

– в системе не должна предоставляться возможность несанкционированного обмена данными между пользователями (механизм санкционированного обмена данными должен предоставляться);

– прикладной пользователь не должен иметь доступ к настройкам, связанным с безопасностью системы.

3.5.1. Типы механизмов управления доступом

Дискреционное управление доступом – разграничение доступа между поименованными субъектами и поименованными объектами. При этом задание правил разграничения доступа осуществляется на основе матрицы доступа. В качестве субъекта может рассматриваться не только пользователь (и процессы, выполняемые от его имени), но и группа пользователей. Учётная информация субъекта и объекта – их идентификаторы (например, имя пользователя и имя файла).

Матрица доступа должна содержать явное и недвусмысленное перечисление допустимых типов доступа (чтение, изменение и т.д.), т.е. тех типов доступа к данному ресурсу, которые являются санкционированными для данного субъекта.

Пример матрицы доступа для субъектов «Администратор» и группа «Пользователи» приведён в табл. 3.2.

Таблица 3.2

Пример матрицы доступа

	Администратор	Пользователи
Программа1	чтение, запись, выполнение	чтение, выполнение
Принтер1	печать, управление очередью печати	печать
Съёмные носители	чтение, запись	чтение

Преимущество дискреционного управления доступом:

– гибкость настроек доступа – любому субъекту можно назначить индивидуальные права доступа.

Недостатки:

– усложнение администрирования системы при задании настроек и поддержании их в актуальном состоянии;

– усложнение администрирования системы при вводе в систему новых пользователей.

Сложности администрирования при предоставлении доступа связаны с необходимостью перечисления всех субъектов, которым разрешён доступ к защищаемому объекту. Из-за этого могут возникнуть ошибки при добавлении новых объектов или субъектов в систему, а также при необходимости изменения прав доступа.

Упрощение администрирования возможно при использовании мандатного механизма управления доступом. Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Метки конфиденциальности чаще всего являются иерархическими, описывая т.н. полномочия. Таким образом, для назначения прав доступа используются метки конфиденциальности, назначаемые субъектам (уровень доступа к информации) и объектам доступа (уровень конфиденциальности). Самый простой подход к назначению меток – разделение их на три иерархических уровня: «Общедоступно», «Конфиденциально» и «Строго конфиденциально».

Реализация мандатного управления доступом:

– формальное сравнение метки субъекта, запросившего доступ, и метки объекта, к которому запрошен доступ;

– принятие решения о предоставлении доступа на основе правил, основанных на противодействии снижению уровня конфиденциальности защищаемой информации.

Наиболее распространённый набор правил:

– субъект может читать объект, только если уровень метки субъекта в иерархии не ниже, чем уровень метки объекта;

– субъект осуществляет запись в объект, только если уровень метки субъекта равен уровню метки объекта.

Формальное представление этих правил:

– субъект С имеет доступ к объекту О на «Чтение» в случае, если выполняется условие $M\text{с} \geq M\text{о}$;

– субъект С имеет доступ к объекту О на «Запись» в случае, если выполняется условие $M\text{с} = M\text{о}$.

Использование подобных правил позволяет не допустить чтение файла с меткой «Конфиденциально» субъектом с меткой (уровнем доступа) «Общедоступно». Кроме того, становится возможным контроль потоков информации, защищающий конфиденциальные данные от разглашения. При попытке копирования информации из файла с меткой «Конфи-

денциально» в файл с меткой «Общедоступно» субъект будет вынужден повысить уровень конфиденциальности общедоступного файла.

Мандатное управление доступом позволяет при создании новых объектов или изменении прав доступа настраивать только один параметр – метку, что приводит к упрощению администрирования.

Преимущество мандатной модели:

– более простое администрирование по сравнению с дискреционной моделью, что приводит к меньшему количеству ошибок.

Недостаток:

– отсутствует разграничение доступа в пределах одного уровня конфиденциальности.

В современных операционных системах используется ролевое управление доступом. Фактически, оно является расширением дискреционного и мандатного механизма. Дополнительно к правам доступа к объектам пользователю предоставляются привилегии. Привилегия представляет собой действие, которое может привести к нарушению безопасности объекта: резервное копирование файлов, загрузка и выгрузка драйверов устройств и др.

3.5.2. Типы доступа к файловым объектам

Основными типами доступа в операционных системах являются чтение, изменение и выполнение. При этом набор базовых прав доступа в Unix-системах и системах семейства Windows NT отличается. Отличия вызваны разным представлением для пользователя типов доступа для файлов и каталогов.

В Unix-системах и к файлам и к каталогам применяются одинаковые типы доступа, но трактуются они операционной системой по-разному. Права доступа пользователя формируются на основе совокупности предоставленных ему типов доступа: r – доступ на чтение; w – доступ на запись; x – доступ на выполнение.

Типы доступа для файлов в Unix-системах: r – доступ на чтение файла; w – доступ на изменение файла; x – доступ на выполнение файла (если разрешён этот тип доступа, то файл считается исполняемым).

Типы доступа для каталогов в Unix-системах: r – право на получение списка файлов в каталоге; w – право на создание файлов в каталоге; x – право на переход в каталог.

В операционных системах семейства Windows NT набор прав доступа реализует тот же функционал, но их базовое представление может включать несколько типов доступа и иногда друг друга дублировать.

Изменение – разрешает пользователям удалять файлы и каталоги, вносить изменения в разрешения или получать право собственности на файл или папку от другого пользователя.

Чтение и выполнение – разрешает пользователям читать и запускать файлы, не внося изменений в содержание совместно используемого тома или каталога.

Список содержимого папки – позволяет пользователям просматривать содержимое каталогов (применимо только к каталогам).

Чтение – разрешает пользователям просматривать содержимое тома или каталога. Они также могут открывать файлы, но не имеют права сохранять изменения.

Запись – разрешает пользователям делать записи в папках или каталогах, но запрещает открывать файлы или просматривать список файлов.

Кроме основных прав доступа, существуют дополнительные права, которые и являются теми «кирпичиками», из которых формируются основные.

Возможность изменять права доступа к файлу, кроме администратора, предоставляется владельцу этого файла. По умолчанию в операционных системах владельцем файла становится пользователь, создавший данный файл. Это приводит к тому, что пользователь, имеющий право чтения файла с конфиденциальной информацией, может скопировать эту информацию в созданный файл. После чего, может предоставить доступ к новому файлу тем пользователям, которые не имеют допуска к конфиденциальной информации. Таким образом, подобный подход к назначению владельца файла может привести к утечке информации.

Файловая система является иерархической структурой, поэтому чаще всего бывает нужно задать дочерним файлам и каталогам такие же права доступа, как и каталогу, в котором они находятся. Для автоматизации процесса назначения прав дочерним каталогам применяется механизм наследования прав. При применении наследования каждый создаваемый каталог или файл будет автоматически получать права, установленные для родительского каталога.

Конечно, в операционных системах существует возможность отмены наследования или дополнения наследуемых прав. При этом частичной отмены наследованных прав не существует, поэтому введена возможность явного запрета на использование типа доступа. Из-за наличия возможности дополнения родительских прав возможно возникновение конфликтов при наследовании: например, к файлу доступ разрешён, а к родительскому каталогу явно запрещён; или пользователю доступ разрешён, а группе, в которую он входит – запрещён. Решение о предоставлении доступа к файлу операционная система принимает на основе следующих правил приоритета прав доступа:

– на любом данном уровне иерархии разрешения от нескольких групп объединяются;

– на любом данном уровне отрицательные разрешения (запреты) имеют приоритет над положительными;

– разрешения, предоставленные файловому объекту напрямую, имеют приоритет над наследуемыми разрешениями;

– разрешения, унаследованные от «близких родственников», имеют приоритет над разрешениями, унаследованными от «дальних родственников».

3.5.3. Управление доступом к устройствам

В стандартных дистрибутивах операционных системах чаще всего возможности управления доступом к устройствам либо практически отсутствуют, либо сильно ограничены. Например, предоставляется возможность только разрешать или запрещать использование какого-либо типа устройств всеми пользователями. Поэтому для корректного разграничения доступа необходимо использовать специализированное программное обеспечение. Тогда возможно предоставление доступа к устройствам только пользователей, которые имеют право с ними работать, а также ограничение работы пользователей по времени суток и дням недели.

Управление доступом к устройствам возможно на уровне интерфейса (порта) и на уровне экземпляра устройства (съёмное устройство, принтеры, жёсткие диски и т.д). Подобный подход позволяет, например, полностью запретить подключение к USB-порту любых устройств или разрешить доступ к порту, но запретить работу с каким-то классом устройств. Также можно запретить доступ к классу устройств (принтерам и др.) вне зависимости от того, через какой порт осуществляется подключение. При управлении доступом к съёмным носителям информации возможно указание типа доступа (чтение, изменение). Для управления доступом к принтерам используются следующие типы доступа: доступ на печать, доступ на управление очередью печати, доступ на управление принтером (установка нового принтера и др.).

При разграничении доступа к съёмным носителям и CD-, DVD-дискам существует возможность использования белого списка устройств. Использование данной функции целесообразно в случае необходимости запрета доступа ко всем носителям, кроме явно разрешённых.

В качестве примера можно привести запрет всех флеш-носителей, принадлежащих пользователям. Разрешёнными будут считаться те носители, которые учтены в организации и предназначены для хранения конфиденциальной информации. В этом случае в белый список должен быть занесён каждый разрешённый носитель.

Второй вариант использования белого списка устройств заключается в разрешении работы с определённой моделью устройств определённого производителя. Это применяется, если в системе используются какие-либо устройства в качестве средств аутентификации.

3.5.4. Управление доступом к программам

Существуют два подхода к управлению доступом к исполняемым файлам. Первый подход реализован в операционных системах по умолчанию – разрешено выполнение всех программ, кроме программ, выполнение которых явно запрещено. Запретить выполнение файла можно при установке прав доступа к нему. Второй подход заключается в запрете выполнения всех программ, кроме явно разрешённых. Тогда управление доступом к программам приводит к обеспечению целостности программной среды. Обеспечение целостности программной среды предназначено для исключения возможности запуска в операционной системе вредоносных и других нежелательных программ (отладчиков, взломщиков паролей и т.п.).

Самый простой вариант реализации второго подхода – назначение каждому пользователю (группе пользователей) каталога, из которого он имеет право запускать любые программы, не имея возможности запуска программ из других каталогов.

В операционных системах семейства Windows NT реализован механизм, позволяющий через групповые политики разрешить/запретить запуск программ из заданного каталога. Основной недостаток, присущий работе с каталогом, заключается в наличии возможности копирования файла в разрешённый каталог. Этот недостаток можно преодолеть за счёт использования возможности разрешения/запрета запуска программ по их хешу.

При использовании правил управления доступом к программам, основанных на хеше, возможно составление конечного списка разрешённых к запуску программ. Разрешённые программы смогут запускаться из любого каталога (запрещённые программы – не смогут). Недостаток использования хеша программы заключается в том, что программы периодически обновляются, как следствие, изменяется их хеш. Это значит, что каждое обновление программы требует изменения списка хешей разрешённых программ.

3.6. Аудит событий

Аудит событий безопасности включает в себя распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности.

Записи, получаемые в результате аудита, могут быть проанализированы, чтобы определить, какие действия, относящиеся к безопасности, происходили, и кто из пользователей их сгенерировал. Изменять записи аудита может только система. Таким образом, задачами, решаемыми аудитом событий, являются:

– обеспечение подотчётности пользователей и администраторов;

– обнаружение попыток нарушения информационной безопасности;

– обеспечение возможности восстановления хода событий при расследовании инцидентов, связанных с информационной безопасностью.

Записи о событиях хранятся в журнале аудита. В случае переполнения журнала операционная система должна заблокировать текущий сеанс пользователя до тех пор, пока администратор очистит данный журнал. При этом операционная система должна предоставлять администратору возможность сохранения копии всех записей журнала.

В рамках аудита безопасности возможна регистрация информации о различных типах действий, запрашиваемых пользователями. Перечень типов событий, фиксируемых операционными системами:

– вход (выход) пользователей в операционную систему;

– доступ к защищаемым ресурсам (создание, чтение, изменение, удаление и др.);

– управление учётными записями (создание, удаление, смена пароля и др.);

– изменение правил разграничения доступа;

– использование привилегий (чтение журнала аудита, резервное копирование и др.);

– работа процессов (запуск программ, обращение процесса к файлу и др.).

Для этих событий должны фиксироваться следующие данные:

– дата и время события;

– имя учётной записи пользователя, запросившего действие;

– имя рабочей станции, где произошло событие;

– тип события;

– было ли дано разрешение на выполнение запрошенного действия (Успех) или в выполнении действия было отказано (Отказ).

Для некоторых типов событий должны фиксироваться дополнительные сведения. При отслеживании работы процессов указывается имя программы с указанием полного пути к ней. При доступе к ресурсам указываются имя ресурса и использовавшийся тип доступа. При изменении правил разграничения доступа указывается не только пользователь, изменявший права, но пользователь, которому они были изменены, а также имя ресурса.

Таким образом, можно, например, установить аудит отказов на доступ к конфиденциальному файлу и выяснить, какие пользователи, не имевшие права доступа, пытались его прочесть. Или установить аудит успехов на работу с принтером и определить, кто распечатывал конфиденциальный документ.

Для удобства и ускорения поиска событий, интересующих администратора, в операционных системах реализована возможность фильтрации. Фильтрация событий возможна по дате события, имени учётной записи пользователя, совершившего действие, типу события и другой фиксируемой в журнале аудита информации.

Дополнительно к функциям регистрации событий операционные системы могут обеспечивать реакцию на подозрительные действия пользователей. Если пользователем запрошено действие или была произведена последовательность действий, потенциально являющихся опасными, то система может на это отреагировать. Варианты реакции системы: оповещение администратора, блокирование учётной записи пользователя, блокирование действий процесса и т.д. Самый простой пример подобной реакции – блокирование учётной записи пользователя после заданного администратором количества неправильных попыток ввода пароля.

Список литературы

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. Наука и Техника, Санкт-Петербург. 2004.

2. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер-класс. / Пер. с англ. 4-е изд. М.: Издательско-торговый дом «Русская Редакция»; СПб.: Питер; 2005. 992 с.

3. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. Москва, 1992.

4. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные требования безопасности. Гостехкомиссия России, 2002.

4. БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

4.1. Ведение в базы данных

4.1.1. Основные определения

Под **информацией** (в бытовом понимании) понимают любые сведения о каком-либо событии, сущности, процессе и т.д., являющемся объектом операций: восприятия, передачи, преобразования или использования.

В нашем сложном мире любая взаимосвязь и коррекция действий возможны только благодаря информации.

Данные можно определить как информацию, фиксированную в определенной форме, пригодной для последующей обработки, хранения и передачи.

Совокупность различных средств, предназначенных для сбора, подготовки, хранения, обработки и выдачи информации в интересах различных пользователей и приложений, представляет собой **информационную систему** (ИС).

Система, при функционировании которой на различных этапах технологического процесса обработки информации принимает участие человек, называется **автоматизированной информационной системой** (АИС).

По характеру обрабатываемой информации ИС делятся на документальные и фактографические.

Документальные ИС служат для работы с документами на естественном языке: монографиями, научными отчетами, диссертациями, текстами законодательных актов и т.д. Основной задачей документальных ИС является поиск документов по их содержанию. (например, система КОНСУЛЬТАНТ – относится к документальным системам)

В фактографических ИС хранимая и обрабатываемая информация представляет собой конкретные сведения, факты, примеры, результаты измерений, справочные и статистические данные (базы данных, применяемые в ПФР относятся к документальным). Информация часто носит оперативный характер. Она выдается пользователю или прикладным программам для обработки. Фактографические ИС реализуются банками данных.

Банк данных – это автоматизированная информационная система, включающая в свой состав комплекс специальных методов и средств (математических, информационных, программных, языковых, организационных и технических) для поддержания динамической модели предметной области с целью обеспечения информационных запросов пользователей [2].

В результате развития технологии ИС система доступа к данным и данные, которые накапливаются в системе, были логически разделены. Поэтому БнД состоит из двух частей:

1) **базы данных** (БД), которая является датологическим представлением информационной модели предметной области;

2) **системы управления базой данных** (СУБД), с помощью которой и реализуется централизованное управление данными, хранимыми в базе, доступ к ним и поддержание их в состоянии, соответствующем состоянию предметной области.

СУБД – программная система, предназначенная для создания БД, поддержания ее в актуальном состоянии, обеспечения эффективного доступа к ней. Доступ к БД возможен только посредством СУБД.

В настоящее время вместо термина банк данных применяют термин база данных. Далее термин база данных будет применяться в этом смысле. Необходимо помнить, что база данных состоит из собственно данных и средства доступа к ним.

4.1.2. Модели данных

Модель предметной области состоит, как правило, из описания конкретных фактов, а также некоторых общих понятий и закономерностей.

В различных системах для задания запроса (например, поискового) из программы пользователя к СУБД применяются разные методы. Можно сказать, что каждая СУБД имеет свои языковые средства, называемые **языком данных** (ЯД). При этом необходимо учитывать, что ЯД не язык программирования в традиционном смысле. Язык данных задает правила обработки запроса (например, поиска), а также указывает элементы данных, т.е. ЯД предполагает определенную структуризацию данных (средства описания данных – **язык описания данных ЯОД**) и средства описания действий, которые необходимо выполнять над данными (**средства манипулирования данными –** ЯМД). Совокупность средств описания и средств манипулирования называется моделью данных.

В настоящее время широко известны три типа моделей данных: иерархическая, сетевая и реляционная. Наиболее перспективной для развития и применения считается реляционная модель представления данных. Основные исследования всех трех типов моделей данных закончены, и они показали, что все три типа моделей равномощны.

4.1.3. Проектирование концептуальной модели данных

4.1.3.1. Основы концептуального моделирования

Концептуальную модель данных (КМД) строят как на инфологическом проектировании (информационная КМД), так и датологическом

проектировании (датологическая/логическая КМД). КМД представляет обобщенную модель предметной области со стороны всех пользователей системы.

Информационная КМД представляет собой формальное описание объектов предметной области, их свойств и отношений между ними, выполненное с точки зрения определенного вида деятельности и без учета каких-либо аспектов реализации БД.

Основными составляющими КМД являются:

- объекты (сущности);
- объектное свойство (атрибут сущности);
- объектное отношение (связь);
- время.

Предметная область БД определена, если известны существующие в ней объекты, их свойства и отношения.

Объекты (сущности) – это вовлеченные в деятельность люди, предметы, события, понятия, документы, места и т.п., информация о которых должна накапливаться в разрабатываемой БД и которые представляют интерес для пользователей.

В качестве объектов в моделях предметной области могут рассматриваться, как материальные объекты (предприятия, изделия, сотрудники и т.д.), так и нематериальные (описание явлений, рефераты статей и т.д.). Выбор объектов осуществляется в соответствии с назначением АИС.

Объекты (сущности) реального мира, о которых будет накапливаться информация, подвергаются классификации, и фиксируется совокупность их свойств (атрибутов), посредством которых будут описаны в БД типы объектов.

Атрибут – это поименованная характеристика (свойство) объекта (сущности), которая принимает значения из некоторого множества значений.

Выбор существенного атрибута или атрибутов носит субъективный характер. Атрибуты могут изменяться, в то время как сам объект остается тем же. На атрибуты могут быть наложены ограничения.

Например:

- уникальность значений в атрибуте;
- значения по умолчанию;
- обязательное указание;
- диапазон значений;
- список значений;
- условия на значения.

Множество всех объектов, имеющих некоторое общее свойство, называется **объектным множеством или типом объектов.**

Элемент объектного множества называется **объект-элемент** или **экземпляр сущности**.

Объект (сущность) – это абстракция экземпляров.

При этом все экземпляры данного типа обладают одинаковыми свойствами (атрибутами). Свойства типа «наследуются» каждым экземпляром объекта данного типа.

Например, объект (сущность) – *Сотрудник*.

Атрибуты Сотрудника: *Фамилия, Имя, Отчество, Дата рождения, Паспорт, ИНН.*

Экземпляры объекта Сотрудник:

Петров Иван Сергеевич 23.02.60 Паспорт1 ИНН 123456

Сидорова Мария Игоревна 08.03.65 Паспорт2 ИНН 654321

Для того чтобы отличить один объект от других объектов данного типа (для различия одного экземпляра объекта от другого), необходим уникальный идентификатор, называемый **первичным ключом (primary key (PK))**.

В качестве первичного ключа можно использовать атрибут или группу атрибутов.

Требования к первичному ключу:

- должен однозначно определять экземпляр сущности;
- должен быть уникален;
- не должен содержать пустых значений (должен быть обязательно указан, NOT NULL);
- не должен меняться;
- не должен быть избыточным.

Выбор первичного ключа лежит на разработчике БД. Первичный ключ может быть суррогатным.

Объекты (сущности) предметной области **состоят в связи**, если хотя бы одному экземпляру одного из них можно поставить в соответствии (по определенному правилу) один или более экземпляров другого.

Связи выступают в концептуальной модели в качестве средства, с помощью которого представляются отношения между объектами, имеющими место в предметной области.

Связь характеризуется **арностью** – числом вступающих в нее сущностей.

Могут встречаться бинарные (между двумя сущностями), тернарные и, в общем случае, *n*-арные связи. Наиболее часто встречаются бинарные связи. Связь характеризуется мощностью связи.

Мощностью связи называется максимальное количество элементов одного объектного множества, связанных с одним элементом другого объектного множества.

Число *M* экземпляров связи, которые могут быть образованы одним экземпляром сущности называется **мощностью связи** со стороны этой сущности.

Наиболее распространены мощности связи:

– **один к одному 1:1** – одному экземпляру одной сущности соответствует один экземпляр другой сущности;

– **один ко многим 1:M** – одному экземпляру одной сущности соответствует несколько экземпляров другой сущности. Данная связь называется направленной. В ней выделяют сущность-родитель и сущность-потомок. Родительская сущность-это сущность мощность связи со стороны которой M (M>1). Потомок – сущность мощность связи со стороны которой 1 или 0 (когда родитель у потомка отсутствует).

Для моделирования связи 1:M необходимо:

– определить родителя и потомка в связи;

– определить первичный ключ в родительской сущности;

– добавить в сущности потомке атрибут/ты первичного ключа родителя.

– данные атрибут/ты первичного ключа родителя в потомке называются **внешним ключом (Foreing Key) FK**.

FK указывает принадлежность потомка к родителю.

Если внешний ключ (FK) входит в состав первичного ключа потомка, то связь называется идентифицирующей. Если FK не входит в состав первичного ключа потомка, то связь является не идентифицирующей.

многие ко многим M:M – одному экземпляру первой сущности соответствует несколько экземпляров второй сущности, одному экземпляру второй сущности соответствует несколько экземпляров первой сущности.

Связь M:M считается не явной. Для моделирования связи M:M вводится дополнительная связующая сущность, которая разбивает связь M:M на связи 1:M и M:1 (рис. 4.1).

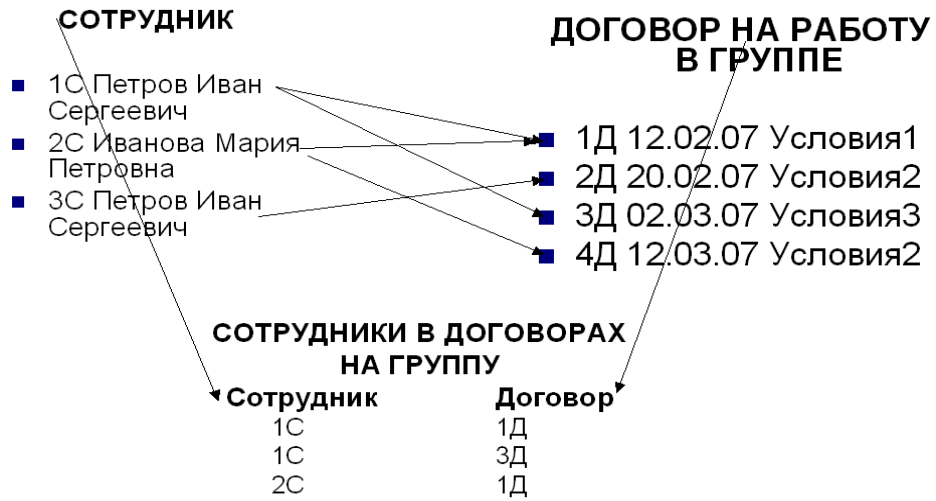


Рис. 4.1. Преобразование связи M:M

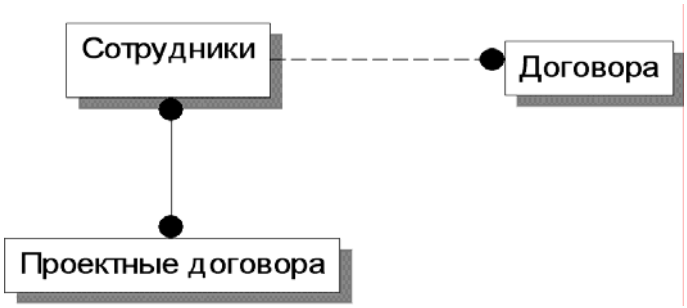
Связь, максимальная мощность которой как минимум в одном направлении равна одному, называется **функциональным.** Мощность связи определяется правилами, действующими в предметной области (бизнес-правилами).

При построении КМД выделяют три основных уровня:

– уровень «сущность-связь» (ER-уровень);

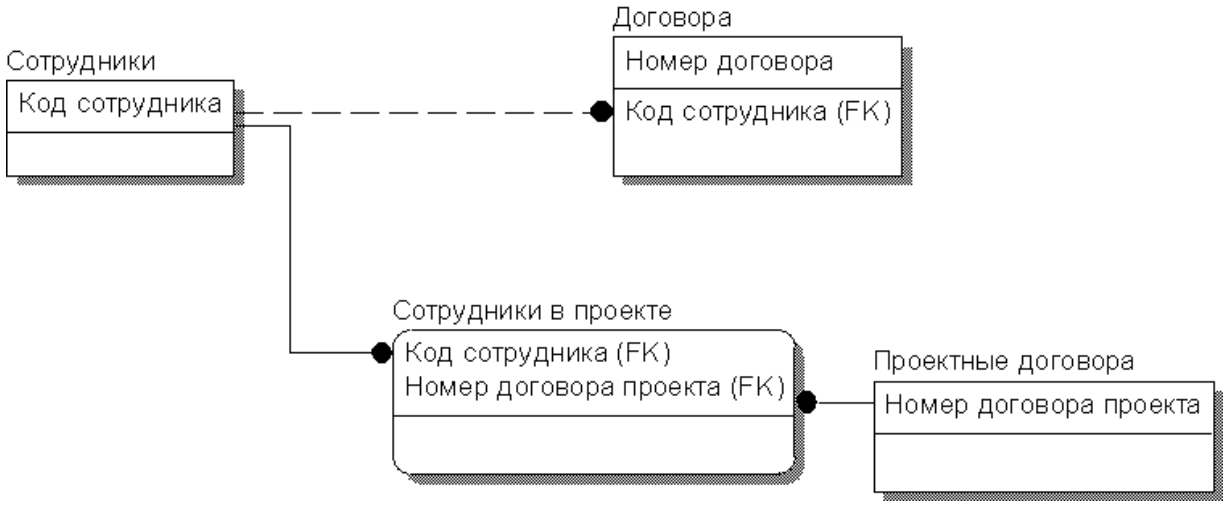
– уровень ключей (КВ-уровень);

– полная атрибутивная модель (FA-уровень).



На уровне «сущность-связь» (ER-уровень) выделяют сущности, связи и мощности связей.

На уровне ключей (КВ-уровень) – выделяют первичные и внешние ключи.



На уровне полной атрибутивной модели (FA-уровень) указываются все атрибуты.

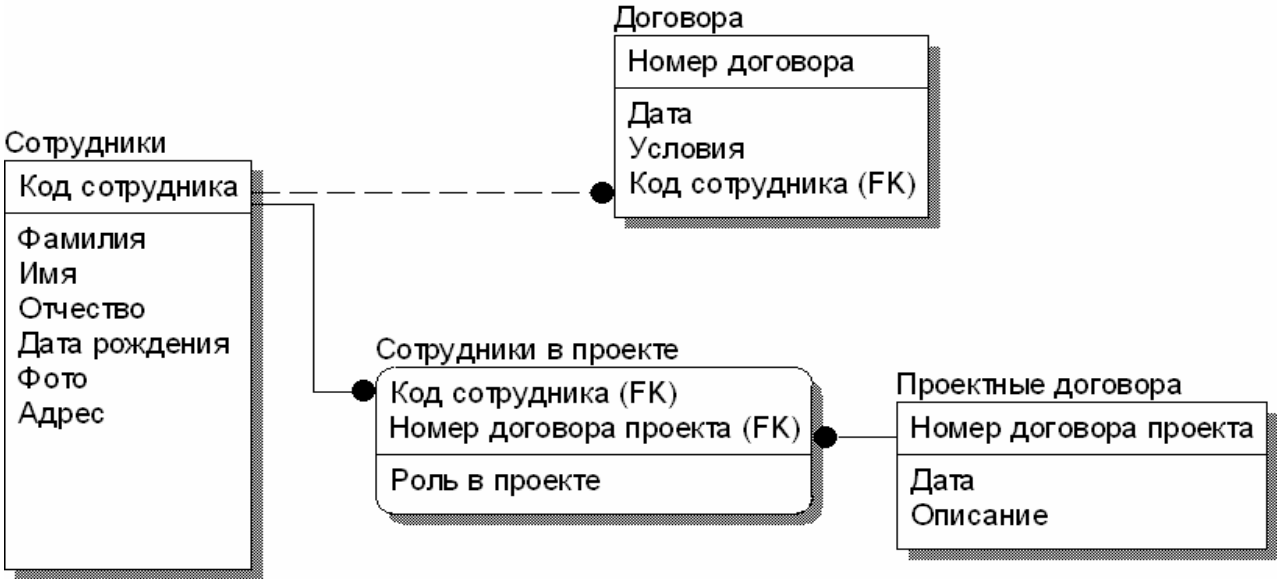


Рис. 4.2. Три уровня концептуальной модели данных

Совокупность типов объектов, их атрибутов и типов связей между ними характеризует типовую структуру предметной области.

Необходимо помнить, что требования пользователей могут меняться со временем, а БД – это динамическая модель предметной области. Фактор времени может изменить способы определения, использования данных, бизнес-правила в системе, структуры данных. Все это должно отразиться в концептуальной модели данных.

При моделировании предметной области проектировщик разбивает ее на ряд локальных областей, моделируя каждую область отдельно, а затем выполняет их объединение посредством связей.

4.1.3.2. Датологическое проектирование

Датологический этап проектирования связан с выбранной системой управления базой данных (СУБД). Он делится на логическое и физическое проектирование БД.

Задача этапа логического проектирования базы данных состоит в разработке ее «логической» структуры в соответствии с инфологической моделью предметной области.

В результате выполнения данного этапа создается концептуальная модель базы данных, специфицированная на языках определения данных.

На этапе логического проектирования строится датологическая логическая модель данных (ЛМД). Это переложенная информационная ЛМД в терминах модели данных СУБД. Проектирование реляционной БД происходит на основе принципов нормализации. Модель данных при этом идентифицирует сущности, домены, атрибуты, связи между данными и поддерживает единый концептуальный взгляд на данные и взаимосвязи.

После построения ЛМД ее необходимо сопроводить дополнительным материалом, уточняющим и поясняющим ее смысл. Для этого необходимо составить глоссарий разработанной структуре БД, с указанием наложенных ограничений.

Глоссарий является обязательным дополнением. Он содержит описание отдельных диаграмм модели и определения сущностей, атрибутов, доменов.

Обязательные компоненты глоссария:

– имена – уникальные, осмысленные и соответствующие предметной области наименования сущностей, атрибутов, доменов;

– определения – краткие, точные, однозначные тексты, обеспечивающие правильное понимание смысла имен.

Определения должны быть одинаково применимы в любом контексте, в котором встречается имя. Глоссарий рекомендуется сформировать в виде таблиц для сущностей, атрибутов, доменов:

– для сущностей:

Имя сущности	Определение	Ограничения

– для атрибутов:

Имя атрибута	Определение	Ограничения

– для доменов:

Имя домена	Определение	Ограничения

Или в виде сводной таблицы глоссария:

Имя сущности 1	Определение	Ограничения
Имена атрибутов сущности 1		
Имя атрибута 1 сущности1		
Имя атрибута 2 сущности1		
Имя атрибута n сущности1		
Имя сущности2		
Имена атрибутов сущности 2		
Имя атрибута1 сущности2		
Имя атрибута2 сущности2		
и т.д.		
Имя домена 1		
Имя домена 2		
и т.д.		

4.1.3. Нормализация данных

Обсудим один из основных принципов проектирования данных – принцип *нормализации.*

Нормализация представляет собой процесс реорганизации данных путем ликвидации повторяющихся групп и иных противоречий в хранении данных с целью приведения таблиц к виду, позволяющему осуществлять непротиворечивое и корректное редактирование данных. Нередко после нормализации к структуре БД добавляется одна или несколько таблиц.

Теория нормализации основана на концепции нормальных форм. Говорят, что таблица находится в данной нормальной форме, если она удовлетворяет определенному набору требований. Теоретически существуют пять нормальных форм, но на практике обычно используются только первые три. Это делается с целью упрощения структуры БД.

Таблица соответствует **первой нормальной форме**, если все значения ее полей атомарны и все записи – уникальны.

Говорят, что реляционная таблица находится **во второй нормальной форме**, если она находится в первой нормальной форме и ее не ключевые поля полностью зависят от всего первичного ключа.

Говорят, что реляционная таблица находится в **третьей нормальной форме**, если она находится во второй нормальной форме и все ее не ключевые поля зависят только от первичного ключа.

Если в отношении, находящемся в третьей нормальной форме, отсутствуют многозначные зависимости, но имеются другие зависимости от ключа, то третья нормальная форма будет иметь аномалии операций. В этом случае рассматривают усиленную третью нормальную форму (форму Бойса-Кодда).

Отношение находится в нормальной форме **Бойса-Кодда**, если оно находится в третьей нормальной форме и каждый детерминант отношения является возможным ключом отношения. Атрибут (или комбинацию атрибутов), от которого какой-либо другой атрибут зависит функционально (полно), называют детерминантом.

Четвертая нормальная форма запрещает хранить независимые компоненты в одной таблице, когда между этими компонентами существуют отношения многие-ко-многим. Можно решить проблему приведения к четвертой нормальной форме, поместив каждый многозначный атрибут в отдельную таблицу вместе с ключом, от которого этот атрибут зависит.

Пятая нормальная форма была предложена для того, чтобы исключить аномалии, связанные с особым типом ограничительных условий, называемых совместимыми зависимостями. Эти зависимости имеют в основном теоретический интерес. Не было предложено правил приведения к пятой нормальной форме.

Нормализация устраняет избыточность данных, что позволяет снизить объем хранимых данных и избавиться от описанных выше аномалий их изменения.

4.1.4. Технология клиент-сервер

«Клиент-сервер» – это модель взаимодействия компьютеров в сети. Как правило, компьютеры не являются равноправными. Каждый из них имеет свое, отличное от других, назначение, играет определенную роль. Некоторые компьютеры в сети владеют и распоряжаются информационно-вычислительными ресурсами, такими как процессоры, файловая система, почтовая служба, служба печати, база данных. Другие имеют возможность обращаться к этим службам, пользуясь услугами первых. Компьютер, управляющий тем или иным ресурсом, принято называть сервером этого ресурса, а компьютер, желающий им воспользоваться – клиен-

том. Конкретный сервер определяется видом ресурса, которым он владеет. Так, если ресурсом являются базы данных, то речь идет о сервере баз данных, назначение которого – обслуживать запросы клиентов, связанные с обработкой данных; если ресурс – это файловая система, то говорят о файловом сервере или файл-сервере и т.д.

Локальное приложение обычно устанавливается на единичном персональном компьютере, там же располагается и БД, с которой работает данное приложение. Однако необходимость коллективной работы с одной и той же БД повлекла за собой перенос БД на сетевой сервер.

Основной проблемой при коллективном доступе к данным, в таких случаях, является проблема обеспечения смысловой и ссылочной целостности данных при одновременном изменении одних и тех же данных.

В ходе эксплуатации таких систем были выявлены общие недостатки файл – серверного подхода. Они состоят в следующем:

- вся тяжесть вычислительной нагрузки при доступе к данным ложится на приложение клиента, что является следствием принципа обработки информации в системах «файл – сервер»: при выдаче запроса на выборку информации из таблицы вся таблица БД копируется на клиентское место, и выборка осуществляется на клиентском месте;
- не оптимально расходуются ресурсы клиентского компьютера и сети; например, если в результате запроса нужно получить 2 записи из таблицы объемом 15 000 записей, то все 15 000 записей будут скопированы с файл-сервера на клиентский компьютер; в результате чего возрастает сетевой трафик, и увеличиваются требования к аппаратным мощностям пользовательского компьютера. Потребности в постоянном увеличении вычислительных мощностей клиентского компьютера обусловливается, в данном варианте, не только развитием программного обеспечения как такового, но и возрастанием обрабатываемых объемов информации;
- в БД на файл-сервере гораздо проще вносить изменения в отдельные таблицы, минуя приложения, непосредственно из инструментальных средств; подобная возможность облегчается тем обстоятельством, что, фактически, у локальных СУБД база данных понятие более логическое, чем физическое, поскольку под БД понимается набор отдельных таблиц, сосуществующих в едином каталоге на диске. Все это позволяет говорить о низком уровне безопасности – как с точки зрения хищения и нанесения вреда, так и с точки зрения внесения ошибочных изменений;
- бизнес – правила (определяют реакцию системы на добавление, изменение, удаление данных и реализуют блокировку действий, которые могут разрушить ссылочную или смысловую целостность БД) в системах файл-сервер реализуются в приложении, что позволяет в разных приложениях, работающих с одной БД, проектировать взаимоисключающие бизнес-правила; смысловая целостность информации при этом может нарушаться.

Приведенные недостатки решаются при переводе приложений из архитектуры файл-сервер в архитектуру клиент-сервер, которая знаменует собой следующий этап в развитии СУБД. Характерной особенностью архитектуры клиент-сервер является перенос вычислительной нагрузки на сервер БД (SQL-сервер) и максимальная разгрузка приложения клиента от вычислительной работы, а также существенное укрепление безопасности данных – как от злонамеренных, так и просто ошибочных изменений.

БД в этом случае помещается на сетевом сервере, как и в архитектуре «файл – сервер», однако прямого доступа к БД из приложений не происходит, функции прямого обращения к БД осуществляет специальная управляющая программа – сервер БД (SQL-сервер), поставляемая разработчиком СУБД.

Взаимодействие сервера БД и приложения-клиента происходит следующим образом: клиент формирует SQL-запрос и отсылает его серверу. Сервер, приняв запрос, выполняет его, и результат возвращает клиенту. В клиентском приложении в основном осуществляется интерпретация полученных от сервера данных, реализация интерфейса с пользователем и ввод данных, а также реализация части бизнес-правил.

Преимущества архитектуры клиент – сервер:

1) большинство вычислительных процессов происходит на сервере; таким образом, снижаются требования к вычислительным мощностям компьютера клиента;

2) снижается сетевой трафик за счет посылки сервером клиенту только тех данных, которые он запрашивал; например, если необходимо сделать из таблицы объемом 15000 записей выборку, результатом которой будут всего 2 записи, сервер выполнит запрос и перешлет клиенту набор данных из 2 записей;

3) упрощается наращивание вычислительных мощностей в условиях развития программного обеспечения и возрастания объемов обрабатываемых данных: проще и чаще дешевле усилить мощности на сетевом сервере или полностью заменить сервер на более мощный, нежели наращивать мощности или полностью заменять 100-500 клиентских компьютеров;

4) БД на сервере представляет собой, как правило, единый файл, в котором содержатся таблицы БД, ограничения целостности и другие компоненты БД. Взломать такую БД, даже при наличии умысла, тяжело. Значительно увеличивается защищенность БД от ввода неправильных значений, поскольку сервер БД проводит автоматическую проверку соответствия вводимых значений наложенным ограничениям и автоматически выполняет необходимые бизнес – правила: кроме того, сервер отслеживает, уровни доступа для каждого пользователя и блокирует осуществление попыток выполнения неразрешенных для пользователя действий, например, изменения или просмотр таблиц; все это позволяет говорить о

значительно более высоком уровне обеспечения безопасности БД и ссылочной и смысловой целостности информации;

5) сервер реализует управление транзакциями и предотвращает попытки одновременного изменения одних и тех же данных;

6) безопасность системы возрастает за счет переноса большей части бизнес – правил на сервер; падает удельный вес противоречащих друг другу бизнес – правил в клиентском приложении, выполняющих разные действия над БД; определить такие противоречивые бизнес-правила в приложениях клиента все еще можно, однако намного труднее их выполнить ввиду автоматического отслеживания сервером БД правильности данных.

При этом схемы использования клиент-серверной технологии приведены на рис. 4.3–4.5. Положительными моментами использования является обилие инструментальных средств. Недостатки: высокая загрузка сети, невозможность удовлетворительного администрирования. Различные по природе функции смешиваются в одной программе.

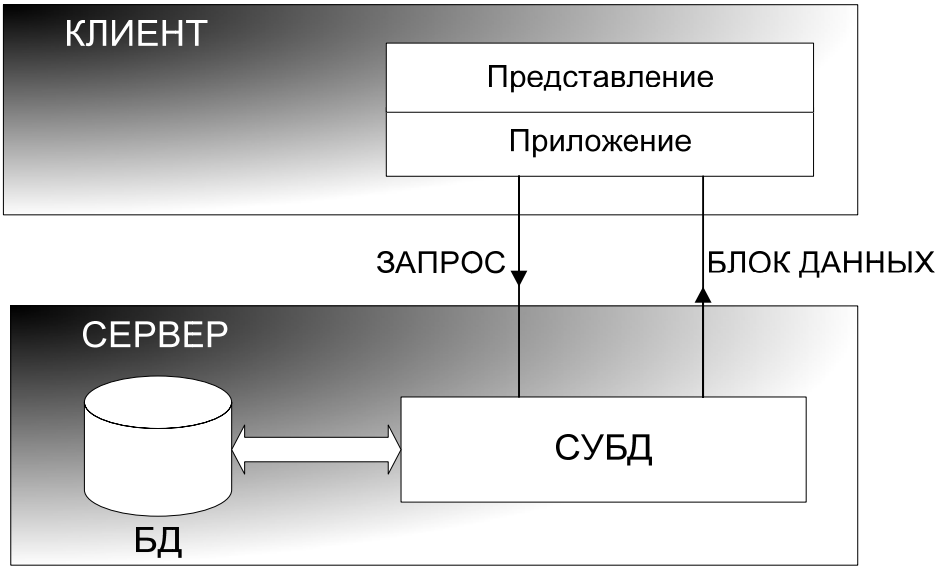


Рис. 4.3. Схема непосредственного клиент-серверного доступа

При взаимной работе коллективом разработчиков с одной базой сложно контролировать взаимную непротиворечивость алгоритмов обработки.

Приложение оформляется как набор хранимых процедур SQL и переносится на компьютер – сервер БД. При этом снижается трафик сети, возникает возможность централизованной обработки данных. Когда БД велики, за счет сложного администрирования приводит к потере качества. Процедурное расширение SQL не является полноценным языком программирования. Отсутствуют средства отладки и тестирования хранимых процедур. На практике, на сервере хранятся простейшие процедуры, вся работа по прежнему проводится на компьютере – клиенте. Требуется дополнительная аппаратура и ПО.

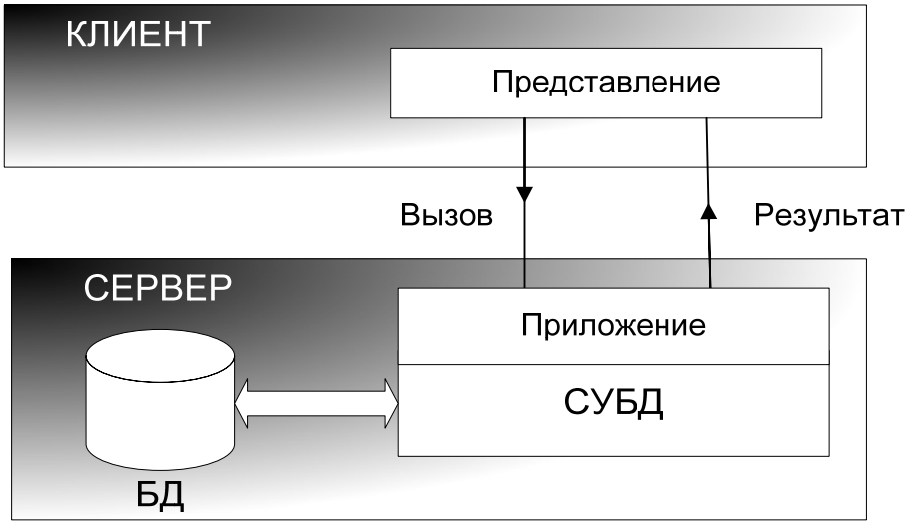


Рис. 4.4. Схема клиент-серверного доступа через приложение на стороне СУБД

В последнем случае: выделение третьего звена – сервера приложений. В этом случае прикладная система независима от СУБД и от клиента. Данная архитектура обеспечивает баланс загрузки и возможность динамической реконфигурации системы. Но при этом дополнительные средства уходят на аппаратуру. Плюс инструментальные средства – Visual Basic, C++, расширенный SQL.

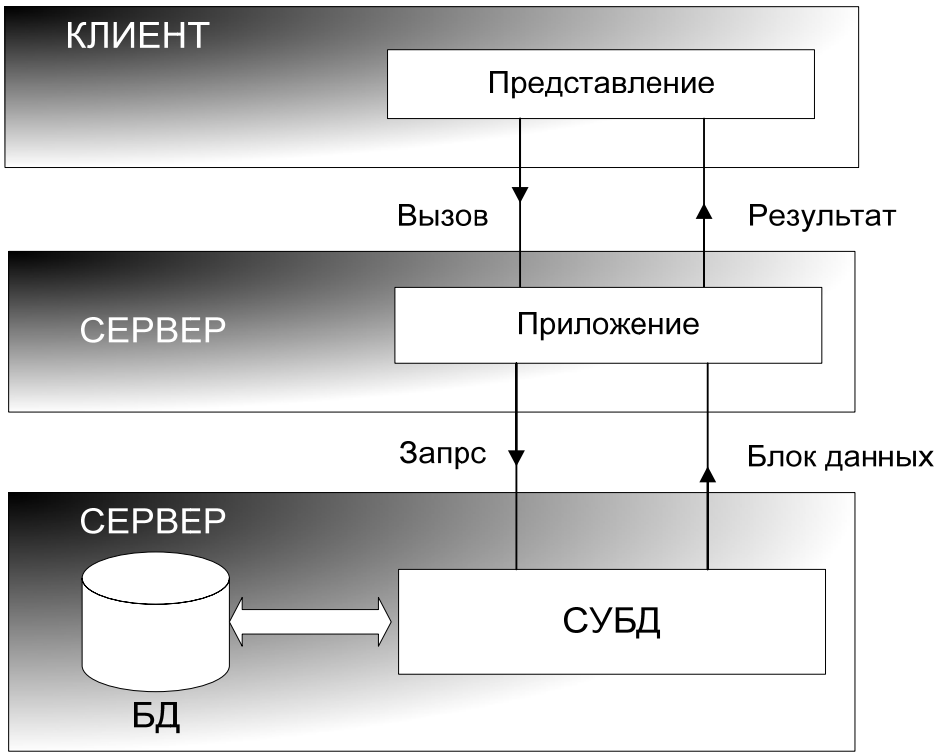


Рис. 4.5. Схема трехзвенного клиент-серверного доступа

4.1.5. Распределенные БД

Одна из главных особенностей современных информационных систем – распределенный характер [6]. Главная проблема таких систем – ор-

ганизация обработки распределенных данных. Данные находятся на компьютерах различных моделей и производителей, функционирующих под управлением различных операционных систем, а доступ к данным осуществляется разнородным программным обеспечением.

На рис. 4.6 приведены режимы работы с базой данных.

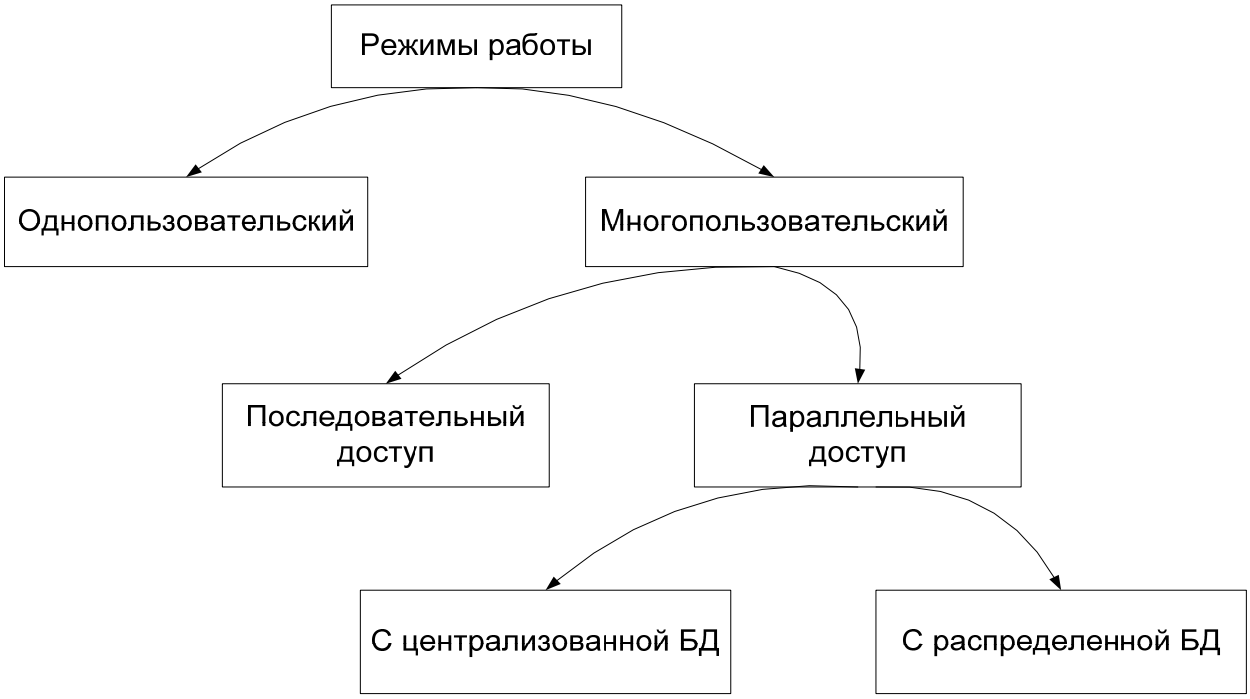


Рис. 4.6. Режимы работы с базой данных

Существуют две технологии: технология распределенных баз данных (Distributed Database) и технология тиражирования данных (Data Replication).

Под распределенной базой данных подразумевают базу, включающую фрагменты из нескольких баз данных, которые располагаются на различных узлах сети компьютеров, и, возможно, управляются различными СУБД. Распределенная база данных выглядит с точки зрения пользователей и прикладных программ как обычная локальная база. В этом смысле слово «распределенная» отражает способ организации базы данных, но не внешнюю ее характеристику.

В отличие от распределенных баз, тиражирование данных предполагает отказ от их физического распределения и опирается на идею дублирования данных в различных узлах сети компьютеров.

Пусть имеется система, построенная по клиент/серверной архитектуре. На компьютере (локальный узел) запускается клиентское приложение. Он соединен в сети с компьютером, на котором выполняется сервер базы данных и находится сама база данных. Существует специальный компонент СУБД обеспечивающий взаимодействие клиента и сервера, называемый коммуникационным сервером. Для поддержки взаимодействия клиента и сервера он должен функционировать на удаленном узле; в то

же время на локальном узле должна выполняться программа связи, взаимодействующая с коммуникационным сервером.

Для обеспечения работы РСУБД заложены следующие принципы:

- Прозрачность расположения. Доступ к информационным ресурсам должен быть полностью прозрачен относительно расположения данных. Когда прикладная программа запускается на локальном узле, а база данных находится на удаленном, возникает проблема идентификации удаленного узла. Для того, чтобы получить доступ к базе данных на удаленном узле, необходимо указать имя удаленного узла и имя базы данных. Если использовать жестко фиксированное имя узла в паре «имя_узла, имя_БД», то прикладная программа становится зависимой от расположения БД;
- Прозрачность сети. Клиент и сервер взаимодействуют по сети с конкретной топологией. Для поддержки взаимодействия всегда используется определенный протокол. Следовательно, оно должно быть организовано таким образом, чтобы обеспечивать независимость как от используемого сетевого аппаратного обеспечения, так и от протоколов сетевого обмена;
- Автоматическое преобразование форматов данных. В сети могут быть компьютеры, отличающиеся разрядностью (16-ти, 32- и 64-х разрядные процессоры), порядком следования байт в слове, представлением чисел с плавающей точкой и т.д. Задача коммуникационного сервера состоит в том, чтобы на уровне обмена данными обеспечить согласование форматов между удаленным и локальным узлами с тем, чтобы данные, извлеченные сервером из базы на удаленном узле и переданные по сети, были правильно истолкованы прикладной программой на локальном узле;
- Автоматическая трансляция кодов. Сервер может работать с одной кодовой таблицей (например, EBCDIC), клиент – с другой (например, ASCII), при этом происходит рассогласование трактовки кодов символов. Поэтому, если на локальном узле используется одна кодовая таблица, а на удаленном – другая, то при передаче запросов по сети и при получении ответов на них необходимо обеспечить трансляцию кодов. Решение этой задачи также ложится на коммуникационный сервер;
- Межоперабельность. Это качество можно трактовать как открытость системы, позволяющую встраивать ее как компонент в сложную разнородную распределенную среду. Межоперабельность достигается как за счет использования интерфейсов, соответствующих международным, национальным и промышленным стандартам, так и за счет специальных решений;
- Прозрачность расположения. Современные информационные системы требуют доступа к разнородным базам данных. Это означает, что в прикладной программе для реализации запросов к базам данных должны быть использованы такие средства, чтобы запросы были понятны раз-

личным СУБД, как реляционным, так и опирающимся на другие модели данных.

Принципиальное отличие технологии тиражирования данных от технологии распределенных баз данных заключается в отказе от распределенных данных. Ее суть состоит в том, что любая БД всегда является локальной. Данные всегда размещаются локально на том узле сети, где они обрабатываются.

Тиражирование данных – это асинхронный перенос изменений объектов исходной базы данных в БД, принадлежащие различным узлам распределенной системы. Функции тиражирования данных выполняет специальный модуль СУБД – сервер тиражирования данных, называемый репликатором. Его задача – поддержка идентичности данных во всех БД. Сигналом для запуска репликатора служит срабатывание правила перехватывающего любые изменения тиражируемого объекта БД. В качестве базиса для тиражирования выступает транзакция к БД. В то же время возможен перенос изменений группами транзакций, периодически или в некоторый момент времени, что дает возможность исследовать состояние принимающей БД на определенный момент времени

4.2. Безопасность баз данных

4.2.1. Введение

Защита информации в процессе ее сбора, хранения и обработки приобретает исключительное значение, поскольку информация представляет собой, чрезвычайно важный ресурс.

Под защитой информации понимается совокупность мероприятий, методов и средств, обеспечивающих решение следующих основных задач:

– целостности, то есть защиту от несанкционированного изменения информации и обеспечение ее существования в неискаженном виде;

– конфиденциальности, то есть защиту от несанкционированного получения информации;

– доступности, то есть защиту от несанкционированного удержания информации и ресурсов.

В соответствии с первым пунктом необходимо предупредить изменение или разрушение данных при сбоях аппаратуры, программных средств, ошибках в работе сотрудников групп эксплуатации.

Обеспечение безопасности базы данных начинается с этапа анализа возможных угроз, который необходим для фиксирования на определенный момент времени состояния БД и определения возможных воздействий на каждый компонент базы.

Необходимо выбрать из всего множества возможных воздействий лишь те, которые могут реально произойти и нанести серьезный ущерб владельцам и пользователям базы.

На этапе планирования формируется система защиты как единая совокупность мер противодействия различной природы. По способам осуществления все меры обеспечения безопасности базы данных подразделяются на: правовые (законодательные), морально-этические, административные, физические и технические (аппаратные и программные) [6].

Наилучшие результаты достигаются при системном подходе к вопросам обеспечения безопасности БД и комплексном использовании различных мер защиты на всех этапах жизненного цикла БД, начиная с самых ранних стадий ее проектирования.

Известно не так много общих (универсальных) способов защиты БД от различных воздействий на нее. Ими являются :

– идентификация и аутентификация субъектов (пользователей, процессов и т.д.) БД;

– контроль доступа к ресурсам БД;

– регистрация и анализ событий, происходящих в БД;

– контроль целостности объектов БД;

– шифрование данных;

– аудит;

– резервирование ресурсов и компонентов БД.

Эти универсальные способы защиты могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты.

4.2.2. Обеспечение целостности данных

Обеспечение целостности базы накладывает ограничения (называемые правилами целостности) на отношения. Функцией системы обеспечения целостности является недопущение противоречий в данных относительно этих условий. Противоречия могут возникнуть в результате ошибок пользователей при вводе данных, путем модификации базы данных, а также при незавершенных операциях модификации по причине сбоев в системе. При этом требуется восстановление данных. При длительной и сложной модификации базы данных накладываемые условия в ходе модификации могут не выполняться.

Проблема целостности заключается в правильности данных в базе данных в любой момент времени и касается защиты данных от непреднамеренных ошибок и их предотвращения.

Поддержка целостности в реляционной модели данных в ее классическом понимании включает в себя три аспекта:

- поддержка структурной целостности;
- поддержка языковой целостности;
- поддержка ссылочной целостности.

Реляционная СУБД работает только со структурой данных типа реляционное отношение. Для обеспечения целостности необходимо поддерживать правила соответствующие реляционной таблице:

- в таблице недолжно быть одинаковых кортежей;
- столбцы таблицы соответствуют атрибутам отношения;
- каждый объект таблицы идентифицируется первичным ключом;
- каждый атрибут таблицы имеет уникальное имя;
- порядок строк в таблице произвольный;
- два отношения, отличающиеся только порядком следования столбцов, считаются одинаковыми.

Проблемы структурной целостности необходимо рассмотреть в случае NULL значений, т.е. таких значений которые на данный момент не определены, но могут быть определены в любое время.

При появлении NULL значений не действуют стандартные правила сравнения: одно неопределенное значение не равно другому неопределенному значению. Для выявления равенства значений в этом случае используют предикаты типа:

<имя атрибута> is NULL

<имя атрибута> is not NULL

Если в данном кортеже указанный атрибут примет неопределенной значение, то предикат is NULL принимает значение true, а предикат is not NULL значение – false. Таблица истинностей логических операций изменилась, поскольку из двузначной превратилась в трехзначную.

Таблица 4.1

a	b	¬ a	a & b	a | b
1	1	0	1	1
1	0	0	0	1
1	–	0	–	1
0	1	1	0	1
0	0	1	0	0
0	–	1	0	–
–	1	–	–	1
–	0	–	0	–
–	–	–	–	–

В табл. 4.1– единица кодирует значение TRUE, нуль – FALSE, – – неопределенное значение.

Поддержка языковой целостности состоит в том, что реляционная СУБД должна обеспечивать языки описания и манипулирования данными не ниже стандарта SQL. То есть не должны быть доступны низко-

уровневые средства манипулирования данными, не соответствующие стандарту. Поэтому доступ к БД возможен и с использованием SQL.

Ссылочная целостность. Означает обеспечение одного из заданных принципов взаимосвязи между экземплярами кортежей взаимосвязанных отношений:

– кортежи подчиненного отношения уничтожаются при удалении кортежа основного отношения, связанного с ним;

– кортежи основного отношения модифицируются при удалении кортежа основного отношения связанного с ним, при этом на месте родительского отношения ставится неопределенное NULL значение.

Ссылочная целостность поддерживается с использованием двух стратегий:

1) не разрешаются операции, приводящие к нарушению ссылочной целостности (обеспечивается проверками наличия кортежей в дочернем отношении, связанными с некоторым кортежем родительского отношения);

2) разрешаются требуемые операции с условием каскадных изменений далее в дочерних узлах.

Эти стратегии являются стандартными и присутствуют во всех СУБД, в которых имеется поддержка ссылочной целостности.

Структурная, языковая и ссылочная целостность определяет правила работы СУБД с реляционными структурами данных. Требования поддержки трех видов говорят о том, что каждая СУБД должна уметь это делать, а разработчики приложений должны их учитывать.

Но для некоторых ограничений, которые связаны с содержанием базы данных, требуются другие методы. Например, при рассмотрении БД «Отдел кадров» ряд бизнес правил не может быть поддержан с помощью вышеперечисленных методов.

Например. На работу преподавателем принимаются граждане, имеющие диплом установленного образца или – каждый работник должен иметь прописку.

Эти виды ограничений сведены в поддержку семантической целостности, обеспечиваемыми механизмами СУБД. Семантическая поддержка обеспечивается двумя путями: декларативным и процедурным.

Декларативный путь связан с наличием в рамках СУБД механизмов обеспечивающих проверку и выполнение ряда декларативно заданных правил-ограничений (бизнес правил).

Существуют следующие виды декларативных ограничений целостности:

1) ограничение целостности атрибута:

– значение по умолчанию;

– уникальность значения;

– задание обязательных и необязательных значений;

– задание условий на значение атрибутов;

2) ограничения целостности, задаваемые на уровне домена. Используются, если в базе присутствуют несколько столбцов разных отношений, которые принимают значения из одного и того же множества допустимых значений. Некоторые СУБД поддерживают доменную структуру и разрешают отдельно определять домены, задавать тип данных для каждого домена и бизнес правила для них. Удобно, если БД большая, содержит сотни отношений. В этом случае поменять условия, задаваемые на домен проще, чем просматривать все атрибуты и менять условия на них;

3) ограничения целостности, задаваемые на уровне отношения. Например, выразить требования на наличие хотя бы одного телефона – рабочего или домашнего в базе данных «Контакты»;

4) ограничения целостности, задаваемые на уровне связи между отношениями: задание обязательности связи, принципов каскадного удаления и каскадного изменения данных. Эти виды ограничений могут быть выражены заданием обязательности или необязательности внешних ключей.

Декларативная семантическая целостность обеспечивается на этапе создания базы данных.

Процедурное обеспечение семантической целостности задается с помощью хранимых процедур и триггеров.

Хранимые процедуры – это подпрограммы на языке SQL, хранящиеся в базах данных и представляющие собой один из видов их общих ресурсов. Тело любой хранимой процедуры представляет последовательность SQL-операторов, например таких, как выборка данных (SELECT), их модификация (UPDATE), удаление данных (DELETE), операторы цикла (LOOP), условные операторы (IF, CASE) и ряд других. Процедуры вызываются оператором CALL и могут использовать как входные параметры (передающие значения в процедуру), так и выходные параметры (возвращающие результаты процедуры вызывающему программному объекту). Процедуры могут вызываться из процедур, функций и других типов программных объектов.

Хранимые процедуры, создаются оператором CREATE PROCEDURE. Модификация тела хранимой процедуры осуществляется оператором ALTER PROCEDURE. Эти операторы могут использовать:

– пользователи, которым разрешено создавать объекты базы данных, т.е. тем кто имеет класс полномочий – RESOURCE;

– администратор базы данных.

Любая хранимая процедура всегда выполняется с привилегиями ее владельца. Это позволяет пользователям, не имеющим прямого доступа к таблицам данных, возможность обращения к этим таблицам через процедуры, которые они имеют право использовать. Для каждой таблицы хранимые процедуры представляет собой унифицированный механизм взаимодействия с ней. Это лишает пользователей сделать что-нибудь лишнее с таблицами данных и способствует поддержанию целостности данных.

Триггер – это специальный вид хранимой процедуры, которую СУБД вызывает при выполнении операций модификации соответствующих таблиц. Триггер автоматически активизируется при выполнении операции, с которой он связан. Триггеры связываются с одной или несколькими операциями модификации над одной таблицей.

Например, триггер может выполняться при вставке, изменении или удалении строки в существующей таблице. Триггер сообщает СУБД, как нужно выполнять команды SQL INSERT, UPDATE или DELETE, чтобы выполнялись бизнес правила организации.

4.2.3. Администрирование базы данных

Автоматизированные информационные системы рассматриваются как ресурсы, требующие не только хороших технических характеристик, но и хорошего управления. Администрация базы данных в основном состоит в обеспечении того, чтобы точная и непротиворечивая информация была доступна пользователям в нужное время и в нужной форме.

Администратор базы данных должен хорошо знать структуру БД, состав и все характеристики системы, так как сбои и нарушения в системе могут возникнуть в самых различных местах.

Функции администратора базы данных главным образом лежат в области работы с пользователями базы данных, планировании, проектировании и реализации информационных систем. Эффективная работа включает в себя разработку общих стандартов и процедур, целью которых является эффективный контроль целостности и защиты данных.

Администратор БД отвечает за:

- проектирование структуры БД, методы упорядочивания файлов БД, методы доступа к файлам БД;
- задание ограничений целостности при описании структуры БД и обработки БД;
- первоначальную загрузку и ведение БД;
- защиту данных;
- обеспечение восстановления БД;
- сбор статистики по характеру запросов;
- анализ эффективности работы БД;
- работу с конечными пользователями;
- подготовку и поддержку ПО;
- организационно-методическую работу по проектированию БД.

Решение вопросов контроля необходимо для эффективного управления базой данных. Поскольку к базе параллельно обращается множество пользователей, поддержание целостности данных и ее защита является сложной, но очень важной задачей.

Администратор базы данных назначается в момент инсталляции системы и наделяется рядом особых привилегий: располагает всеми полномочиями по всем объектам базы данных и для всех команд.

При решении вопросов защиты данных в обязанности администратора базы данных входит следующее:

– классификация данных в соответствии с их использованием;

– определение прав доступа отдельных пользователей к определенным группам данных в базе и ограничений на характер операций, выполняемых пользователем с этими данными;

– организация системы контроля доступа к данным;

– тестирование всех вновь создаваемых средств защиты данных;

– периодическое проведение проверок правильности функционирования системы защиты данных;

– исследование возникающих случаев нарушения защиты данных и проведение политики их предотвращения;

– исследование современных достижений в области технологии защиты данных и их использование для совершенствования соответствующих средств функционирующей БД и т. п.

4.2.4. Транзакции

Транзакция (transaction) представляет собой последовательность операторов языка SQL, которая представляет собой логическую единицу работы СУБД. Управление транзакциями обеспечивает интерпретацию некоторого блока операций как неделимого целого. Управление транзакциями гарантирует, что, либо будут выполнены все операции из блока, либо не будет выполнено ни одной. На основании этого тезиса можно выделить следующие свойства транзакций:

Атомарности. Транзакция должна быть выполнена целиком или не выполнена вовсе.

Согласованности. По мере выполнения транзакции данные переходят из одного согласованного состояния в другое, т.е. транзакция не разрушает взаимной согласованности данных.

Изолированности. Конкурирующие за доступ к БД транзакции выполняются изолированно друг от друга, но для пользователя это может выглядеть так, что они выполняются одновременно.

Долговечности. Если транзакция успешно завершена, то изменения данных, которые были произведены, не могут быть потеряны ни при каких обстоятельствах.

Транзакции необходимы для устранения конфликтов пользователей, пытающихся одновременно обращаться к одним и тем же данным. Конфликты могут состоять в потере изменений, в незафиксированных изменениях и ряде других, более сложных проблем. Потеря изменений проис-

ходит в ситуации, когда две или несколько программ читают одни и те же данные, вносят в них какие-либо изменения и затем пытаются одновременно записать результат по прежнему месту. Разумеется, в базе данных могут быть сохранены изменения, выполненные только одной программой – другие изменения будут потеряны. Транзакции используются для восстановления данных после сбоя или отказа системы.

Источниками отказов могут быть:

1. Системные ошибки. Системные ошибки возникают в случае, если система вошла в нежелательной состояние такое, например, как взаимоблокировка, не позволяющая нормально продолжить выполнение программы. Такой отказ может приводить, а может не приводить к повреждению файлов данных. Принцип блокировки заключается в том, что когда пользователь выбирает данные из БД, СУБД автоматически запрещает к ним доступ, чтобы какой-либо пользователь не мог провести над ними операции обновления. Существует много видов блокировок. В основном операции блокирования и разблокирования производятся автоматически, но в некоторых системах пользователи могут управлять определенными аспектами блокировок, например с помощью команд SQL они могут выбрать уровень применения блокировки (уровень строки или уровень таблицы).

2. Отказы оборудования. Два наиболее часто встречающихся отказа: ошибка диска (авария головки), потеря способности передачи данных через сеть.

3. Логические ошибки. Плохие данные или их отсутствие часто является причиной, не позволяющей нормально продолжить выполнение программы.

В стандарте ANSI/ISO SQL включены операторы фиксации транзакции и отката транзакции COMMIT, ROLLBACK.

COMMIT означает успешное завершение транзакции, все изменения принимаются.

ROLLBACK – прерывание транзакции, отмена выполненных действий сделанных в БД в рамках этой транзакции.

Новая транзакция может начаться непосредственно после оператора ROLLBACK.

Между командами SQL, отмечающими начало и конец транзакций, может помещаться любое количество операторов SQL. В зависимости от синтаксиса, который поддерживает ваша система, это может выглядеть примерно так:

[оператор начала транзакции]
SQL оператор
SQL оператор
SQL оператор
[оператор конца транзакции]

Если какую-то транзакцию необходимо отменить до того, как она будет выполнена – либо по причине какого-то сбоя, либо просто потому, что пользователю что-то не понравилось, – результаты выполнения всех ее операторов, которые успели завершиться, должны быть отменены. Транзакцию можно отменить (или вернуть в исходное положение) с помощью команды транзакции ROLLBACK в любой момент до выполнения команды транзакции COMMIT.

Для сохранения промежуточных состояний, подтверждения или отката транзакции, используется специальный механизм, называемый **журналом транзакций**. Журнал транзакций создается на этапе создания базы данных и обеспечивает надежное хранение данных, возможность восстановления согласованного состояния БД после любого рода сбоев. В журнале транзакций фиксируются все изменения БД. После сбоя восстанавливается всегда последнее согласованное состояние базы.

Восстановление базы происходит в следующих случаях:

1. Индивидуальный откат транзакций (применение ROLLBACK, аварийное завершение работы программы, взаимоблокировка, при параллельном выполнении транзакций).

2. Восстановление после потери содержимого оперативной памяти(мягкий сбой) (аварийное выключение питания, неустранимый сбой процессора).

3. Поломка ВЗУ (жесткий сбой).

В журнале транзакций, каждая транзакция имеет свой номер. Все изменения помечаются номером транзакции и значениями изменяемых атрибутов, там же сохраняются команды начала и конца транзакции.

Транзакция рассматривается как последовательность элементарных атомарных операций. Элементарные операции различных транзакций могут выполняться в произвольной очередности (конечно, внутри каждой транзакции последовательность элементарных операций этой транзакции является строго определенной). Набор из нескольких транзакций, элементарные операции которых чередуются друг с другом, называется **смесью транзакций**. Последовательность, в которой выполняются элементарные операции заданного набора транзакций, называется **графиком запуска** набора транзакций.

Обеспечение изолированности пользователей, таким образом, сводится к выбору подходящего (в каком-то смысле правильного) графика запуска транзакций.

4.2.5. Идентификация и установление подлинности

На самом элементарном уровне концепции обеспечения безопасности баз данных и управления информацией исключительно просты. Не-

обходимо поддерживать два фундаментальных принципа: проверку полномочий (санкционирование) и проверку подлинности (аутентификация).

Идентификация – присвоение объекту уникального имени или числа.

Проверка полномочий основана на том, что для каждого пользователя или процесса информационной системы устанавливается набор санкционированных действий, которые он может выполнять по отношению к определенным объектам.

Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированные действия, действительно является тем, за кого он себя выдает

Указанные проверки используются совместно для принятия решения о доступе.

Идентификация пользователя нужна не только для опознавания, но и для учета обращений к ресурсу.

Подлинность обычно устанавливается один раз, но в установках, обеспечивающих высокую степень безопасности, может потребоваться периодическая перепроверка или перепроверка в определенных условиях. Повторное установление подлинности желательно, например, после системных сбоев.

4.2.5.1. Дискреционная защита

В современных СУБД достаточно развиты средства дискреционной защиты [7]. Дискреционное управление доступам (discretionary access control) – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Дискреционная защита является многоуровневой логической защитой. Логическая защита в СУБД представляет собой набор привилегий или ролей по отношению к защищаемому объекту. К логической защите можно отнести и владение таблицей (представлением). Владелец таблицы может изменять (расширять, отнимать, ограничивать доступ) набор привилегий (логическую защиту) . Данные о логической защите находятся в системных таблицах базы данных и отделены от защищаемых объектов (от таблиц или представлений).

Информация о зарегистрированных пользователях базы данных хранится в ее системном каталоге. Соединение с системой не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась, исключается. В процессе сеанса работы пользователя (от удачного прохождения идентификации и аутентификации до отсоединения от системы) все его действия непосредственно связываются с результатом идентификации. Отсоединение пользователя может быть как нормальным, так и насильственным (исходящим от пользователя-администратора, например в случае удаления пользова-

теля или при аварийном обрыве канала связи клиента и сервера). Во втором случае пользователь будет проинформирован об этом, и все его действия аннулируются до последней фиксации изменений, произведенных им в таблицах базы данных. В любом случае на время сеанса работы идентифицированный пользователь будет субъектом доступа для средств защиты информации от несанкционированного доступа (далее – СЗИ НСД) СУБД.

Следуя технологии открытых систем, субъект доступа может обращаться посредством СУБД к базе данных только из программ, поставляемых в дистрибутиве или подготовленных им самим, и только с помощью штатных средств системы.

Все субъекты контроля системы хранятся в таблице полномочий системы и разделены для системы на ряд категорий, например CONNECT, RESOURCE и DBA. Набор таких категорий определяется производителем СУБД. Для каждого отдельного вида подключения:

- CONNECT – конечные пользователи. По умолчанию им разрешено только соединение с базой данных и выполнение запросов к данным, все их действия регламентированы выданными им привилегиями;
- RESOURCE – привилегированные пользователи, обладающие правом создания собственных объектов в базе данных (таблиц, представлений, синонимов, хранимых процедур). Пользователь – владелец объекта обладает полным набором привилегий для управления данным объектом;
- DBA – категория администраторов базы данных. Включает возможности обеих предыдущих категорий, а также возможность вводить (удалять) в систему (из системы) субъекты защиты или изменять их категорию.

Набор привилегий можно определить для конкретного зарегистрированного пользователя или для группы пользователей (это могут быть собственно группы пользователей, роли и т.п.). Объектом защиты может являться таблица, представление, хранимая процедура и т.д. (подробный список объектов защиты имеется в документации к используемой СУБД). Субъектом защиты может быть пользователь, группа пользователей или роль, а также хранимая процедура, если такое предусматривается используемой реализацией. Если из используемой реализации следует, что хранимая процедура имеет «двойной статус» (она и объект защиты, и субъект защиты), то нужно очень внимательно рассмотреть возможные модели нарушителей разграничения прав доступа и предотвратить эти нарушения, построив, по возможности, соответствующую систему защиты.

При использовании хранимых процедур следует обращать особое внимание на то, от имени какого пользователя выполняется данная хранимая процедура в каждом конкретном случае.

Привилегии конкретному пользователю могут быть назначены администратором явно и неявно, например через роль. Роль – это еще один

возможный именованный носитель привилегий. С ролью не ассоциируют перечень допустимых пользователей – вместо этого роли защищают паролями, если, конечно, такая возможность поддерживается производителем СУБД. Роли удобно использовать, когда тот или иной набор привилегий необходимо выдать (или отобрать) группе пользователей. С одной стороны, это облегчает администратору управление привилегиями, с другой – вносит определенный порядок в случае необходимости изменить набор привилегий для группы пользователей сразу. Нужно особо отметить, что при выполнении хранимых процедур и интерактивных запросов может существовать зависимость набора привилегий пользователя от того, как они были получены: явно или через роль.

Если используемая вами реализация обладает подобным свойством, то изменение привилегий у группы пользователей следует реализовать как набор команд или как административную процедуру (в зависимости от предпочтений администратора).

Предложения управления привилегиями:

• назначение привилегии:

GRANT привилегия [ON объект] TO субъект [WITH GRANT OPTION]

• отмена привилегии:

REVOKE привилегия [ON объект] FROM субъект

Если субъект=пользователь, то привилегия назначается ему явно. Если субъект=роль, то для управления привилегиями используются соответственно:

GRANT ROLE имя_роли [ON объект] TO субъект [WITH GRANT OPTION]

REVOKE ROLE имя_роли [ON объект] FROM субъект

Назначение привилегии всем пользователям системы осуществляется следующим образом:

GRANT привилегия [ON объект] TO PUBLIC

В этом случае каждый новый созданный пользователь автоматически получит такую привилегию. Отмена привилегии осуществляется так:

REVOKE привилегия [ON объект] FROM PUBLIC

Необходимо иметь в виду, что некоторые реализации, например IBM DB2, используют группы пользователей, определенные в операционной системе. Поэтому следует обращать внимание на особенности реализации аналогов ролей в СУБД. Нужно выяснить, содержит ли реализация SQL-предложения вида:

CREATE ROLE имя_роли

DROP ROLE имя_роли

При управлении доступом к таблицам и представлениям набор привилегий в реализации СУБД определяется производителем.

Привилегии выборки и модификации данных:

SELECT – привилегия на выборку данных;

INSERT – привилегия на добавление данных;

DELETE – привилегия на удаление данных;

UPDATE – привилегия на обновление данных (можно указать определенные столбцы, разрешенные для обновления).

Привилегии изменения структуры таблиц:

ALTER – изменение физической/логической структуры базовой таблицы (изменение размеров и числа файлов таблицы, введение дополнительного столбца и т.п.);

INDEX – создание/удаление индексов на столбцы базовой таблицы;

ALL – все возможные действия над таблицей.

В реализациях могут присутствовать другие разновидности привилегий, например:

CONTROL (IBM DB2) – комплексная привилегия управления структурой таблицы,

REFERENCES – привилегия создания внешних ключей, RUNSTAT – выполнение сбора статистической информации по таблице и другие.

Однако дискреционная защита является довольно слабой, так как доступ ограничивается только к именованным объектам, а не собственно к хранящимся данным. В случае реализации информационной системы с использованием реляционной СУБД объектом будет, например, именованное отношение (то есть таблица), а субъектом – зарегистрированный пользователь. В этом случае нельзя в полном объеме ограничить доступ только к части информации, хранящейся в таблице. Частично проблему ограничения доступа к информации решают представления и использование хранимых процедур, которые реализуют тот или иной набор бизнес-правил.

4.2.5.2. Представления

Представление (view) – это сформированная выборка кортежей, хранящихся в таблице (таблицах). К представлению можно обращаться точно так же, как и к таблицам, за исключением операций модификации данных, поскольку некоторые типы представлений являются немодифицируемыми. Часто в реализациях view хранится как текст, описывающий запрос выборки, а не собственно выборка данных; выборка же создается динамически на момент выполнения предложения SQL, использующего view. Но разграничить доступ, например, к двум документам, которые удовлетворяют одному и тому же условию выборки, уже нельзя. Это связано с тем, что даже если ввести отдельный атрибут, который будет хранить информацию о метке конфиденциальности документа, то средствами SQL можно будет получить выборку данных без учета атрибута данной метки.

4.2.5.3. Мандатная защита

Средства мандатной защиты предоставляются специальными (trusted) версиями СУБД.

Мандатное управление доступом (mandatory access control) – это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Средства произвольного управления доступом не могут помешать авторизованному пользователю законным образом получить секретную информацию и затем сделать ее доступной для других, неавторизованных, пользователей. При произвольном управлении доступом привилегии существуют отдельно от данных (в случае реляционных СУБД – отдельно от строк реляционных таблиц), в результате чего данные оказываются «обезличенными» и ничто не мешает передать их кому угодно даже средствами самой СУБД; для этого нужно лишь получить доступ к таблице или представлению.

Физическая защита СУБД главным образом характеризует данные (их принадлежность, важность, представительность и пр.). Это в основном метки безопасности, описывающие группу принадлежности и уровни конфиденциальности и ценности данных объекта (таблицы, столбца, строки или поля). Метки безопасности (физическая защита) неизменны на всем протяжении существования объекта защиты (они уничтожаются только вместе с ним) и территориально (на диске) располагаются вместе с защищаемыми данными, а не в системном каталоге, как это происходит при логической защите.

Кроме разграничения доступа к информации посредством меток конфиденциальности, защищенные СУБД предоставляют средства слежения за доступом субъектов к объектам защиты (аудит).

Использование СУБД с возможностями мандатной защиты позволяет разграничить доступ собственно к данным, хранящимся в информационной системе, от доступа к именованным объектам данных.

Существуют реализации, позволяющие разграничивать доступ вплоть до конкретного значения конкретного атрибута в конкретной строке конкретной таблицы. Дело не ограничивается одним значением метки конфиденциальности – обычно сама метка представляет собой набор значений, отражающих, например, уровень защищенности устройства, на котором хранится таблица, уровень защищенности самой таблицы, уровень защищенности атрибута и уровень защищенности конкретного кортежа.

Все перечисленные объекты (независимо от их иерархии в базе данных) разбиваются здесь на группы принадлежности. Объект может принадлежать только одной из групп (это может быть, например, разбиение

по отделам организации). Группы принадлежности напрямую связаны с группами субъектов Субъект вправе видеть только данные своей группы, если между группами субъектов не установлены отношения доверия.

Все объекты выстроены в иерархию по уровням конфиденциальности и по уровням ценности или важности. Уровень конфиденциальности разбивает объекты по доступности на чтение (и даже на просмотр). Пользователь с более низким уровнем доступа не будет знать даже о существовании объектов с более высоким уровнем конфиденциальности. Уровень ценности, напротив, разбивает данные (объекты) по важности, ограничивая возможность их удаления и модификации.

Создать пользователя с произвольными уровнями может только администратор системы. Остальные администраторы (DBA) могут создавать пользователей (или изменять уровень пользователям) лишь в пределах отведенных им уровней. Пользователь может принудительно пометить вводимые данные, указав в списке атрибутов уровни доступа для соответствующих записей и полей (при выполнении операторов INSERT или UPDATE). По умолчанию вносимые данные наследуют уровни пользователя, вносящего/изменяющего данные. Защищаемые объекты: пользователи, таблицы, столбцы, записи (вносится при выполнении INSERT), поля записей (изменяются при выполнении UPDATE). Уровни, как и группы, нельзя использовать в случае, если они не созданы специальными запросами.

Конфигурация, к которой имеет доступ хотя бы один программист, не может считаться безопасной. Поэтому обеспечение информационной безопасности баз данных – дело весьма сложное, и во многом вследствие самой природы реляционных СУБД.

В целостной системе безопасности компьютерной среды, где исчерпывающая программа защиты информации обеспечивается за счет взаимодействия операционных систем, сетей, систем баз данных и других сервисов, проверка подлинности имеет прямое отношение к безопасности баз данных. Многие механизмы защиты баз данных, непосредственно зависят от наличия надежных средств проверки подлинности.

Модели безопасности, основанные на базовых механизмах проверки полномочий и подлинности, не решают таких проблем, как хищения пользовательских идентификаторов и паролей или злонамеренные действия некоторых пользователей, обладающих полномочиями. Например, программист, работающий над учетной системой, имеющей полный доступ к учетной базе данных, может встроить троянского коня в код программы с целью хищения средств или с другими подобными умыслами.

Отметим, что СУБД не должна разрешать выполнение какой-либо операции над базой данных пользователю, не получившему на это соответствующие права. Будем также считать, что санкционирование доступа

к данным (т.е. предоставление пользователю соответствующих прав) выполняется администратором базы данных.

Рассмотрим уровни доступа к базе данных, каждый из которых может оказаться целесообразным для предоставления определенной категории пользователей:

1. Неограниченный доступ ко всем отношениям в базе данных и, их поколениям.

2. Неограниченный доступ к группе отношений и их поколениям.

3. Ограниченный доступ к группе отношений и их поколениям.

На уровне отношения в СУБД различают следующие уровни доступа:

1) неограниченный доступ ко всему отношению для всех типов операций;

2) запрет на доступ к любым частям отношения для всех типов операций;

3) доступ к любой части отношения без права изменения ее содержимого;

4) доступ к любой части отношения, но с правом изменения значений только для атрибутов A_1, A_2,..., A_r. Неограниченный доступ только к одному кортежу отношения для всех типов операций;

5) доступ только к одному кортежу отношения без права изменения содержимого этого кортежа;

6) неограниченный доступ к атрибутам A_1, A_2,..., A_r отношения для всех типов операций и запрет доступа к остальным атрибутам отношения;

7) доступ только к атрибутам A_1, A_2,..., A_r отношения без права изменения их значений и запрет доступа к остальным атрибутам отношения;

8) доступ только к атрибутам A_1, A_2,..., A_r отношения с правом изменения значений только для атрибутов A_L,..., A_p (где $\{A_l,..., A_p\} \subset \{A_1, A_2,..., A_r\}$) и запрет доступа к остальным атрибутам отношения;

9) доступ в соответствии с п. 1, 3, 4, 5, 6, 7, 8, 9, но с ограничением по интервалу времени (с t_1 по t_2);

10) доступ в соответствии с п. 1, 3, 4, 5, 6, 7, 8, 9, но с разрешением изменения значений только в случае выполнения условий соответственно F_i на значения атрибутов (например, если значение атрибута не превышает некоторой величины N);

11) разрешение права применения вычислительных операторов (суммирование, вычитание и т.п.) к атрибутам A_1, A_2,..., A_r без права доступа к этим атрибутам или изменения их значений.

Приведенный список уровней доступа показывает требуемый диапазон работы и необходимую гибкость системы защиты данных общего назначения. Однако в настоящее время нет реальных систем, в которых бы были реализованы все эти возможности для защиты данных. Причиной является необходимость значительных затрат ресурсов системы (времен-

ных, аппаратных и других) на поддержание полной системы защиты данных.

Сочетание средств проверки полномочий и проверки подлинности – мощное оружие в борьбе за безопасность информационных систем и баз данных. Если все пользователи, работающие в интерактивном режиме или запускающие пакетные приложения, достаточно надежны и имеют допуск к максимально закрытой информации, хранимой в системе, то такая стратегия обеспечения безопасности может быть вполне адекватной.

Эта модель оказывается, однако, неудовлетворительной, если в учреждении необходимо организовать компьютерную среду с многоуровневой безопасностью.

4.2.6. Многоуровневая модель

Многоуровневая безопасность означает, что, во-первых, в вычислительной системе хранится информация, относящаяся к разным классам безопасности, и, во-вторых, часть пользователей не имеет доступа к информации, относящейся к высшему классу безопасности.

Современные информационные системы требуют другую, более изощренную схему безопасности – обязательный или принудительный контроль доступа (mandatory access control). Он основан на отказе от понятия владельца данных и опирается на так называемые метки безопасности (security labels), которые присваиваются данным при их создании. Каждая из меток соответствует некоторому уровню безопасности. Метки служат для классификации данных по уровням. Например, для правительственных и коммерческих организаций такая классификация выглядит следующим образом.

Правительственная

- совершенно секретно;
- секретно;
- конфиденциальная информация;
- неклассифицированная информация.

Другой пример относится к частной компании, где возможны такие уровни иерархии (сверху вниз):

- секретно;
- конфиденциально;
- для служебного пользования;
- для неограниченного распространения.

Так как данные расклассифицированы по уровням безопасности метками, конкретный пользователь получает ограниченный доступ к данным. Он может оперировать только с данными, расположенными на том уровне секретности, который соответствует его статусу. При этом он не является владельцем данных.

Эта схема безопасности опирается на механизм, позволяющий связать метки безопасности с каждой строкой любой таблицы в базе данных. Любой пользователь может потребовать в своем запросе отобразить любую таблицу из базы данных, однако увидит он только те строки, у которых метки безопасности не превышают уровень его компетенции.

Базы данных с многоуровневой безопасностью строятся обычно на основе модели Белла–ЛаПадула (Bell–LaPadula), которая предназначена для управления субъектами, т.е. активными процессами, запрашивающими доступ к информации, и объектами, т.е. файлами, представлениями, записями, полями или другими сущностями данной информационной модели.

Объекты подвергаются классификации, а каждый субъект причисляется к одному из уровней допуска (clearance) к классам объектов. Классы и уровни допуска совместно называются классами или уровнями доступа.

Класс доступа состоит из двух компонентов. Первый из них – это иерархический компонент. Второй компонент представляет собой некоторое множество неиерархических категорий, которые могут относиться к любому уровню иерархии.

Однако в модели Белла–ЛаПадула создается «решетка», где неиерархические компоненты каждого уровня иерархии автоматически приписываются к следующему более высокому уровню иерархии (так называемое «обратное наследование»). Эта структура показана на рис. 4.7.

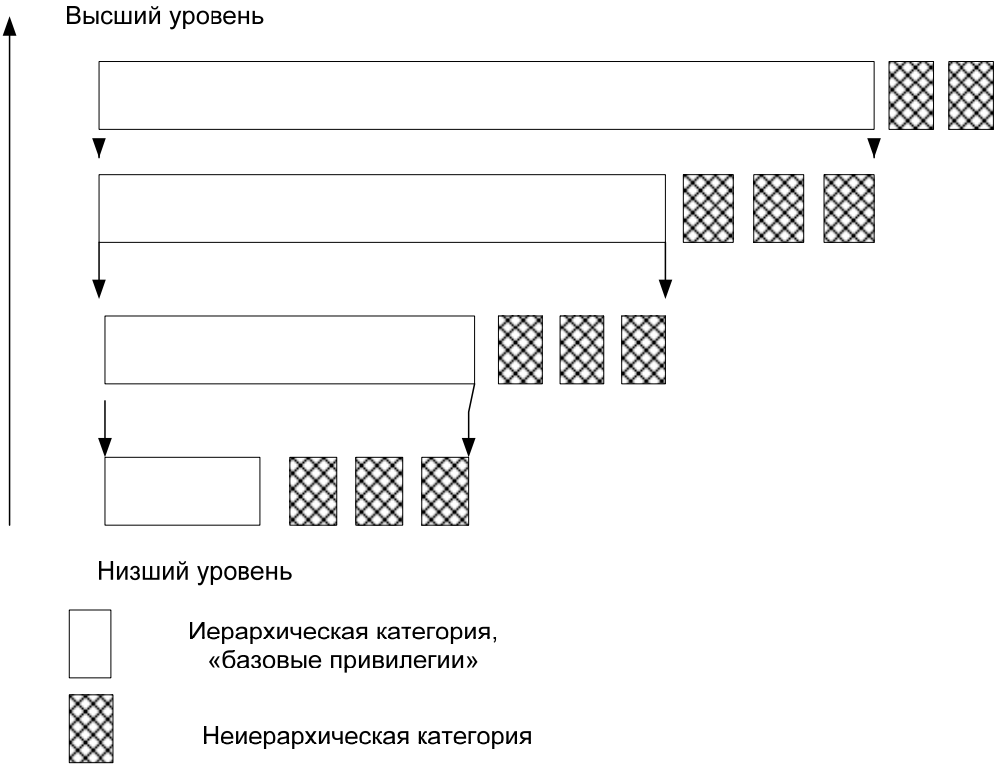


Рис. 4.7

До сих пор наше обсуждение касалось вполне очевидных понятий. Из него следует, что субъект уровня допуска CL1 имеет доступ на чтение

к объектам класса CL2, если CL2 не выше CL1. Например, пользователь с уровнем допуска «совершенно секретно» имеет доступ к объектам классов «совершенно секретно», «секретно», «конфиденциально» и «без грифа».

Менее очевидно другое свойство, называемое –свойством, которое позволяет субъекту иметь доступ на запись к объекту только в том случае, если уровень допуска этого субъекта такой же или более низкий, чем класс объекта – операнда операции записи. Это означает, что информация, принадлежащая какому-либо уровню, никогда не может быть записана в какой-либо объект, имеющий более низкий уровень, чем ее источник, поскольку это могло бы потенциально привести по неосторожности к разрушению классификации информации в рассматриваемой системе.

Принципы Белла – ЛаПадула сами по себе вполне здравые, но требование поддержки нескольких уровней безопасности в пределах одной таблицы (или в одной базе данных) сопряжено с рядом серьезных проблем.

4.2.7. Защита данных при статистической обработке

Процедуры статистической обработки позволяют получить агрегированную информацию о подмножествах некоторого множества объектов (вычисление сумм, получение средних и т.п.). В настоящем разделе рассматриваются процедуры статистической обработки, реализующие только вычислительные функции с арифметическими операциями сложения, вычитания, умножения и деления.

Для статистических процедур существуют свои специфические проблемы защиты данных, связанные с тем, что во многих случаях допускаются запросы типа «подсчитать средний возраст сотрудников отдела» и в то же время запрещается доступ к анкетным данным любого конкретного сотрудника отдела без специального разрешения.

Первым шагом в решении этой проблемы является введение в состав языка манипулирования данными специальных агрегативных функций для вычисления сумм и средних, которые должны применять пользователи в указанном выше случае. Тогда конкретные исходные данные попадают в рабочие поля агрегатных функций, а в рабочие поля прикладных программ поступает уже значение сумм и средних.

Однако применение агрегатных функций не решает вопрос полностью, поскольку, применяя одну и ту же функцию несколько раз, каждый раз несколько видоизменяя состав множества обсчитываемых объектов, можно затем получить путем сравнения результатов интересующее конкретное данное.

Рассмотрим базу данных, содержащую n записей. Пусть $V=\{V_1, V_2, ..., V_n\}$ – множество значений некоторого неключевого поля этих записей. Линейным запросом называется сумма

$$\sum_{i=1}^{n} C_i V_i,$$

где C_i – произвольные действительные числа. Наиболее важными случаями линейных запросов являются суммы по множеству записей S, когда

$$\begin{cases} C_i = 1, \text{ если запись } i \text{ принадлежит множеству } S, \\ C_i = 0, \text{ если запись } i \text{ не принадлежит множеству } S. \end{cases}$$

Существует следующая теорема. Пусть допускаются линейные запросы, продуцирующие по меньшей мере m элементов (т.е. обрабатывают m записей), и никакие два запроса не могут иметь более k общих элементов (т.е. k общих записей). Предположим, что ρ элементов уже известны (т.е. для ρ записей конкретные значения поля известны). Тогда для вычисления некоторого еще не известного элемента (значения поля в интересующей нас записи) необходимо сделать не менее $1+(m - 1 - \rho)/k$ запросов.

Если же ввести ограничения на структуру запросов, то в целом ряде случаев можно добиться исключения возможности раскрытия конкретных данных. Пусть ключ записи состоит из k полей; кроме того, предполагается, что в запросе допускается специфицировать не более S полей ключа (т.е. выполняется поиск по частичному соответствию ключа). Тогда, если $S < k$, никакая статистическая функция, использующая только операции сложения, вычитания, умножения и деления, не позволит определить значение данного конкретной записи.

Список литературы

1. Кагаловский М.Р. Технология баз данных на персональной ЭВМ. М.: Финансы и статистика ,1992. 224 с.

2. Гэри Хансен, Джеймс Хансен. Базы данных: разработка и управление: Пер. с англ. М.: ЗАО «Издательство БИНОМ», 1999. 704 с.

3. Боуман Джудит, Эмерсон Сандра, Дарновски Марси. Практическое руководство по SQL. Изд. 3-е: пер. с англ. К.: Диалектика, 1997. 320 с.

4. Саймон А.Р. Стратегические технологии баз данных: менеджмент на 2000 год: Пер. с англ./ Под ред. И с предисл. М.Р. Кагаловского. М.: Финансы и статистика, 1999. 479 с.

5. Базы даны: модели, разработка реализация / Т.С. Карпова. СПб.: Питер, 2001. 304 с.

6. Глеб Ладыженский. Системы управления базами данных – коротко о главном. http://www.jetinfo.ru/1995/3-5/1/article1.3-5.1995.html

7. Лилия Козленко. Информационная безопасность в современных системах управления базами данных / КомпьютерПресс. №3. 2002.

5. БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

При рассмотрении безопасности информационных систем обычно выделяют две группы проблем: безопасность компьютера и сетевую безопасность.

К *безопасности компьютера* относят все проблемы защиты данных, хранящихся и обрабатываемых компьютером, который рассматривается как автономная система. Эти проблемы решаются средствами операционных систем и приложений, таких как базы данных, серверы приложений и т.д., а так же встроенными аппаратными средствами компьютера.

Под *сетевой безопасностью* понимают все вопросы, связанные со взаимодействием устройств в сети. Это, прежде всего, защита данных в момент их передачи по линиям связи и защита от несанкционированного удаленного доступа в сеть.

Хотя проблемы компьютерной и сетевой безопасности трудно отделить друг от друга, настолько тесно они связаны, совершенно очевидно, что сетевая безопасность имеет свою специфику.

Компьютер, работающий в сети, по определению не может полностью отгородиться от мира, он должен общаться с другими компьютерами, возможно, даже удаленными от него на большое расстояние. Поэтому обеспечение безопасности сети является задачей значительно более сложной.

Помимо проблем, порождаемых возможностью удаленного входа в сетевые компьютеры, сети по своей природе подвержены еще одному виду угроз – перехвату и анализу сообщений, передаваемых по сети, а также созданию ложного объекта. Большая часть средств обеспечения сетевой безопасности направлена на предотвращение именно этих типов нарушений.

Вопросы сетевой безопасности приобретают особое значение при построении корпоративной сети на базе публичных сетей (таких как Интернет). Поставщики услуг публичных сетей пока редко обеспечивают защиту пользовательских данных при их транспортировке по своим магистралям, возлагая на пользователей заботы по обеспечению конфиденциальности, целостности и доступности информации и информационных ресурсов.

5.1. Основные термины и определения

Основные термины и определения взяты из федеральных законов и нормативных документов, регламентирующих защиту информации и информационных ресурсов.

Под **автоматизированной системой** (АС) обработки информации понимают организационно-техническую систему, представляющую 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;
- обслуживающего персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Частным случаем, такой АС является информационная система, построенная на базе корпоративной сети.

Для обеспечения информационной безопасности необходимо постоянно поддерживать следующие свойства информации и систем ее обработки:

доступность информации – такое свойство системы (инфраструктуры, средств и технологии обработки, в которой циркулирует информация), которое характеризует ее способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам (готовность к обслуживанию поступающих от субъектов) запросов всегда, когда в обращении к ним возникает необходимость;

конфиденциальность информации – такую субъективно определяемую (приписываемую) характеристику (свойство) информации, которая указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих прав на доступ к ней.

Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Под **безопасностью автоматизированной системы** (системы обработки информации, компьютерной системы) следует понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных, пользователей и персонала) от разного рода нежелательных воздействий.

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

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

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

Кроме того, необходимо дать определения таким понятиям как угрозы, уязвимости и атаки на компоненты АС.

Угроза – это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба.

Уязвимость – это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака – это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

5.2. Классификация сетей

С точки зрения информационной безопасности, для классификации компьютерных сетей наиболее целесообразно использовать критерий структуры, который позволяет выявить вероятное расположение злоумышленника, каналы утечки информации, объекты системы, подверженные негативному воздействию.

Данный критерий используется в нормативных документах по защите конфиденциальной информации и персональных данных, разработанных ФСТЭК России («Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)).

Согласно критерию структуры информационные системы (ИС), построенные на базе компьютерных сетей, можно разделить на следующие типы:

- ИС на базе автоматизированного рабочего места (АРМ), подключенного к сети общего пользования (к сети международного информационного обмена) – информационная система представляет собой выделенный компьютер, непосредственно подключенный к сети провайдера;
- ИС на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена) – информационная система представляет собой локальную сеть компьютеров, не имеющую подключения к публичным сетям (Интернет);
- ИС на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного об-

мена) – информационная система представляет собой локальную сеть компьютеров, имеющую подключение к публичным сетям (Интернет);

▪ИС на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена) – информационная система представляет собой соединение нескольких локальных сетей компьютеров с помощью выделенного канала связи и ни одна из них не имеет подключения к публичным сетям (Интернет);

▪ИС на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена) – информационная система представляет собой соединение нескольких локальных сетей компьютеров и хотя бы одна из них имеет подключение к публичным сетям (Интернет). Обычно данную конфигурацию информационной системы еще называют корпоративная сеть.

5.3. Типовая сеть крупной организации

В настоящее время корпоративные компьютерные сети играют важную роль в деятельности многих организаций.

Крупные организации имеют территориально распределенную структуру, в которой можно выделить центральный (головной) офис и филиалы. Типичной ситуацией является необходимость организации удаленного доступа к информационным ресурсам сети предприятия пользователей, находящихся в командировке. Нередки ситуации, когда сотрудники выполняют часть работы дома.

В общем случае можно выделить следующие элементы корпоративной сети:

- Подсеть центрального (головного) офиса;
- Подсети филиалов;
- Компьютеры удаленных пользователей и их домашние компьютеры.

Данные элементы соединяются посредством открытых сетей общего пользования, к которым относится и сеть Интернет.

Типичная конфигурация корпоративной сети представлена на рис. 5.1.

Подключаясь к публичным сетям (Интернет), организация преследует определённые цели и пытается эффективно решить следующие задачи:

- обеспечить внутренним пользователям доступ к внешним ресурсам. Это в первую очередь WWW – ресурсы, FTP – архивы, электронная почта и т.п.;
- предоставить доступ пользователям из внешней сети к некоторым внутренним ресурсам (корпоративному WEB-серверу, FTP-серверу и т.д.);
- обеспечить взаимодействие с удалёнными филиалами и отделениями;

• организовать доступ к ресурсам внутренней сети мобильных пользователей.

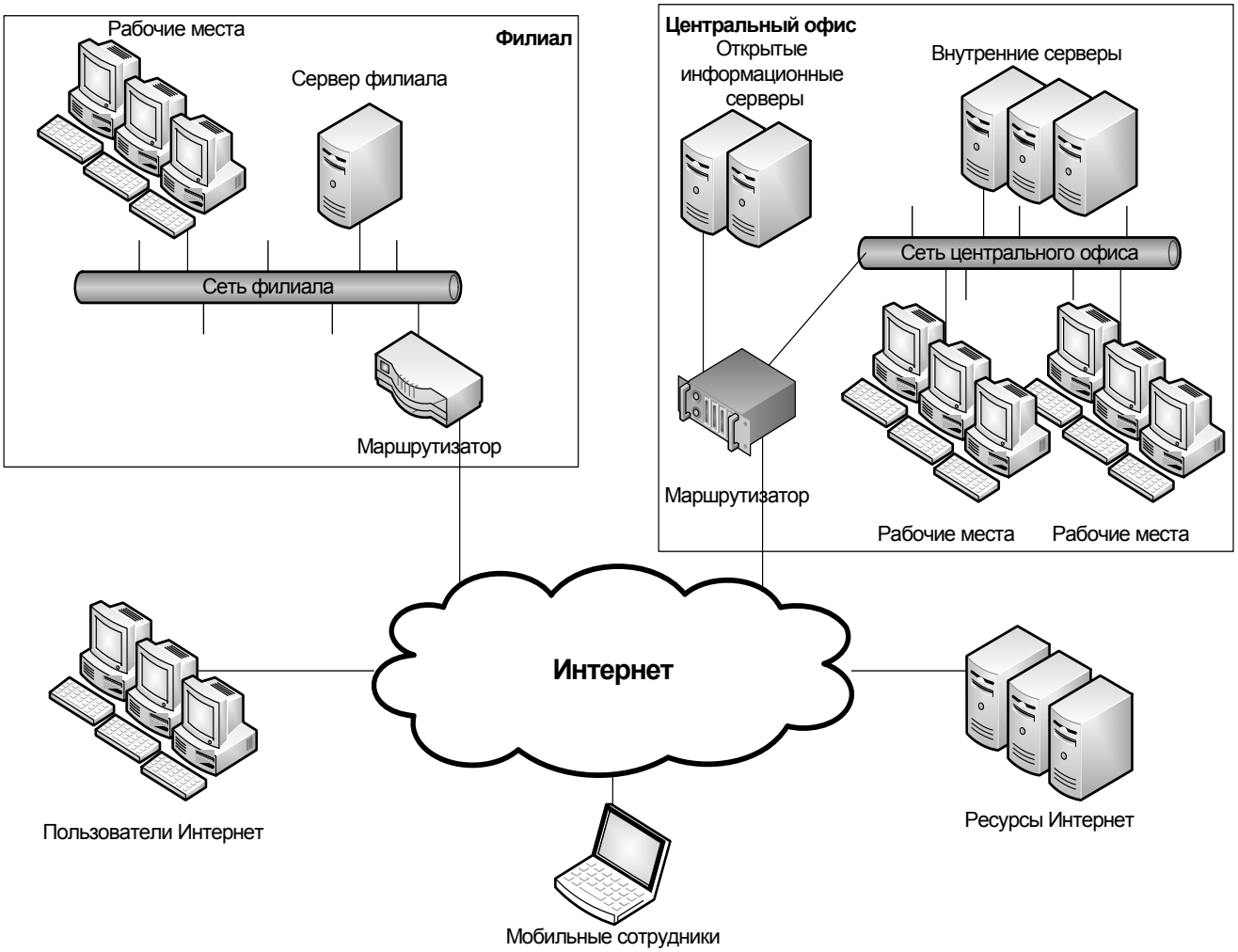


Рис. 5.1. Типовая структура корпоративной сети предприятия

Решая перечисленные задачи, организация сталкивается с рядом проблем, связанных с безопасностью. При взаимодействии с удалёнными филиалами и мобильными пользователями по открытым каналам возникает угроза перехвата передаваемой информации. Предоставление всеобщего доступа к внутренним ресурсам порождает угрозу внешних вторжений, имеющих целью получения конфиденциальной информации или выведение из строя узлов внутренней сети.

Сеть организации может быть либо изолированной от внешнего мира (что очень условно), либо может иметь соединение с сетями общего пользования, например с Интернет. В первом случае, проблемы безопасности связаны с нарушениями со стороны внутренних пользователей и обслуживающего персонала системы. Во втором случае, к внутренним нарушителям добавляются внешние.

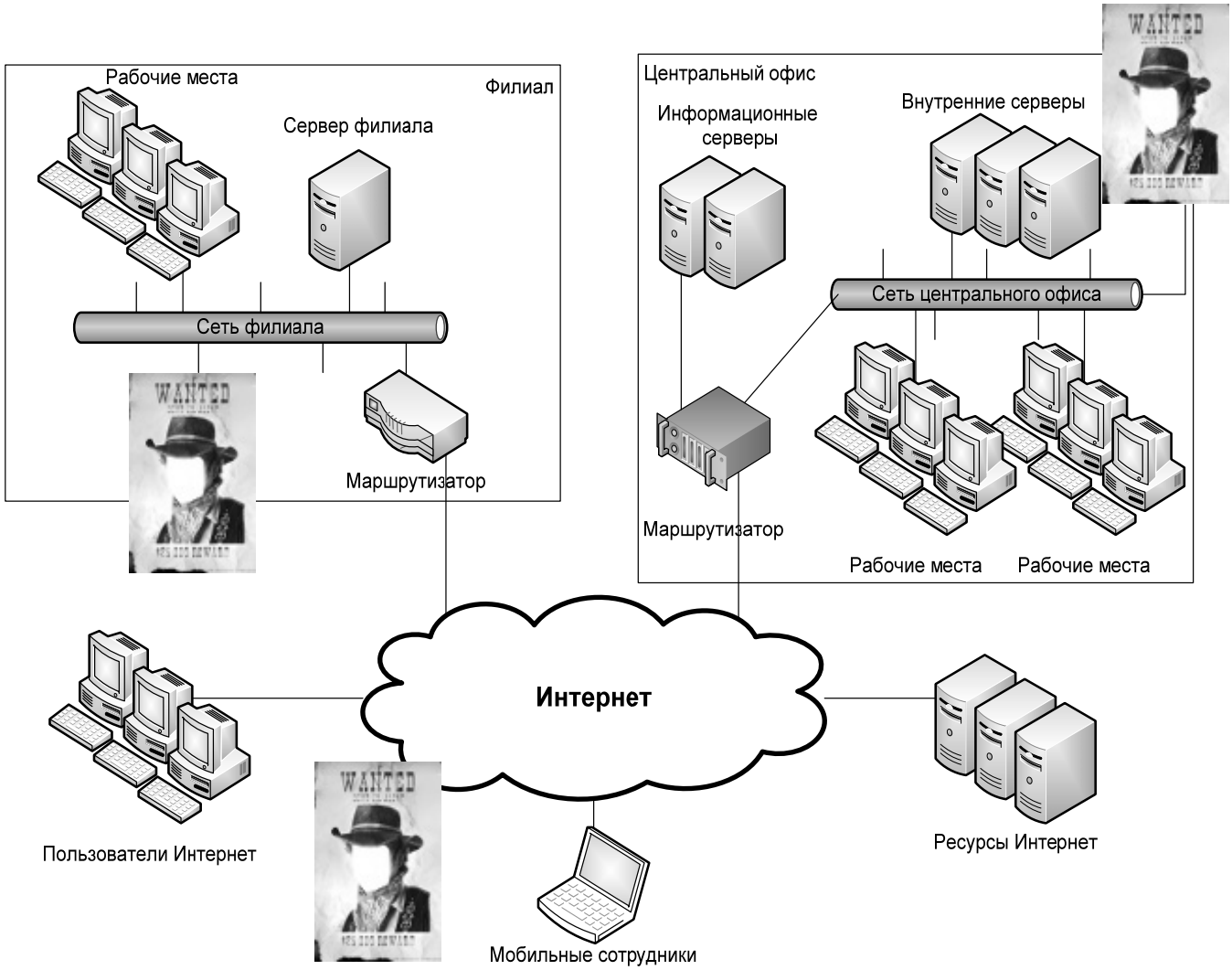


Рис. 5.2. Условное расположение внешних
и внутренних злоумышленников в структуре корпоративной сети

5.4. Уровни информационной инфраструктуры корпоративной сети

Информационная инфраструктура корпоративной сети содержит различные средства, которые решают конкретные задачи по обработке и/или передаче информации. Каждый элемент инфраструктуры обладает определенными уязвимостями, которые позволяют злоумышленнику проводить определенную разновидность атаки. Всю информационную инфраструктуру корпоративной сети можно разделить на несколько уровней:

- Уровень персонала;
- Уровень приложений;
- Уровень СУБД;
- Уровень операционных систем;
- Уровень сети.

К уровню сети относятся используемые сетевые протоколы (TCP/IP, NetBEUI, IPX/SPX), каждый из которых имеет свои особенности, уязвимости и связанные с ними возможные атаки.

К уровню операционных систем (ОС) относятся установленные на узлах корпоративной сети операционные системы (Windows, UNIX и т.д.).

В отдельный уровень выделяют системы управления базами данных (СУБД), так как они являются неотъемлемой часть любой корпоративной сети и предоставляют промежуточные функции по хранению и управлению данными.

На четвертом уровне находятся всевозможные приложения, используемые в корпоративной сети. Это может быть программное обеспечение Web-серверов, различные офисные приложения, браузеры и т.п.

На верхнем уровне информационной инфраструктуры находятся пользователи и обслуживающий персонал автоматизированной системы, которому присущи свои уязвимости с точки зрения безопасности.

5.5. Классификация угроз, уязвимостей, атак

5.5.1. Классификация угроз

Информационные системы подвержены широком у кругу угроз.

Все угрозы условно можно разделить на две большие группы: угрозы утечки информации по техническим каналам связи и угрозы несанкционированного доступа к информации.

Первая группа угроз включает в себя угрозы утечки акустической (речевой), видовой информации, а так же утечки по каналу ПЭМИН.

Вторая группа угроз характеризуется различными способами реализации несанкционированного получения доступа к информации, в том числе с использованием возможностей компьютерных сетей.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности АС, насчитывающий сотни пунктов. Наиболее характерные и часто реализуемые из них следующие:

- несанкционированное копирование носителей информации;
- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
- игнорирование организационных ограничений (установленных правил) при определении ранга системы.

Классификация всех возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков.

По природе возникновения:

- Естественные угрозы – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

• Искусственные угрозы – угрозы информационной безопасности АС, вызванные деятельностью человека.

По степени преднамеренности проявления:

• Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.

• Угрозы преднамеренного действия.

По непосредственному источнику угроз:

• Угрозы, непосредственным источником которых является природная среда.

• Угрозы, непосредственным источником которых является человек.

• Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.

• Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства.

По положению источника угроз:

• Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС.

• Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС.

• Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).

• Угрозы, источник которых расположен в АС.

По степени зависимости от активности АС:

• Угрозы, которые могут проявляться независимо от активности АС.

• Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных.

По степени воздействия на АС:

• Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС.

• Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС.

По этапам доступа пользователей или программ к ресурсам АС:

• Угрозы, которые могут проявляться на этапе доступа к ресурсам АС.

• Угрозы, которые могут проявляться после разрешения доступа к ресурсам.

По способу доступа к ресурсам АС:

• Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС.

• Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС.

По текущему месту расположения информации, хранимой и обрабатываемой в АС:

- Угрозы доступа к информации на внешних запоминающих устройствах.
- Угрозы доступа к информации в оперативной памяти.
- Угрозы доступа к информации, циркулирующей в линиях связи.
- Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере.

В соответствии с существующими подходами, принято считать, что информационная безопасность АС обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности (невозможности несанкционированного получения какой-либо информации), целостности (невозможности несанкционированной или случайной ее модификации) и доступности (возможности за разумное время получить требуемую информацию). Соответственно для автоматизированных систем было предложено рассматривать три основных вида угроз:

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

В информационных системах на базе автономного АРМ, а так же в ИС не имеющих подключения к сетям общего пользования, угрозы воз-

никают в связи с действиями нарушителя, имеющего доступ в ИС, т.е. внутреннего нарушителя.

В ИС, имеющих подключение к сетям общего пользования, угрозы возникают в связи с действиями нарушителя, как имеющего доступ в ИС, так и не имеющего такового доступа, т.е. к внутренним нарушителям добавляются внешние.

В ИС на базе автономного АРМ возможны все виды угроз, за исключением угроз, связанных с реализацией протоколов сетевого взаимодействия и каналов передачи данных.

В ИС на базе локальных, распределенных сетей, а так же имеющих подключение к сетям общего пользования дополнительно возникают угрозы, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных.

Например, для распределенных ИС, имеющих подключение к сетям общего пользования, возможна реализация следующих угроз:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИС и принимаемой в ИС из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы внедрения ложного объекта как в информационной системе, так и во внешних сетях;
- угрозы подмены доверенного объекта;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

5.5.2. Классификация уязвимостей

Из приведенных выше определений угроз, уязвимостей и атак видно, что производя определенную атаку, нарушитель обязательно использует некоторую уязвимость информационной системы. Иначе говоря, если нет уязвимости, то невозможна и атака, её использующая. Поэтому одним из важнейших механизмов защиты является процесс поиска и устранения уязвимостей информационной системы.

Прежде всего, рассмотрим возможные варианты (критерии) классификации уязвимостей IP-сетей. Такая классификация нужна, например,

для создания упорядоченной базы данных уязвимостей, которая может пополняться по мере обнаружения новых уязвимостей.

Источники возникновения уязвимостей

Часть уязвимостей закладывается ещё на этапе проектирования. В качестве примера можно привести сервис TELNET, в котором имя пользователя и пароль передаются по сети в открытом виде. Это явный недостаток, заложенный на этапе проектирования. Некоторые уязвимости подобного рода трудно назвать недостатками, скорее это особенности проектирования. Например, особенность технологии Ethernet – общая среда передачи.

Другая часть уязвимостей возникает на этапе реализации (программирования). К таким уязвимостям относятся, например, ошибки программирования стека TCP/IP, приводящие к отказу в обслуживании. Сюда же следует отнести и ошибки при написании приложений, приводящие к переполнению буфера и т.п.

И, наконец, уязвимости могут быть следствием ошибок, допущенных в процессе эксплуатации информационной системы. Сюда относятся неверное конфигурирование операционных систем, протоколов и служб, использование нестойких паролей пользователей, паролей учетных записей «по умолчанию» и др.

Классификация уязвимостей по уровню в инфраструктуре АС

Следующий вариант классификации уязвимостей – по их уровню в информационной инфраструктуре организации. Это наиболее наглядный вариант классификации, т. к. он показывает, что конкретно уязвимо.

- К *уровню сети* относятся уязвимости сетевых протоколов – стека TCP/IP, протоколов NetBEUI, IPX/SPX (например, аутентификация узлов на основе назначаемого ip-адреса в протоколе IP).
- *Уровень операционной системы* охватывает уязвимости Windows, UNIX, Novell и т.д., т.е. конкретной операционной системы.
- *На уровне баз данных* находятся уязвимости конкретных СУБД – Oracle, MS SQL, Sybase и др.
- К *уровню приложений* относятся уязвимости программного обеспечения WEB, SMTP серверов, клиентских программ и т.п.
- *Персонал и пользователи системы* также уязвимы. Например, один из путей внедрения вредоносных программ – это провоцирование пользователей на запуск присланных по электронной почте приложений.

Классификация уязвимостей по степени риска

Этот вариант (критерий) классификации уязвимостей является достаточно субъективным (условным). Если придерживаться взгляда компании Internet Security Systems, можно выделить уязвимости трех уровней риска:

- *Высокий уровень риска* – уязвимости, позволяющие атакующему получить непосредственный доступ к узлу с правами суперпользователя

или в обход межсетевых экранов или иных средств защиты (полный контроль над атакуемым объектом).

- *Средний уровень риска* – Уязвимости, позволяющие атакующему получить информацию, которая с высокой степенью вероятности позволит в дальнейшем получить полный контроль над объектом и доступ к любым его ресурсам.
- *Низкий уровень риска* – Уязвимости, позволяющие злоумышленнику осуществлять сбор критичной информации о системе.

5.5.3. Классификация атак

Также как и уязвимости, атаки можно классифицировать по различным признакам.

Наиболее важно для понимания сути происходящих атак представлять механизмы их реализации. Основными механизмами реализации атак являются:

- *пассивное прослушивание* – состоит в перехвате трафика сетевого сегмента
- *подозрительная активность* – сканирование портов (служб) объекта атаки, попытки подбора пароля
- *бесполезное расходование вычислительного ресурса* – исчерпание ресурсов атакуемого узла или группы узлов, приводящее к снижению производительности, зависанию службы или операционной системы (переполнение очереди запросов на соединение и т п.)
- *нарушение навигации* (создание ложных объектов и маршрутов) – изменение маршрута сетевых пакетов, таким образом, чтобы они проходили через хосты и маршрутизаторы нарушителя, изменение таблиц соответствия условных Internet-имен и IP-адресов (атаки на DNS) и т.п.
- *выведение из строя* – посылка пакетов определённого типа на атакуемый узел, приводящая к отказу узла или работающей на нём службы (WinNuke и др.)
- *запуск приложений на объекте атаки* – выполнение враждебной программы в оперативной памяти объекта атаки (троянские кони, передача управления враждебной программе путём переполнения буфера, исполнение вредоносного мобильного кода на Java или ActiveX и др.)

Информацию об известных и новых обнаруживаемых уязвимостях можно найти в сети Интернет на сайтах, таких как:

Иностранные:

www.iss.net – компания Internet Security Systems;

www.cert.org – координационный центр CERT;

www.sans.org – институт системного администрирования, сетевых технологий и защиты;

www.ciae.org – группа реагирования на инциденты в области компьютерной безопасности;

www.securityfocus.com – информация об обнаруженных уязвимостях с подробными пояснениями и группой новостей и др.;

osvdb.org – открытая база данных уязвимостей.

Отечественные:

www.sreport.ru – база данных уязвимостей Интернет-серверов;

www.securitylab.ru – информация об уязвимостях различного системного и прикладного программного обеспечения.

Common Vulnerabilities and Exposures (CVE) – это список стандартных названий для общеизвестных уязвимостей. Основное назначение CVE – это согласование различных баз данных уязвимостей и инструментов, использующих такие базы данных. Например, одна и та же уязвимость может иметь различные названия в базе данных Internet Scanner и CyberCop Scanner . Появление CVE – это результат совместных усилий известных мировых лидеров в области информационной безопасности: институтов, производителей ПО и т.д. Поддержку CVE осуществляет MITRE Corporation (www.mitre.org).

Процесс получения индекса CVE (CVE entry) начинается с обнаружения уязвимости. Затем уязвимости присваивается статус кандидата CVE и соответствующий номер (CVE candidate number). После этого происходит обсуждение кандидатуры при помощи CVE Editorial Board и вынесение решения о получении или неполучении индекса CVE .

Подробнее узнать о CVE и получить список **CVE entry** можно по адресу: **http://cve.mitre.org/cve** .

5.6. Защитные механизмы и контрмеры

Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и несанкционированного доступа (НСД) к информации используются различные методы и средства защиты (защитные механизмы). Некоторые из них используются исключительно в информационных системах, построенных на базе компьютерных сетей. Другие могут применяться как для защиты узла сети, так и для автономного АРМ. Основными методами и средствами защиты являются:

- **идентификация** (именование и опознавание) и **аутентификация** (подтверждение подлинности) субъектов (пользователей) и объектов (ресурсов, компонентов, служб) системы;
- **разграничение доступа** пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- **регистрация и оперативное оповещение** о событиях, происходящих в системе и имеющих отношение к безопасности;

- **криптографическое закрытие** хранимых и передаваемых по каналам связи данных;
- **контроль целостности и аутентичности** (подлинности и авторства) передаваемых и хранимых данных;
- **изоляция (защита периметра) компьютерных сетей** (фильтрация трафика, скрытие внутренней структуры и адресации путем трансляции адресов);
- **контроль вложений** (выявление компьютерных вирусов, вредоносных кодов и их нейтрализация);
- **выявление уязвимостей** (слабых мест) системы;
- **обнаружение и противодействие атакам** (опасным действиям нарушителей).

Перечисленные механизмы защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты (организационными и техническими мерами защиты).

В зависимости от класса информационной системы в состав мероприятий по защите информации от НСД и неправомерных действий входят следующие мероприятия:

- защита от НСД при однопользовательском режиме обработки;
- защита от НСД при многопользовательском режиме обработки и равных правах доступа к ним субъектов доступа;
- защита от НСД при многопользовательском режиме обработки и разных правах доступа;
- защита информации при межсетевом взаимодействии информационных систем;
- антивирусная защита;
- обнаружение вторжений.

Мероприятия по защите данных реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты, обнаружения вторжений.

Мероприятия по обнаружению вторжений в информационных системах проводятся в соответствии с требованиями нормативных документов Федеральной службы безопасности Российской Федерации.

Кроме этого, в ИС выше определенного класса должен проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения.

В информационных системах должны использоваться только сертифицированные по требованиям безопасности информации технические средства и системы защиты.

5.6.1. Средства анализа защищенности сетей

Перед подразделениями защиты информации и управлениями автоматизации организации периодически возникает задача проверки, насколько реализованные или используемые механизмы защиты соответствуют положениям принятой в организации политики безопасности.

Контроль эффективности защиты осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации или нарушение нормального функционирования средств обработки и передачи информации.

Средства анализа защищенности, так называемые сканеры безопасности (security scanners), помогают определить факт наличия уязвимости на узлах корпоративной сети и своевременно устранить их (до того, как ими воспользуются злоумышленники).

Средства анализа защищенности выполняют серию тестов по обнаружению уязвимостей, аналогичных тем, которые применяют злоумышленники при подготовке и осуществлении атак на корпоративные сети. Поиск уязвимостей основывается на использовании базы данных, которая содержит признаки известных уязвимостей сетевых сервисных программ и может обновляться путем добавления новых описаний уязвимостей. Сканирование начинается с получения предварительной информации о системе, например, о разрешенных протоколах и открытых портах, о версиях операционных систем и т.п., и может заканчиваться попытками имитации проникновения, используя широко известные атаки, например, подбор пароля методом «грубой силы» («brute force»).

Применяя средства анализа защищенности можно быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в ней сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). Эти средства также вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные уязвимости (слабые места в защите) системы.

Функционировать такие средства могут на сетевом уровне, уровне операционной системы (ОС) или на уровне приложения.

Средства анализа защищенности сетевых сервисов (служб)

Наибольшее распространение получили средства анализа защищенности сетевых сервисов (служб) и протоколов. Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и т.п. позволяют с высокой степенью эффективности проверять

защищенность информационной системы, работающей в сетевом окружении.

Использование в сетях Internet/Intranet протоколов TCP/IP, которые характеризуются наличием в них неустранимых уязвимостей, привело к появлению в последнее время новых разновидностей информационных воздействий на сетевые службы и представляющих реальную угрозу защищенности информации. Средства анализа защищенности сетевых служб применяются для оценки защищенности компьютерных сетей по отношению к внутренним и внешним атакам. По результатам анализа защищенности сетевых сервисов этими средствами генерируются отчеты, включающие в себя список обнаруженных уязвимостей, описание связанных с ними возможных угроз и рекомендации по их устранению.

Типичная схема проведения анализа защищенности (на примере системы Internet Scanner) приведена на рис. 5.3.

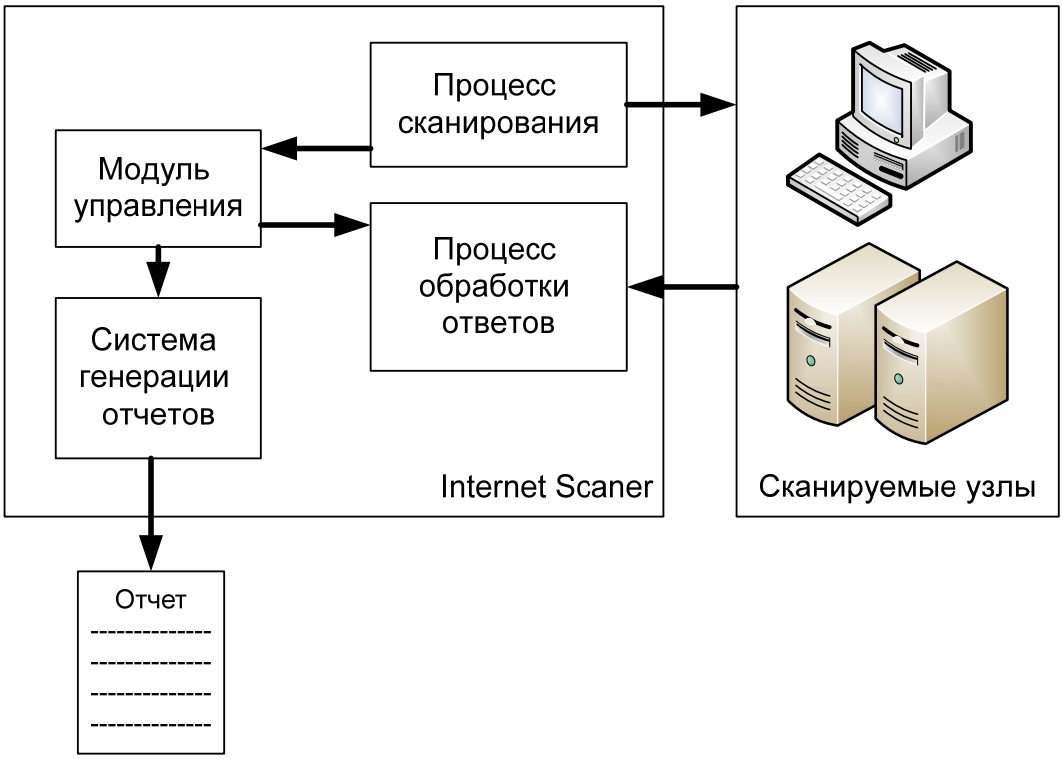


Рис. 5.3. Схема анализа защищенности сети
на примере системы Internet Scaner

К числу средств анализа данного класса относится программа SATAN (автор В.Венема), Netprobe фирмы Qualix Group и Internet Scanner фирмы Internet Security System Inc. Другие известные сканеры: NESSUS, XSpider, LanGuard, ShadowSecurityScanner, X-Scan.

Средства анализа защищенности операционных систем

Вторыми по распространенности являются средства анализа защищенности операционных систем (например, UNIX и Windows NT). Однако, из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей

ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь общие параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры.

Средства этого класса предназначены для проверки настроек операционных систем, влияющих на их защищенность. К таким настройкам можно отнести параметры учетных записей пользователей (account), например длину пароля и срок его действия, права пользователей на доступ к критичным системным файлам, уязвимые системные файлы, установленные patch'и («заплаты») и т.п.

Данные системы в отличие от средств анализа защищенности сетевого уровня проводят сканирование не снаружи, а изнутри анализируемой системы и не предполагают имитацию атак внешних злоумышленников. Кроме возможностей по обнаружению уязвимостей некоторые системы анализа защищенности на уровне ОС (например, System Scanner компании Internet Security Systems) позволяют автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в организации.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек правилам, установленным в организации.

Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей. Системы анализа защищенности на уровне ОС могут быть использованы не только отделами защиты информации, но и управлениями автоматизации для контроля конфигурации операционных систем.

К числу средств анализа данного класса относятся:

- программное средство администратора ОС Solaris ASET (Automated Security Tool), которое входит в состав ОС Solaris;
- пакет программ COPS (Computer Oracle and Password System) для администраторов Unix-систем;
- система System Scanner (SS) фирмы Internet Security System Inc. для анализа и управления защищенность операционных систем Unix и Windows;
- Microsoft Baseline Security Analyzer (MBSA) – простое средство для определения состояния безопасности операционной системы и других программных продуктов в соответствии с рекомендациями Microsoft.

Средства анализа защищенности приложений

Средств анализа защищенности приложений на сегодняшний день не так много, как этого хотелось бы. Возможности по анализу защищенности приложении частично реализованы как в системах анализа сетевых сервисов, так и в системах анализа операционной системы (для широко распространенных прикладных систем, типа Web-браузеров – Netscape Navigator, Microsoft Internet Explorer и т.п.). Из средств, которые предназначены исключительно для анализа защищенности приложений, можно назвать, Database Scanner компании Internet Security Systems, предназначенный для проверки целостности, прав доступа, подсистемы аутентификации и т.п. в СУБД Microsoft SQL Server, Sybase и Oracle.

5.6.2. Средства обнаружения атак

В последнее время сообщения о проникновении в корпоративные сети и атаках на Web, FTP, почтовые и другие сервера появляются с ужасающей частотой. Злоумышленники преодолевают установленные в организациях защитные средства (системы аутентификации, межсетевые экраны и т.д.), установленные для разграничения доступа к ресурсам корпоративной сети. С ростом квалификации злоумышленники становятся более изощренными в разработке и применении методов проникновения за защитную преграду.

Обнаружить таких злоумышленников очень трудно. Они маскируются под авторизованных пользователей, используют промежуточные узлы для сокрытия своего истинного адреса, осуществляют атаки, распределенные во времени (в течение нескольких часов) и пространстве (одновременно с нескольких узлов) и т.д. Некоторые атаки значительно «растянуты» во времени, другие осуществляются за очень короткое время (минуты и даже секунды), что также не позволяет обнаружить и предотвратить их стандартными защитными средствами. Необходимы динамические методы, позволяющие обнаруживать, оперативно реагировать и предотвращать нарушения безопасности.

Одной из технологий, которая может быть применена для обнаружения нарушений, является технология обнаружения атак (intrusion detection).

Средства обнаружения атак (Intrusion Detection Tools) в сетях предназначены для осуществления оперативного (в реальном времени) контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирования при обнаружении признаков атак (нападений на узлы и устройства корпоративной сети).

Системы обнаружения вторжений строятся с учетом особенностей реализации атак, этапов их развития и основаны на целом ряде методов обнаружения атак.

Выделяют три группы методов обнаружения атак:

- сигнатурные методы;
- методы выявления аномалий;
- комбинированные методы (использующие совместно алгоритмы, определенные в сигнатурных методах и методах выявления аномалий).

Сигнатурные методы выявления атак основаны на том, что большинство возможных сетевых атак известны и развиваются по схожим сценариям. Система обнаружения атак может обнаружить признаки атаки сравнивая параметры и содержимое каждого пакета с некоторой базой данных сигнатур, после чего принимает решение.

Метод выявления аномалий базируется на сравнении так называемого профиля нормального поведения пользователя с реальным поведением. При этом могут выявляться аномалии в сигнатурах атак (отклонения от известных сигнатур), выявляемые статистическими методами, аномалии трафика (например, в интенсивности передачи пакетов данных с определенным сетевым адресом отправителя), выявляемые как обычными статистическим методами, так и специфическими методами, основанными, например, на использовании аппарата нейронных сетей, аномалии в служебных данных, вызванные ошибками нарушителя и др. При использовании данного метода предполагается, что отклонение от нормального поведения является подозрительным и может быть оценено как признак атаки.

Системы обнаружения вторжений являются модульными продуктами, части которых устанавливаются на различных узлах сети. На рабочем месте администратора, как правило, устанавливаются средства администрирования и мониторинга системы обнаружения вторжений. На остальных узлах сети устанавливаются так называемые «агенты», которые осуществляют сбор и первичную обработку данных. В зависимости от преследуемых целей агенты системы обнаружения вторжений могут устанавливаться в демилитаризованной зоне, на ключевых сегментах корпоративной сети или «снаружи» за межсетевым экраном.

5.6.3. Сетевые анализаторы и «снифферы»

Главный недостаток сетевых технологий – незащищённость передаваемой информации. Метод доступа, положенный в основу этой технологии, требует от узлов, подключённых к сети, непрерывного прослушивания всего сетевого трафика. Это означает, что узлы такой сети могут перехватывать информацию, адресованную свои соседям. Данная уязвимость технологий делает возможным проведение атак, использующих механизм «пассивного прослушивания». Средства для проведения таких атак – это **анализаторы протоколов** или **снифферы**.

Термин «сниффер» («нюхач») впервые был использован компанией Network Associates в названии известного продукта «Sniffer (r) Network Analyzer». В самом общем смысле слово «сниффер» обозначает устройство, подключенное к компьютерной сети и записывающее весь ее трафик подобно телефонным «жучкам», записывающим телефонные разговоры. Однако чаще всего «снифферoм» называют программу, запущенную на подключенном к сети узле и просматривающую весь трафик сетевого сегмента.

Работа «сниффера» использует основной принцип технологии Ethernet – общую среду передачи. Это означает, что любое устройство, подключенное к сетевому сегменту, может слышать и принимать все сообщения, в том числе предназначенные не ему. Сетевые адаптеры Ethernet могут работать в двух режимах: селективном (non-promiscuous) и неселективном (promiscuous). В первом случае, принимаются только сообщения, предназначенные данному узлу. Фильтрация осуществляется на основе MAC-адреса фрейма. Во втором случае фильтрация не осуществляется и узел принимает все фреймы, передаваемые по сегменту.

Специализированные программы, переводящие сетевой адаптер в неселективный режим и собирающие весь трафик сети для последующего анализа, называются анализаторами протоколов или «снифферами». Собранный трафик сегмента может быть отображен на экране, записан в файл и т.п. Так как компьютеры обмениваются по сети двоичной информацией, в обязанности «сниффера» обычно входит расшифровка (декодирование) и вывод информации в удобном (читаемом) виде.

Анализатор протоколов – программный продукт «двойного» применения. Он может быть использован специалистами и администраторами сетей для анализа происходящих в сети процессов и диагностики неисправностей. С другой стороны, снифферы используются злоумышленниками для проведения атак (механизм атаки – «пассивное прослушивание»). Кроме того, тот же принцип пассивного прослушивания трафика лежит в основе работы средств обнаружения атак.

Анализаторы протоколов могут перехватывать сообщения только внутри сегмента, в котором они находятся. Для «межсегментной» атаки используются методы, позволяющие перенаправить трафик из другого сегмента на узел нарушителя и реализующие атаки типа «создание ложного объекта-посредника» на сетевом и транспортном уровнях модели OSI.

В сети Internet можно найти множество анализаторов протоколов для различных операционных систем. Для операционных систем семейства Windows одним из лучших является анализатор протоколов «SnifferPro» компании Network Associates (www.nai.com). Кроме огромного количества функций по перехвату пакетов, он поддерживает и возможность генерации пакетов.

Анализатор протоколов Network Monitor входит в состав операционной системы Windows Server. Однако он позволяет просматривать не весь трафик, а только его часть, относящуюся к узлу, на котором он установлен. Полнофункциональная версия Network Monitor входит в состав System Management Server и обладает всеми возможностями классических анализаторов протоколов.

В некоторых случаях программы, осуществляющие перехват сообщений на более высоких уровнях сетевого взаимодействия, так же называют снифферами. Такие программы могут собирать статистические данные о работе сети, перехватывать сообщения IM систем (ICQ и др.), перехватывать сообщения с паролями пользователей в различных службах и т.д.

Меры защиты от «снифферов» следуют из принципа их работы и цели атак:

• **Шифрование информации**. Так как целью прослушивания обычно является перехват критичной (конфиденциальной) информации, то эта мера защиты сделает невозможным последующий анализ перехваченных данных.

• **Построение сетей на основе интеллектуальных коммутаторов (switches).** Это аппаратное решение проблемы, сводящее к минимуму «общую среду передачи». При использовании коммутаторов можно обеспечить режим, когда каждая рабочая станция будет работать на своем отдельном сегменте.

• **Использование сетевых адаптеров, не поддерживающих неселективный режим.** Некоторые из сетевых адаптеров не поддерживают неселективный режим на аппаратном уровне, другие снабжаются драйвером, не допускающим работу в неселективном режиме.

• **Обнаружение несанкционированно используемых на компьютерах анализаторов протоколов.** Как было указано выше, обнаружить сниффер достаточно сложно. Однако существуют программные средства, разработанные для этой цели – антиснифферы. В качестве примера можно привести программный продукт Antisniff компании Lopht.

Обнаружение снифферов

Так как сниффер – это пассивное устройство, обнаружить его достаточно сложно. Обычно присутствие сниффера можно обнаружить по каким-либо косвенным признакам, свойственным конкретному снифферу, или по неселективному режиму работы сетевой карты на узле.

Самый известный инструмент для обнаружения снифферов – утилита AntiSniff от компании Lopht Heavy Industries. Текущая версия программы работает в среде Windows и позволяет обнаружить в сетевом сегменте адаптер, работающий в неселективном режиме.

Другой программой данного класса является PromiScan – инструмент Windows 2000, который помогает системным администраторам найти снифферы в локальной сети.

5.6.4. Протокол разрешения адресов ARP

Протокол разрешения адресов ARP описан в документе RFC 826. Необходимость протокола ARP продиктована тем обстоятельством, что IP-адреса узлов сети назначаются независимо от их физических (MAC) адресов. Поэтому для доставки сообщений по сети нужен механизм, устанавливающий соответствие между физическим (MAC) адресом узла и его IP-адресом.

В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом. Результаты запросов заносятся в специальную ARP-таблицу, которая используется впоследствии для сокращения количества широковещательных запросов.

Атаки на протокол ARP:

Посылка ложного ARP;

ARP-Spoofing.

Меры защиты от атак на протокол ARP Атаки, связанные с уязвимостями протокола ARP являются внутрисегментными и поэтому представляет угрозу для пользователя только в случае нахождения атакующего внутри сегмента сети. Однако, по статистике нарушений информационной безопасности, большинство взломов сетей выполняется изнутри сотрудниками организаций. Защиты от атак на протокол ARP в общем случае не существует, т.к. используемые уязвимости являются по сути особенностями работы технологии Ethernet (широковещательность).

Однако, можно порекомендовать следующее:

- нарушителя нужно искать внутри сетевого сегмента атакуемого объекта;
- полезно вести таблицу соответствия MAC-адресов и IP-адресов, которую следует периодически обновлять;
- использовать статические записи в таблице ARP хотя бы для наиболее важных узлов сети.

5.6.5. Безопасность сетевого уровня

Основное назначение сетевого уровня – маршрутизация или обеспечение связи различных (в том числе разнородных) сетей. Основу стека протоколов TCP/IP составляет протокол межсетевого взаимодействия – Internet Protocol (IP). К основным функциям протокола IP относятся:

- перенос между сетями различных типов адресной информации в унифицированной форме,
- сборка и разборка пакетов при передаче их между сетями с различным максимальным значением длины пакета.

Большинство атак на протокол IP направлены на противодействие корректному выполнению данных функций. К таким атакам относятся Address Masquerading (Адресный маскарад), Address Spoofing (подделка адреса) и ошибки фрагментации.

Address Masquerading

На рис. 5.4 нарушитель, дождавшись отключения легального NFS-клиента, присваивает себе его IP-адрес.

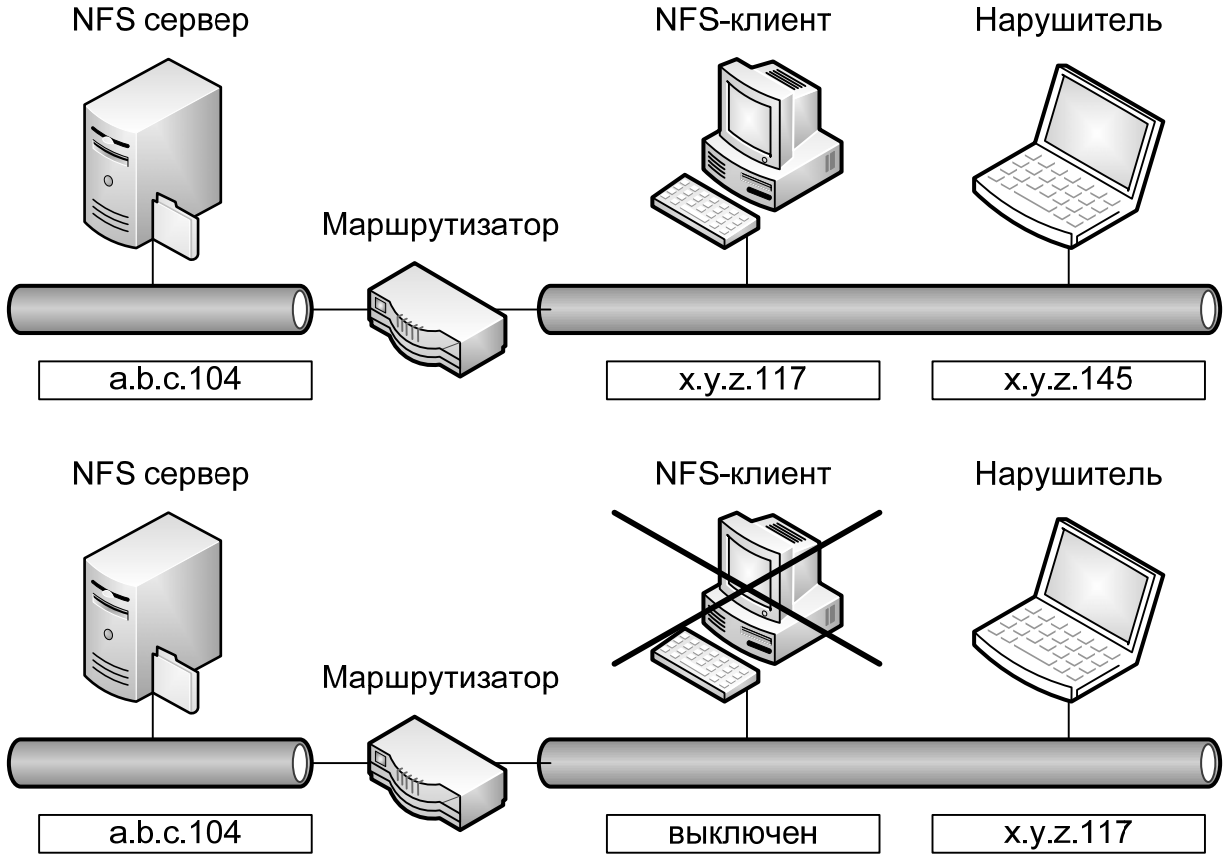


Рис. 5.4. Схема проведения атаки Address Masquerading

Аутентификация (подтверждение подлинности) на уровне IP относится к компьютерам, а не к пользователям. Поскольку IP-адрес конфигурируется программно, обычно бывает легко задать для узла другой IP-адрес, так что узел будет корректно работать в сети. Если аутентификация осуществляется по IP-адресу узла, это позволит атакующему получить доступ к ресурсам, к которым он при обычных условиях доступа иметь не должен. Такое действие называется Address Masquerading (Адресный маскарад). Протоколы прикладного уровня, как например, Network File System (NFS) могут быть уязвимыми к подобного рода атакам, если нет дополнительной аутентификации на основе имени и пароля пользователя.

Address Spoofing

Address Spoofing в простейшем варианте представляет собой замену адреса отправителя или получателя пакета и отправку такого пакета в сеть.

Средства программирования под UNIX позволяют легко манипулировать сетевыми пакетами, например, формировать их заголовки. В качестве примера можно привести известную утилиту **Nmap**, некоторые режимы которой позволяют задать поддельные адреса отправителя пакетов. Стандартными средствами Windows это осуществить несколько сложнее.

Ошибки фрагментации

Большое количество атак на протокол IP связано с одной из его функций – фрагментацией. Посылка специфических пакетов, где определённым образом заполнены поля заголовка, отвечающие за фрагментацию, может приводить к зависанию или понижению производительности узла. Как правило, используемыми уязвимостями во всех случаях являются ошибки реализации. Исправление этих ошибок – это установка пакетов обновления программного обеспечения.

5.6.6. Межсетевые экраны

Для осуществления разграничения доступа к ресурсам информационной системы при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран находится в составе защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Межсетевые экраны (МСЭ) занимают важное место в комплексе средств обеспечения безопасности корпоративной сети. Иногда используются термины «брандмауэр» или «firewall». Согласно документу «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации» Гостехкомиссии при Президенте РФ, межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т.е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе.

Чаще всего основным назначением МСЭ является воплощение политики безопасности, принятой в организации в вопросах обмена информацией с внешним миром.

МСЭ как средство обеспечения безопасности, реализует следующие механизмы защиты:

- трансляция адресов для сокрытия структуры и адресации внутренней сети;
- фильтрация проходящего трафика;
- управление списками доступа на маршрутизаторах;
- дополнительная идентификация и аутентификация пользователей стандартных служб (на проходе);
- ревизия содержимого (вложений) информационных пакетов, выявление и нейтрализация компьютерных вирусов;
- виртуальные частные сети (для защиты потоков данных, передаваемых по открытым сетям – обеспечения конфиденциальности, – применяются криптографические методы);
- противодействие некоторым видам атак на внутренние ресурсы.

Классификация МСЭ

Основным критерием классификации МСЭ является поддерживаемый ими уровень сетевой модели OSI. В соответствии с этим вариантом классификации различают следующие типы МСЭ:

1. пакетные фильтры;
2. шлюзы уровня соединения (circuit-level gateway);
3. шлюзы прикладного уровня (application-level gateway).

Последние два типа МСЭ используют технологию «Proxy», согласно которой между двумя взаимодействующими узлами имеется «посредник». Альтернативным вариантом является технология Stateful Inspection, предложенная компанией Check Point.

Пакетные фильтры

Процесс фильтрации пакетов основан на проверке содержимого их заголовков. Пакетные фильтры осуществляют анализ информации сетевого и транспортного уровней модели OSI. Это сетевые адреса (например, IP) отправителя и получателя пакета, а также (хотя и необязательно) номера портов отправителя и получателя пакета. Обычно пакетные фильтры организуются на маршрутизаторах. При этом используются штатные средства самих маршрутизаторов или операционных систем. В частности, маршрутизаторы Cisco, Bay Networks и других производителей снабжены функциями сетевой фильтрации. Большинство программных сетевых фильтров представляют собой бесплатные или условно-бесплатные утилиты. Они реализованы для множества сетевых ОС, в том числе для UNIX, Windows, NetWare.

Шлюзы уровня соединения

Работа шлюзов уровня соединения основана главным образом на номерах портов, т.е. на типе трафика.

Этот и следующий тип МСЭ основан на использовании так называемого принципа посредничества, когда запрос принимается МСЭ, анали-

зируется и только потом перенаправляется реальному серверу. Прежде чем разрешить установление соединения между компьютерами внутренней и внешней сети, посредники уровня соединения сначала как минимум регистрируют клиента. При этом неважно, с какой стороны (внешней или внутренней) этот клиент находится. При положительном результате регистрации между внешним и внутренним компьютерами организуется виртуальный канал, по которому пакеты передаются между сетями.

Ключевым моментом, отличающим шлюз уровня соединения от шлюза прикладного уровня, является «статичность». Например, если правила разрешают передачу данных по ftp (20-й порт), то пакеты ftp-data будут пропускаться, даже если нет управляющего ftp-соединения (21-й порт).

Наиболее известным примером шлюза уровня соединения можно считать шлюз с преобразованием IP-адресов (Network Address Translation, NAT).

Шлюзы прикладного уровня

Шлюзы прикладного уровня (application-level proxy), часто называемые proxy-серверами, контролируют и фильтруют информацию на прикладном уровне модели OSI. Они различаются по поддерживаемым протоколам прикладного уровня. Наиболее часто поддерживаются службы Web (HTTP), FTP, SMTP, POP3/IMAP, NNTP, Gopher, telnet, DNS, RealAudio/RealVideo. Когда клиент внутренней сети обращается, например, к серверу Web, то его запрос попадает к посреднику Web (или перехватывается им). Последний устанавливает связь с сервером от имени клиента, а полученную информацию передает клиенту. Для внешнего сервера посредник выступает в качестве клиента, а для внутреннего клиента – в качестве сервера Web. Аналогично посредник может работать и в случае внешнего клиента и внутреннего сервера.

Работа посредников прикладного уровня основана на типе протокола прикладного уровня, в отличие от шлюзов уровня соединения, базирующихся на номерах портов. Кроме того, здесь обязательным требованием является установление соединения.

Технологии Proxy и Stateful inspection

В рассмотренных выше типах МСЭ, предполагающих посредничество при установлении соединения (шлюзах уровня соединения и прикладного) реализована так называемая технология Proxy. Эта технология широко распространена и применяется в таких известных моделях МСЭ, как Microsoft Proxy Server и CyberGuard Firewall.

Однако для выработки окончательных решений о разрешении того или иного соединения для служб TCP/IP (т.е. пропустить, запретить, аутентифицировать, сделать запись об этом в журнале), МСЭ должен уметь получать, хранить, извлекать и манипулировать информацией со всех уровней сетевой семиуровневой модели и из других приложений. Недос-

таточно только лишь просматривать отдельные пакеты. Информация о состоянии, извлеченная из имевших место ранее соединений и других приложений, используется для принятия окончательного решения о текущей попытке установления соединения. В зависимости от типа проверяемого пакета, для принятия решения важными могут быть как текущее состояние соединения, которому он принадлежит (полученное из его истории), так и состояние приложения, его использующего.

Stateful Inspection – технология нового поколения, удовлетворяет всем требованиям к безопасности, приведенным выше.

Эта технология позволяет контролировать данные вплоть до уровня приложения, не требуя при этом отдельного процесса-посредника (proxy) для каждого защищаемого протокола или сетевой службы. В результате достигаются высокие показатели производительности, высокая гибкость решений и возможность быстро и достаточно просто адаптировать систему под новые нужды.

Основываясь на технологии инспекции пакетов с учетом состояния протокола, МСЭ обеспечивает наивысший уровень безопасности. Метод Stateful inspection обеспечивает сбор информации из пакетов данных, как коммуникационного, так и прикладного уровня, что достигается сохранением и накоплением ее в специальных контекстных таблицах, которые динамически обновляются. Такой подход обеспечивает максимально возможный уровень безопасности, контролируя соединения на уровнях от 3 до 7 сетевой модели OSI, тогда как proxy посредники могут контролировать соединения только на 5–7 уровнях.

Варианты расположения МСЭ

Вопрос размещения МСЭ в корпоративной сети рассматривается с учетом конкретных особенностей уже имеющихся средств защиты, целей подключения и т.д. Однако можно выделить несколько общих схем, приемлемых для большинства конфигураций.

Схема 1. Здесь МСЭ и маршрутизатор размещены на одном узле. Это удобно, поскольку оба устройства работают на сетевом уровне.

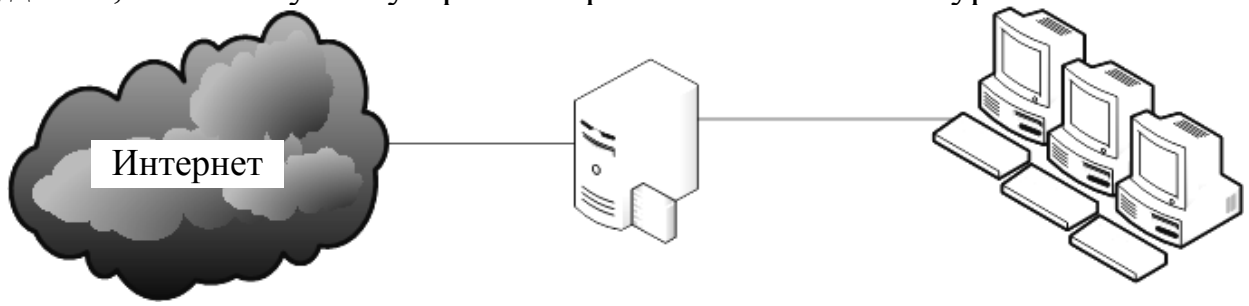
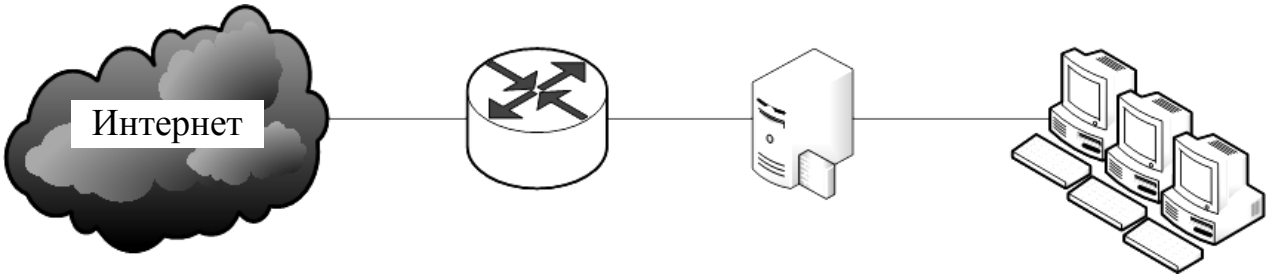
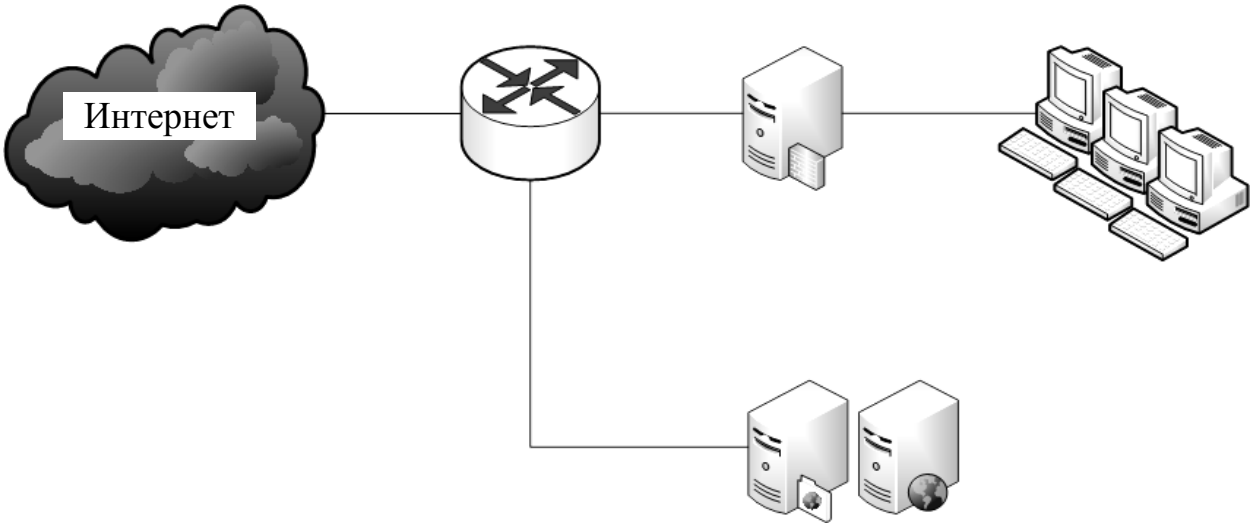


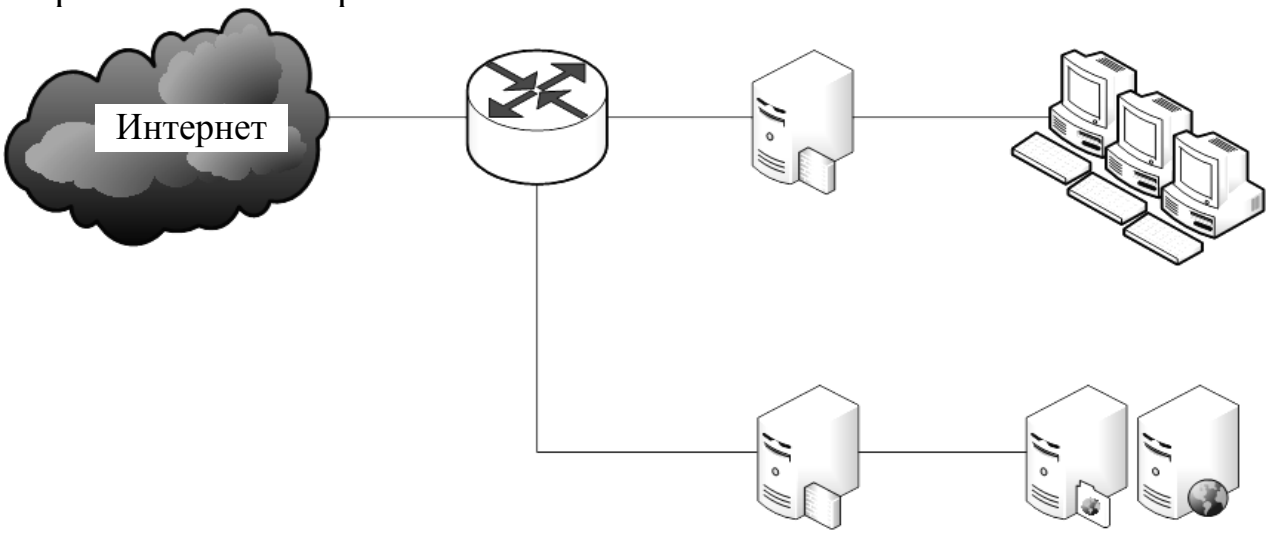
Схема 2, вероятно, вторая по распространённости, уместна в том случае, если в корпоративной сети используется аппаратный маршрутизатор (например, Cisco), а МСЭ представляет собой программный продукт. В этом случае МСЭ является единственной видимой снаружи машиной.



Одной из целей подключения к сетям общего пользования является возможность предоставить доступ внешним пользователям к некоторым внутренним ресурсам (WWW, FTP и др.). Поэтому при расположении МСЭ такие ресурсы должны быть доступны снаружи. Так возникает схема 3.



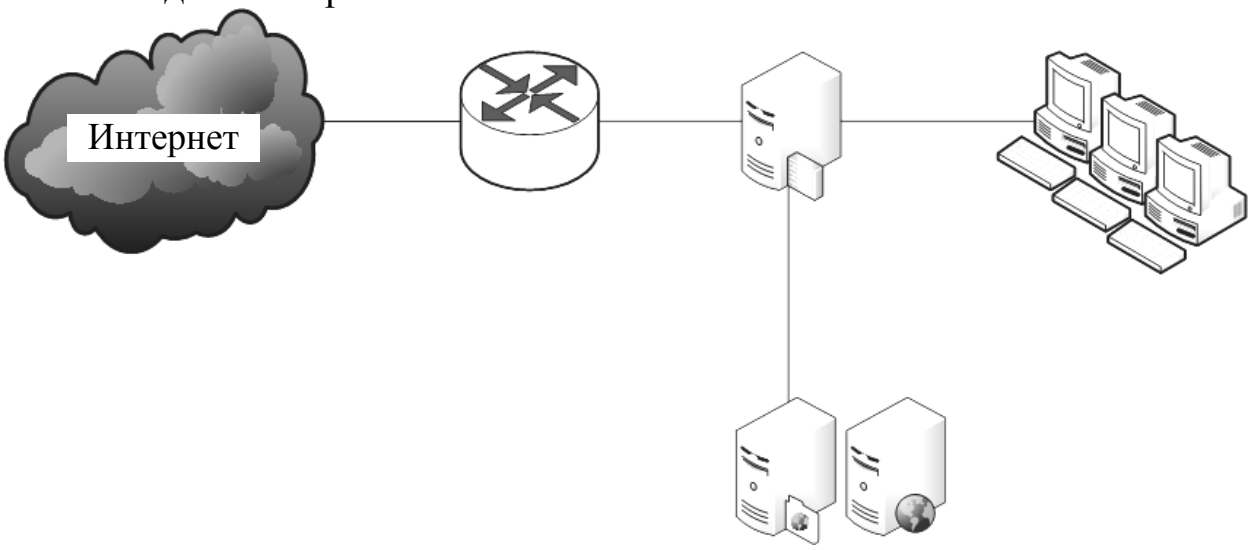
Рано или поздно встаёт вопрос защиты видимых снаружи узлов. По аналогии с защищёнными узлами корпоративной сети в качестве средства защиты используется МСЭ. Возникает следующая схема, не получившая распространения из-за высокой стоимости и представляющая чисто теоретический интерес.



Поэтому возникает следующая схема, третья по распространённости, в которой доступные снаружи узлы подключены к отдельному сетевому интерфейсу МСЭ.

Поскольку внешние пользователи должны иметь возможность непосредственного доступа к некоторым ресурсам узлов внутренней сети, то

возникает опасность, что, взломав защиту на этих узлах, они смогут использовать их в качестве плацдарма для атаки на другие (недоступные снаружи напрямую) узлы внутренней сети. Для защиты от такого рода угроз безопасности применяется метод, основанный на создании так называемой демилитаризованной зоны.



DMZ (De-Militarized Zone) – это специальная область сети, подключенная непосредственно к устройству разграничения доступа, относительно безопасная нейтральная «область сети пониженного риска», предназначенная для осуществления обмена между внутренними и внешними системами. Обычно это сеть, связанная с дополнительным сетевым интерфейсом на компьютере – шлюзе (межсетевом экране). Использование такого решения обеспечивает прохождение любого трафика DMZ через устройство разграничения доступа и контроля, что позволяет реализовать необходимые защитные меры, направленные против атак взломщиков.

Без использования DMZ, располагая общедоступные серверы в защищаемой сети, мы подвергаем всю внутреннюю сеть потенциальной опасности: взломщики могут воспользоваться особенностями программного обеспечения сервера, получить доступ к нему, а затем и ко всей сети.

При расположении же общедоступных серверов в DMZ, в случае их взлома нарушитель не получит дополнительных преимуществ по проникновению во внутреннюю сеть, так как доступ из DMZ во внутреннюю сеть контролируется firewall. Такой подход позволяет создавать наиболее безопасные конфигурации подключения к Интернет.

МСЭ позволяют эффективно реализовать политику безопасности, касающуюся вопросов обмена информацией с внешним миром. Однако, наряду с очевидными достоинствами, МСЭ имеют ряд ограничений:

- МСЭ не защищают от атак со стороны внутренних злоумышленников, т. е. пользователей, прошедших аутентификацию и авторизацию
- МСЭ не защищают соединения, установленные в обход средств защиты, например, с использованием модемов
- МСЭ могут быть неверно сконфигурированы

• МСЭ защищают только от небольшого количества всех возможных типов атак.

Требования к межсетевым экранам

Требования к межсетевым экранам установлены в документе «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Межсетевые экраны должны удовлетворять следующим требованиям:

По целевым качествам – обеспечивать безопасность защищаемой внутренней сети и полный контроль над внешними подключениями и сеансам связи.

По управляемости и гибкости – обладать мощными и гибкими средствами управления для полного воплощения в жизнь политики безопасности организации.

По производительности и прозрачности – работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик при максимальной нагрузке.

По самозащищенности – обладать свойством самозащиты от любых не санкционированных воздействий.

Перечень показателей межсетевых экранов по классам защищенности представлен в табл. 5.1.

Таблица 1

Показатель защищенности	5	4	3	2	1
Управление доступом	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская документация	+	=	+	=	+

5.6.7. Виртуальные частные сети

Виртуальная частная сеть (Virtual Private Network – VPN) – это технология, обеспечивающая безопасную связь по открытой общедоступной сети. В общем случае VPN решает три задачи:

• организация связей между филиалами;

• соединение с партнерами и клиентами;

• взаимодействие мобильных сотрудников с корпоративной сетью.

Термин «частная сеть» означает принадлежность оборудования и каналов связи сети предприятию и гарантию конфиденциальности информации, передаваемой по этой сети. В случае распределенных информационных систем частные сети не получили большого распространения.

Гораздо чаще предприятие применяет для связей своих филиалов арендуемые каналы связи. При аренде канала в таких сетях предприятие делит пропускную способность магистральных каналов и коммутаторов с другими абонентами провайдера. Полоса пропускания арендованного канала строго фиксирована, полностью выделяется предприятию и является его собственностью. Корпоративные данные практически не доступны для абонентов, не являющимися пользователями корпоративной сети или сотрудниками провайдера. Это обуславливает высокую степень защищенности данных.

Организация VPN через открытые сети

Если сети центрального офиса и каждого из филиалов имеют соединения с Интернет, то это дает потенциальную возможность получать доступ к ресурсам любого узла Интернет. Следовательно, пользователь одного филиала предприятия могут получать доступ через Интернет к ресурсам узлов других филиалов или центрального офиса. Построение VPN на базе Интернет имеет следующие преимущества:

- простота и доступность реализации;
- низкая стоимость.

Но, наряду с достоинствами имеются следующие недостатки:

- непредсказуемость пропускной способности;
- возможность перехвата информации, передаваемой по открытой сети.

Существуют разнообразные способы построения VPN, отличающиеся распределением функций по поддержанию VPN между корпоративной сетью и провайдером. В одном случае все функции по поддержанию VPN выполняет провайдер, гарантируя конфиденциальность и качество обслуживания клиентского трафика от точки входа в открытую сеть до точки выхода. В другом случае предприятие организует VPN собственными силами, за счет применения специальных VPN-продуктов в своей сети.

Как правило, все VPN-продукты обеспечивают только шифрование данных, но не гарантируют пропускную способность. Эта задача может быть решена только силами провайдера.

Виртуальная частная сеть – объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную сеть, обеспечивающую безопасность данных.

Виртуальные частные сети обладают несколькими характеристиками:

- Трафик шифруется для обеспечения защиты от прослушивания.
- Осуществляется аутентификация удаленного сайта.
- Виртуальные частные сети обеспечивают поддержку множества протоколов.
- Соединение обеспечивает связь только между двумя конкретными абонентами.

Виртуальные частные сети, как правило, подразделяются на два типа: пользовательские VPN и узловые VPN. Различие между ними заключается в методе использования, а не в способе отделения трафика каждым из двух типов сетей.

Пользовательские VPN представляют собой виртуальные частные сети, построенные между отдельной пользовательской системой и узлом или сетью организации. Часто пользовательские VPN используются сотрудниками, находящимися в командировке или работающими из дома. Сервер VPN может являться межсетевым экраном организации либо быть отдельным VPN-сервером. Пользователь подключается к интернету через телефонное подключение к локальному поставщику услуг, через канал DSL или кабельный модем и инициирует VPN-соединение с узлом организации через интернет.

Сеть VPN поддерживается отдельным приложением на компьютере пользователя.

В то время как пользователь имеет VPN-соединение с внутренней сетью организации, он также может соединяться и работать с интернетом или выполнять другие действия как обычный пользователь интернета.

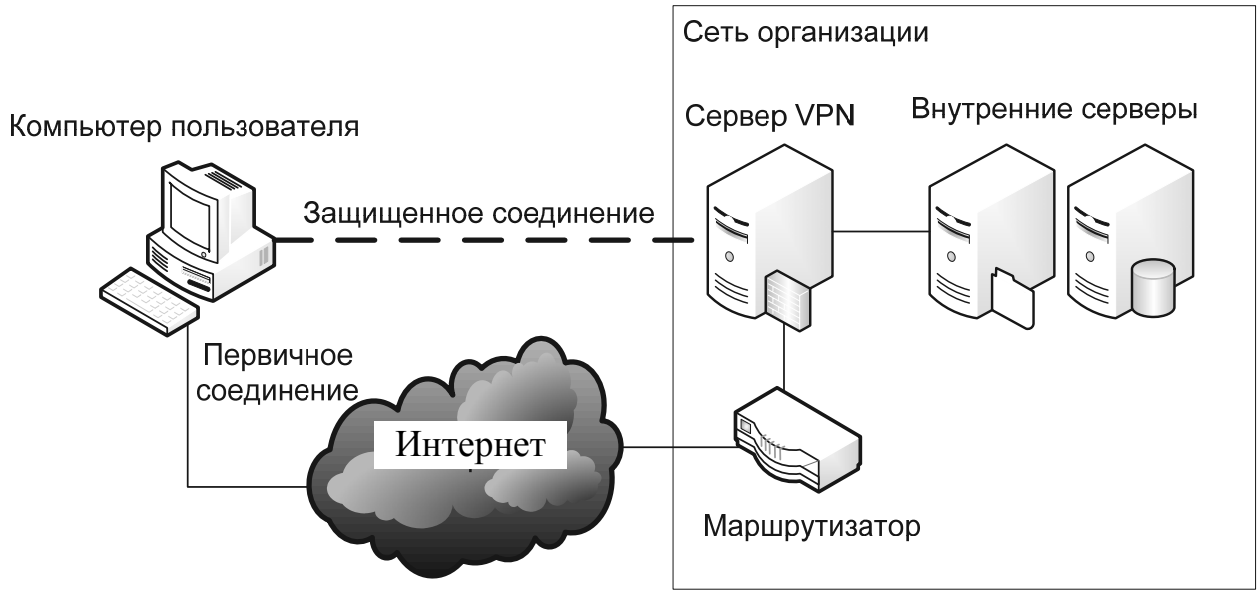


Рис. 5.5. Схема использования пользовательских VPN

Узловые VPN используются организациями для подключения к удаленным узлам без применения дорогостоящих выделенных каналов или для соединения двух различных организаций, между которыми необходима связь для осуществления информационного обмена, связанного с деятельностью этих организаций. Как правило, VPN соединяет один межсетевой экран или пограничный маршрутизатор с другим аналогичным устройством.

Сеть VPN состоит из четырех ключевых компонентов:

- Сервер VPN.
- Алгоритмы шифрования.

• Система аутентификации.
• Протокол VPN.
•

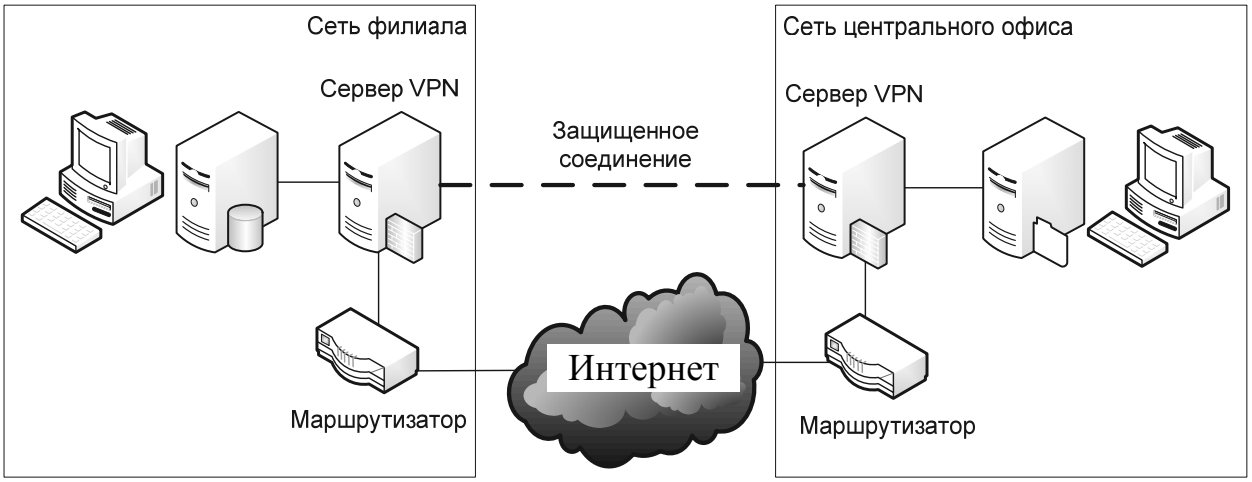


Рис. 5.6. Схема использование узловых VPN

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию.

Сервер VPN представляет собой компьютер, выступающий в роли конечного узла соединения VPN. Данный сервер должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Различные варианты размещения сервера VPN представлены на следующих кадрах.

Алгоритм шифрования, используемый в VPN, должен быть стандартным мощным алгоритмом шифрования.

Система аутентификации VPN должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают (пароли), того, что у них есть (электронные ключи) или с помощью данных о том, кем они являются (сертификаты).

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика.

Устройства VPN могут играть роль шлюза или клиента.

Шлюз VPN – это устройство, подключенное к нескольким сетям, выполняющее функции шифрования и аутентификации для узлов «позади» него. Размещение шлюза VPN аналогично размещению межсетевого экрана. Шлюз VPN может быть реализован всеми вышеперечисленными способами.

Клиент VPN – это программный или программно-аппаратный комплекс, сетевые возможности которого модифицированы для выполнения обмена с шлюзами VPN или другими VPN-клиентами. Как правило, VPN – клиент представляет собой программное решение, дополняющее стандартную операционную систему.

6. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Проблемой защиты информации путем ее преобразования занимается *криптология* (*kryptos* – тайный, *logos* – наука). Криптология разделяется на два направления – *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

Криптография – наука, занимающаяся преобразованием информации с целью скрытия ее содержания.

Сфера интересов *криптоанализа* – разработка методов, позволяющих взламывать криптографические средства защиты информации.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.
2. Ассиметричные криптосистемы (криптосистемы с открытым ключом).
3. Управление ключами.

Основные направления использования криптографии:

- защиты от утечки информации (**конфиденциальность и контроль доступа**);
- защиты от модификации информации (**целостность**);
- проверки подлинности передаваемых сообщений, пользователей, технических средств, программ (**аутентификация**);
- обеспечения юридической значимости электронных документов и невозможности отказаться от совершенных действий (**неотказуемость**).

6.1. Терминология

Открытый (исходный) текст – исходные данные, передаваемые или хранимые в последующем с использованием криптографии.

(За)шифрованный (закрытый) текст – данные, полученные после криптографического преобразования.

Криптосистема (шифр) – семейство обратимых криптографических преобразований открытого текста в зашифрованный.

Ключ – сменный элемент криптосистемы, то есть конкретное секретное состояние параметров криптоалгоритма, обеспечивающее выбор одного варианта преобразования из совокупности возможных.

(**За)шифрование** – процесс преобразования открытого текста в закрытый с помощью определенных правил криптосистемы.

Расшифрование – процесс, обратный зашифрованию.

Криптографическая стойкость – способность противостоять криптоанализу.

В криптосистемах часто приходится строить примеры взаимодействия двух объектов **А** и **Б**.

Криптографы придумали для этих объектов имена – **Алиса** и **Боб**.

Иногда в появляется третий субъект – злоумышленник, его обозначают «**В**», **враг**.

6.2. Угрозы со стороны участников информационного обмена

Угрозы со стороны злоумышленника

- Ознакомление с содержанием переданного сообщения.
- Навязывание получателю ложного сообщения – как полная его фабрикация, так и внесение искажений в действительно переданное сообщение.
- Изъятие переданного отправителем сообщения из системы таким образом, чтобы получатель не узнал о факте передачи сообщения;
- Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи.

Угрозы со стороны отправителя

- Разглашение переданного сообщения.
- Отказ от авторства в действительности переданного им сообщения.
- Утверждение, что некоторое сообщение отправлено получателю когда в действительности отправка не производилась.

Угрозы со стороны получателя

- Разглашение полученного сообщения.
- Отказ от факта получения некоторого сообщения когда в действительности оно было им получено.
- Утверждение, что некоторое сообщение получено от отправителя когда в действительности предъявленное сообщение сфабриковано самим получателем.

6.3. Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

6.4. Основные алгоритмы шифрования

Метод шифровки/дешифровки называют **шифром** (**cipher**). Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют **ключ** для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано только если известен ключ. Ключ, используемый для дешифровки может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают.

Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы секретным ключом) и асимметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

Симметричные алгоритмы подразделяют на **потоковые шифры** и **блочные шифры**. Потоковые позволяют шифровать информацию поби-

тово, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

Асимметричные шифры (также именуемые алгоритмами с открытым ключом, или – в более общем плане – криптографией с открытым ключом) допускают, чтобы открытый ключ был доступн всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют **открытым ключом**, а ключ для дешифрования – **закрытым ключом** или **секретным ключом**.

Современные алгоритмы шифровки/дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

Симметричные алгоритмы работают быстрее, чем асимметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения.

Многие качественные криптографические алгоритмы доступны широко – в книжном магазине, библиотеке, патентном бюро или в Интернет. К широко известным симметричным алгоритмам относятся DES и IDEA, к асимметричным – RSA. В России за стандарт шифрования принят ГОСТ 28147-89.

6.5. Симметричные криптосистемы

Симметричные криптосистемы – криптосистемы в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Задача: передать от объекта А объекту Б сообщение с сохранением конфиденциальности.

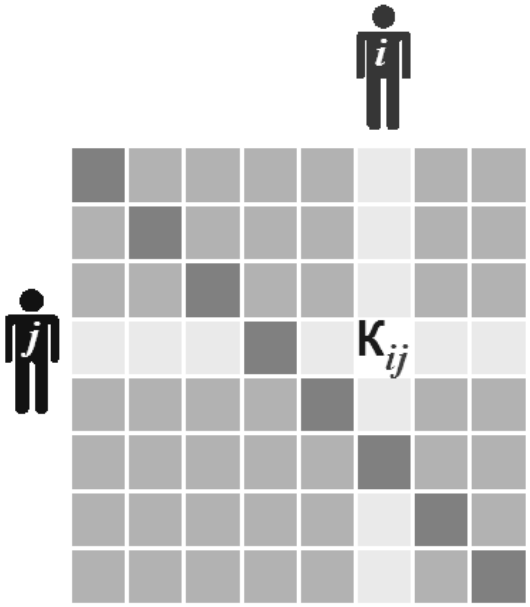


Задача управления ключами:

- требуется создать и доставить ключ абоненту
- необходимо согласовать, какой тип информации на каких ключах шифруется
- иногда требуется заменить скомпрометированный или «отживший» отведенное время ключ

Преимуществами систем с симметричными ключами являются:

- скорость
- высокая криптостойкость



Основные недостатки:

- Сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые необходимо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950 и т.д.
- Сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.

Российский стандарт:

- ГОСТ 28147-89, ключ 256 бит

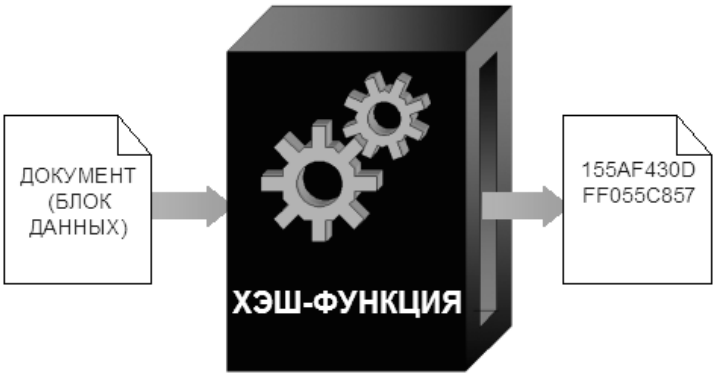
Западные стандарты:

- DES, ключ 56 бит, утратил стойкость в силу малой длины ключа
- 3DES, ключ 168 бит
- AES, ключ 256 бит
- BlowFish, RC2, RC4, CAST, IDEA …



6.6. Криптографические хэш-функции

Хэширование (хэш-функции) – преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины таким образом, чтобы изменение входных данных приводило к непредсказуемому изменению выходных данных.



Задача: обеспечение целостности данных.

Расчет хэш-функции:

- Входное значение рассматривается как последовательность n-битных блоков.
- Входное значение обрабатывается последовательно блок за блоком, и создается m-битное значение хэш-кода.

Свойства:

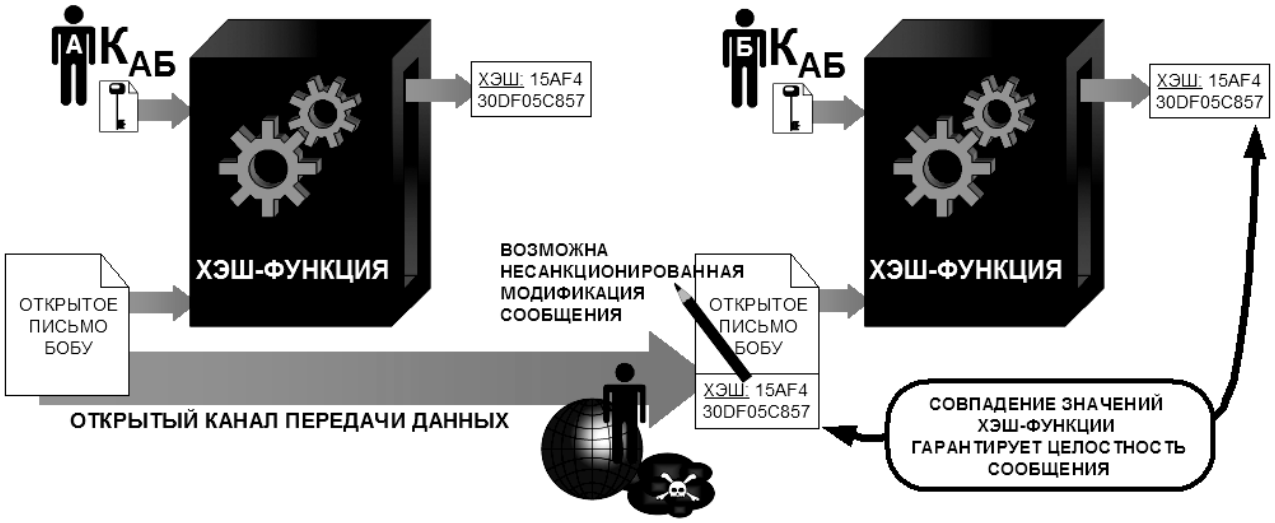
- однонаправленность: подсчитать хэш-значение легко, а предсказать исходный текст, который даст заданное значение хэша невозможно;
- высокая контекстная чувствительность: любое изменение исходного текста (один бит!) приводит к непредсказуемому изменению хеш-значению.

Применяемые алгоритмы расчета хэш-функций:

- ГОСТ Р 34.11-94 (в РФ)
- Message Digest 5 (MD5)
- Secure Hash Algorithm 1 (SHA-1)

Имитовставка – блок информации, применяемый для контроля целостности, зависящий от ключа и данных.

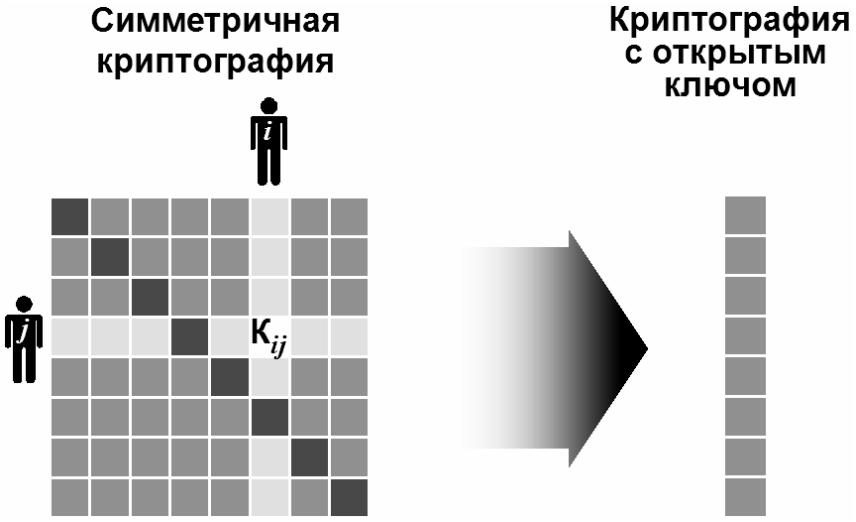
Режим расчета имитовставки описан в **ГОСТ 28147-89.**



6.7. Ассиметричные криптосистемы (криптосистемы с открытым ключом)

Ассимметричные криптосистемы – криптосистемы в которых зашифрование и проверка электронной цифровой подписи (ЭЦП) проводится с использованием открытого ключа, а расшифрование и формирование ЭЦП с использованием закрытого (секретного) ключа.

Задача: обеспечить конфиденциальность информации в больших открытых системах.



Цифровые подписи

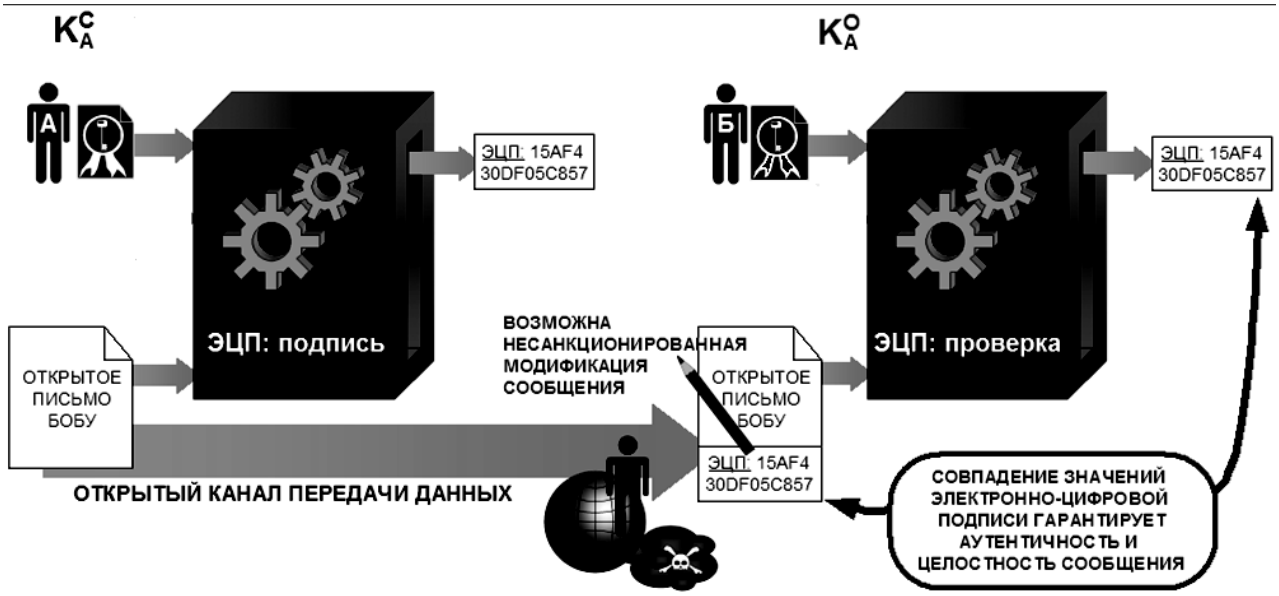
Некоторые из асимметричных алгоритмов могут использоваться для генерирования (формирования) **цифровой подписи**. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу). Также подписи используются для проставления **штампа времени** (**timestamp**) на документах: сторона, которой мы доверяем, подписывает документ со штампом времени с помощью своего секретного ключа и, таким образом, подтверждает, что документ уже существовал в момент, объявленный в штампе времени.

Цифровые подписи также можно использовать для удостоверения (**сертификации – to certify**) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит подписываются стороной, которой доверяем. При этом

доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим a-priori, что ему можно доверять). В **централизованной инфраструктуре ключей** имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агентства; их также называют **сертификационными агентствами** – **certification authorities**). В **распределенной инфраструктуре** нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название **сети доверия** (**web of trust**) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый **дайджест** (**message digest**) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.



Свободно доступны несколько методов создания и проверки цифровых подписей.

Ассимметричные криптоалгоритмы:

- ГОСТ Р 34.10–94, 2001, стандарты РФ;
- Diffie-Hellman;
- RSA – Rivest, Shamir, Adelman;
- El Hamal;
- DSA – Digital Signature algorithm, стандарт США.

Свойства электронной цифровой подписи:

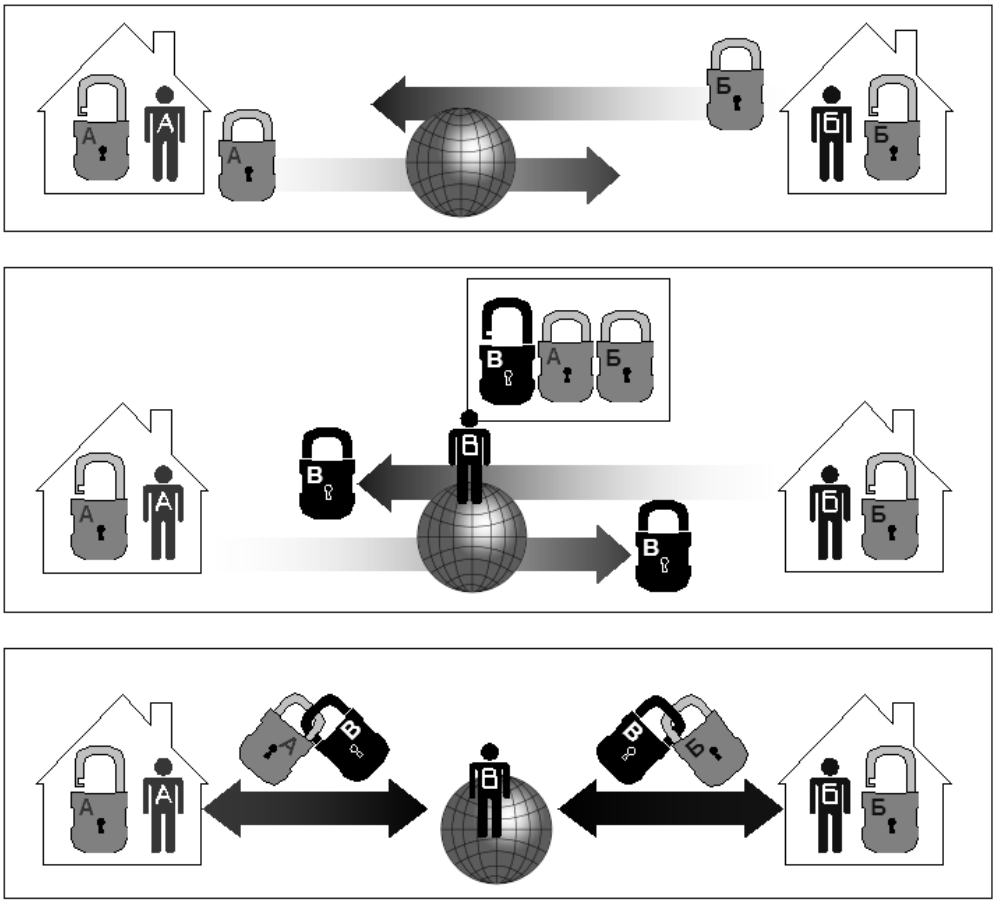
- уникальна;
- неотъемлема от документа;
- может быть создана только автором (владельцем секретного ключа ЭЦП).

Преимущества:

- решают задачу ключевого управления (отсутствует обмен секретами между участниками защищенного взаимодействия);
- обеспечивают неотрекаемость на основе ЭЦП;

Недостатки:

- высокие вычислительные затраты;
  - решение: применение «гибридных» алгоритмов с использованием симметричного шифрования;
- отсутствует прямая возможность аутентификации ключевого обмена;
  - атака «Man in the Middle» (человек посередине).



Атака «Man in the Middle»:

- Алиса и Боб попытались обменяться открытыми ключами;
- Злоумышленник сумел перехватить этот обмен и выдать Алисе свой открытый ключ от имени Боба и наоборот;
- после этого он сможет расшифровать сообщения Алисы, перешифровать их с использованием открытого ключа Боба и передать результат Бобу;
  - конфиденциальность нарушена;
  - Алиса и Боб никогда не узнают о нарушении конфиденциальности.

6.8. Управление ключами

Сертификаты

Задача защиты ключей от подмены решается с помощью сертификатов.

Сертификат представляет собой структуру данных, которая содержит открытый ключ владельца сертификата и подписана электронной цифровой подписью его издателя.

Назначение сертификата – удостоверение издателем подлинности связи между открытым ключом субъекта и информацией, его идентифицирующей.

Структура сертификата X.509 v.3 определена в международных стандартах ITU-T X.509 и RFC 2459.

Сертификат X.509 v3 состоит из трех частей:

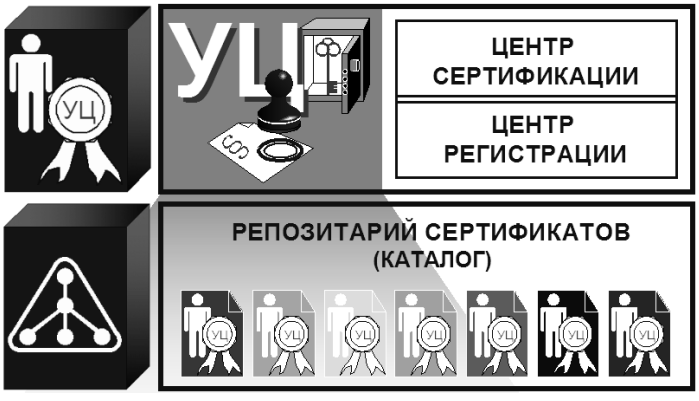
- «Тело» сертификата – формат, версия и серийный номер сертификата, атрибуты владельца (subject) и издателя (issuer) сертификата, значение открытого ключа, расширения сертификата.
- Алгоритм ЭЦП, на котором произведена подпись удостоверяющего центра (certificate authority, CA).
- ЭЦП удостоверяющего центра (значение).

Инфраструктура открытых ключей (Public Key Infrastructure, PKI) – система управления криптографической защитой, на основе ассиметричных криптосистем и **сертификатов**.

В качестве издателей сертификатов в ИОК выступают специальные **удостоверяющие центры**.

Компоненты ИОК и их функции

- Центр Сертификации;
- Центр Регистрации;
- Конечные пользователи;
- Репозитарий (каталог) сертификатов.



Компоненты ИОК и их функции

■ Центр Сертификации (или Удостоверяющий Центр) – основная управляющая компонента ИОК, предназначенная для формирования электронных сертификатов подчиненных Центров и конечных пользователей. Кроме сертификатов, ЦС формирует список отозванных сертификатов с регулярностью, определенной Регламентом системы.

К основным функциям ЦС относятся:

■ Формирование собственного секретного ключа и сертификата ЦС;

■ Формирование сертификатов подчиненных Центров;

■ Формирование сертификатов открытых ключей конечных пользователей;

■ Формирование списка отозванных сертификатов;

■ Ведение базы всех изготовленных сертификатов и списков отозванных сертификатов;

Компоненты ИОК и их функции

■ Центр Регистрации

Опциональная компонента ИОК, предназначенная для регистрации конечных пользователей. Основная задача ЦР – регистрация пользователей и обеспечение их взаимодействия с ЦС. В задачи ЦР может также входить публикация сертификатов и СОС в сетевом справочнике.

■ Пользователи

Пользователь, приложение или система, являющиеся владельцами сертификата и использующие ИОК.

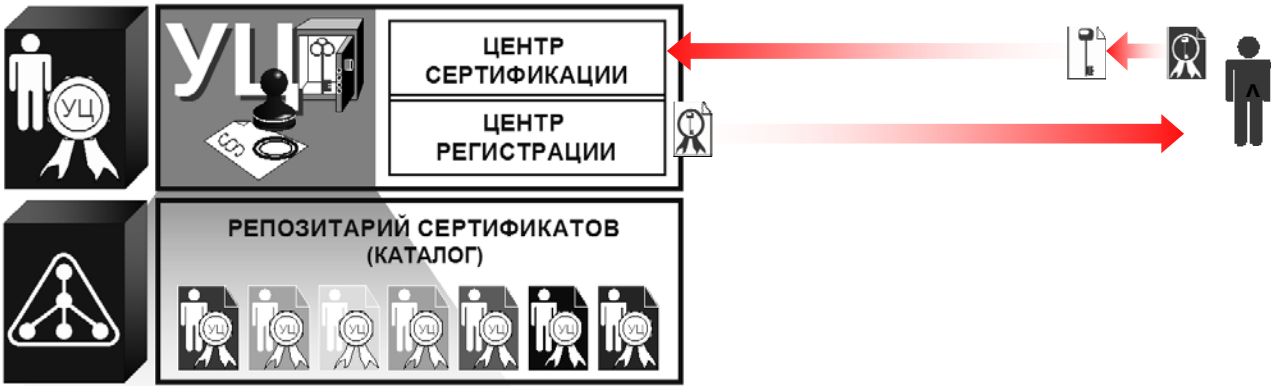
■ Репозитарий (каталог сертификатов)

Опциональная компонента ИОК, содержащая сертификаты и списки отозванных сертификатов и служащая для целей распространения этих объектов среди пользователей с использованием протокола LDAP (HTTP, FTP).

Децентрализованное издание сертификатов

Конечный пользователь генерирует ключевую пару, включает открытый ключ в запрос на сертификат и направляет его для сертификации в УЦ:

■ схема обеспечивает уникальность и полную секретность личного ключа пользователя.



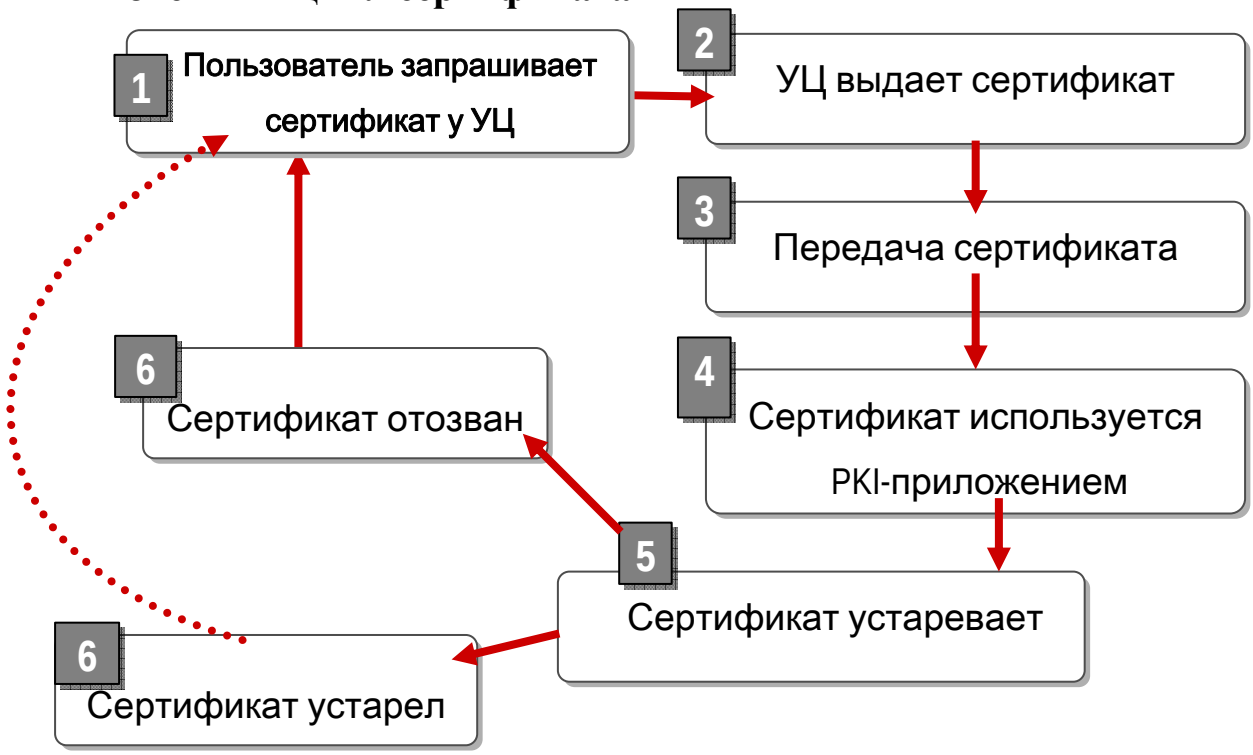
Централизованное издание сертификатов

Ключевые пару генерирует и распространяет администратор удостоверяющего центра

■ схема эксплуатационно более проста, чем децентрализованное издание ключей



Жизненный цикл сертификата



Отзыв сертификата

Существует целый ряд причин, по которым доверие к сертификату может быть подорвано до истечения срока его действия. Примеры:

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения ключевых носителей.
- Получение сертификата незаконным путем.
- Изменение сведений о субъекте.

ИОК допускает распределенную проверку сертификата, которая не требует прямого обмена данными с центральным доверенным объектом,

выпустившим этот сертификат. Для этого необходима информация об отзыве сертификатов.

В инфраструктуре открытых ключей предусмотрены специальные **списки отозванных сертификатов (CRL – Certificate Revocation List)**. Клиенты УЦ могут получить эту информацию и записать ее в локальное хранилище, чтобы использовать для проверки сертификатов.

Обычно опубликованные УЦ списки доступны клиентам через сеть.

Использование ИОК в приложениях

- ИОК используется для управления ключами и электронными сертификатами в приложениях или для формирования ЭЦП электронных документов, приложений и т.д.
- **Электронная почта и документооборот**

Защищенные электронная почта и документооборот используют криптографию для шифрования сообщений или файлов и формирования ЭЦП. Из наиболее известных и распространенных стандартов стоит отметить протокол S/MIME (Secure Multipurpose Internet Mail Extensions), который является расширением стандарта Internet почты MIME (Multipurpose Internet Mail Extensions).

- **Web приложения**

Web броузеры и сервера используют ИОК для аутентификации и конфиденциальности сессии, а также для онлайновых банковских приложений и электронных магазинов. Наиболее распространенным протоколом в этой сфере является протокол SSL (Secure Sockets Layer).

- **ЭЦП файлов и приложений**

Использование ЭЦП для подписи приложений и файлов позволяет безопасно распространять их по сети Internet. При этом пользователь уверен в корректности полученного приложения от фирмы-разработчика.

6.9. Криптоанализ и атаки на криптосистемы

Криптоанализ – это наука о дешифровке закодированных сообщений не зная ключей. Имеется много криптоаналитических подходов. Некоторые из наиболее важных для разработчиков приведены ниже.

Атака со знанием лишь шифрованного текста (**ciphertext-only attack**): Это ситуация, когда атакующий не знает ничего о содержании сообщения, и ему приходится работать лишь с самим шифрованным текстом. На практике, часто можно сделать правдоподобные предположения о структуре текста, поскольку многие сообщения имеют стандартные заголовки. Даже обычные письма и документы начинаются с легко предсказуемой информации. Также часто можно предположить, что некоторый блок информации содержит заданное слово.

Атака со знанием содержимого шифровки (**known-plaintext attack**): Атакующий знает или может угадать содержимое всего или час-

ти зашифрованного текста. Задача заключается в расшифровке остального сообщения. Это можно сделать либо путем вычисления ключа шифровки, либо минуя это.

Атака с заданным текстом (**chosen-plaintext attack**): Атакующий имеет возможнот получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Некоторые методы шифрования и, в частности, RSA, весьма уязвимы для атак этого типа. При использовании таких алгоритмов надо тщательно следить, чтобы атакующий не мог зашифровать заданный им текст.

Атака с подставкой (**Man-in-the-middle attack**): Атака направлена на обмен шифрованными сообщениями и, в особенности, на протокол обмена ключами. Идея заключается в том, что когда две стороны обмениваются ключами для секретной коммуникации (например, используя шифр Диффи-Хелмана, Diffie-Hellman), противник внедряется между ними на линии обмена сообщениями. Далее противник выдает каждой стороне свои ключи. В результате, каждая из сторон будет иметь разные ключи, каждый из которых известен противнику. Теперь противник будет расшифровывать каждое сообщение своим ключом и затем зашифровывать его с помощью другого ключа перед отправкой адресату. Стороны будут иметь иллюзию секретной переписки, в то время как на самом деле противник читает все сообщения.

Одним из способов предотвратить такой тип атак заключается в том, что стороны при обмене ключами вычисляют криптографическую хэш-функцию значения протокола обмена (или по меньшей мере значения ключей), подписывают ее алгоритмом цифровой подписи и посылают подпись другой стороне. Получатель проверит подпись и то, что значение хэш-функции совпадает с вычисленным значением. Такой метод используется, в частности, в системе ФотуРисунок (Photuris).

Атака с помощью таймера (**timing attack**): Этот новый тип атак основан на последовательном измерении времен, затрачиваемых на выполнение операции возведения в стенень по модулю целого числа. Ей подвержены по крайней мере следующие шифры: RSA, Диффи-Хеллман и метод эллиптических кривых.

Имеется множество других криптографических атак и криптоаналитических подходов. Однако приведенные выше являются, по-видимому, наиболее важными для практической разработки систем. Если кто-либо собирается создавать свой алгоритм шифрования, ему необходимо понимать данные вопросы значительно глубже.

Выбор для конкретных ИС должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты в общем-то должен опираться на какие-то *критерии эффективности*. К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Наиболее простой критерий такой эффективности – *вероятность раскрытия ключа* или *мощность множества ключей* (*M*). По сути это то же самое, что и *криптостойкость*. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей.

Однако этот критерий не учитывает других важных *требований к криптосистемам*:

- невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры;
- совершенство используемых протоколов защиты;
- минимальный объем используемой ключевой информации;
- минимальная сложность реализации (в количестве машинных операций), ее стоимость;
- высокая оперативность.

Желательно конечно использование некоторых интегральных показателей, учитывающих указанные факторы.

Для учета стоимости, трудоемкости и объема ключевой информации можно использовать удельные показатели – отношение указанных параметров к мощности множества ключей шифра.

Часто более эффективным при выборе и оценке криптографической системы является использование экспертных оценок и имитационное моделирование.

В любом случае выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в ИС информации.

6.10. Характеристики безопасности, обеспечиваемые средствами криптографической защиты информации

- **Конфиденциальность** – Информация должна быть защищена от несанкционированного прочтения как при хранении, так и при передаче. Обеспечивается шифрованием.
- **Контроль доступа** – Информация должна быть доступна только для того, для кого она предназначена. Обеспечивается шифрованием.
- **Аутентификацию –** Возможность однозначно идентифицировать отправителя. Обеспечивается электронной цифровой подписью и сертификатом.
- **Целостность –** Информация должна быть защищена от несанкционированной модификации как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью и имитовставкой.
- **Неотрекаемость** – Отправитель не может отказаться от совершенного действия. Обеспечивается электронной цифровой подписью и сертификатом.

6.11. Удостоверяющий центр

6.11.1. Основные положения

Современные тенденции и мобильность диктуют нам использование Интернета. На смену бумажным документам пришли электронные, а личные контакты все чаще уступают место переписке по электронной почте. Возникает проблема обеспечения целостности и зашиты от несанкционированного доступа передаваемой информации. Одним из наиболее совершенных механизмов аутентификации участников информационных систем и контроля целостности электронных документов является Электронная Цифровая Подпись (ЭЦП). Технология Public Key Infrastructure (PKI), используемая в Российской Федерации, является наиболее эффективной и широко применяется в мировой практике использования ЭЦП.

Теория криптографической структуры открытых ключей основана на получении двух ключей из одной функции. Один ключ называется открытым ключом, а другой ключ называется индивидуальным ключом. Они так названы потому, что открытый ключ может быть известен всем, а индивидуальный ключ – нет.

Существует идея, ставшая общепринятой, что открытые ключи могут быть доступны любому, возможно в общедоступном списке, например, таком, как X.509. Существует проблема доверия: каким образом пользователи узнают, что их предположительно правильный ключ действительно правильный.

Благодаря использованию цифровых сертификатов, получатель сообщения может быть уверен в том, что открытый ключ отправителя является подлинным. Для реализации этой идеи отправитель сообщения должен получить цифровой сертификат из независимого источника, которому он доверяет. Эта третья сторона называется Удостоверяющим Центром (УЦ). Удостоверяющий центр должен удовлетворять следующим условиям: УЦ должен быть надежным и его открытый ключ должен быть широко доступен, чтобы иметь возможность проверять подписи. При этом удостоверяющий центр берет на себя ответственность за выданный им сертификат.

Под термином «надежный» понимается, что УЦ не должен подписывать сертификат, не будучи уверенным, что имя на сертификате действительно соответствует открытому ключу.

Правовой основой в РФ выступает «Закон об Электронной Цифровой Подписи», который четко определяет государственную структуру PKI и дает рекомендации коммерческим структурам PKI. Согласно закону, казалось, что структура взаимодействия УЦ на Российской арене будет

единственной и универсальной PKI. Будет единственный «корневой» орган выдачи сертификатов, к которому будут принадлежать все подчиненные УЦ. На практике оказалось, что такой подход не очень хорош и на сегодня существует множество «корней», к которым могут привести цепочки сертификатов [26].

Существует проблема совместимости средств ЭЦП различных производителей. Даже сертифицированные Системы Криптографической Защиты Информации (СКЗИ) различных российских производителей, реализующие единые российские криптографические стандарты, практически несовместимы между собой. Каждое из этих средств использует свои собственные идентификаторы алгоритмов. Сертификаты УЦ, построенного на базе одного СКЗИ, не смогут обслуживать криптосистемы, построенные на базе других СКЗИ, а подпись, сформированная одним СКЗИ, не может быть проверена другим СКЗИ. Пока проблема совместимости не решена, конечный пользователь вынужден поддерживать у себя два СКЗИ: свое собственное и применяемое партнером по юридически значимому документообороту.

Владельцы сертификатов должны иметь возможность использования единого сертификата в различных PKI системах, что облегчит их работу и упростит процедуру разрешения конфликтных ситуаций. В идеале в случае полной совместимости, при соответствующей кросс – сертификации, с одним сертификатом можно было бы участвовать в различных, как корпоративных, так и государственных структурах PKI, в том числе и разных производителей. Это является целью построения единой PKI.

Российский рынок предлагает не так много программного обеспечения в данной области. А существующие решения обладают рядом ограничений и высокой стоимостью лицензий. По законодательству необходимо использовать только сертифицированные СКЗИ. Большинство зарубежных аналогов не использует Российские криптографические стандарты. Также необходима поддержка гибридной модели доверия, которая необходима для построения систем, содержащих в своем составе различные реализации PKI, для снижения расходов на поддержку инфраструктуры в целом. Необходимо обеспечить гибкую систему управления и контроля над инфраструктурой PKI. Не секрет что даже небольшие проблемы в работе Инфраструктуры Открытых Ключей очень дорого обходятся корпорациям, поэтому очень важно в составе решения иметь инструментарий, способный эффективно реагировать как на штатные, так и аварийные ситуации, производить анализ и получать отчеты о состоянии системы. Поэтому очевидна целесообразность создания собственного программного обеспечения удостоверяющего центра.

Одним из важных аспектов создания собственного удостоверяющего центра, является разработка программного обеспечения защищенного каталога удостоверяющего центра. Существует необходимость обеспечить

поддержку большого количества пользователей удостоверяющего центра. Также важнейшими критериями защищенного каталога является управление сертификатом, управление статусом сертификатов, управление списком отзыва.

В качестве дополнительного аспекта необходимо рассмотреть и создать модуль связи с криптографическими функциями, который обеспечивает набор криптографических функций и позволяет производить манипуляции, связанные с генерацией ключей, создания запросов, сертификатов.

К таким организациям, выполняющим функции удостоверяющего центра можно отнести: Удостоверяющий Центр Сибири (ГОУ ВПО ТУСУР); ЗАО «Удостоверяющий Центр Московской области»; ЗАО «Удостоверяющий Центр»; ЗАО «Удостоверяющий Центр Нижний Новгород», ЗАО «ПФ СКБ Контур», ООО «Крипто-Про» и ряд других.

Необходимо также отметить создание в 2004г. Федеральным агентством по информационным технологиям, в рамках реализации мероприятий ФЦП «Электронная Россия», удостоверяющего центра (далее – УЦ) и реестра УФО.

6.11.2. Международный опыт

Развитие законодательства в зарубежных странах и международного права в области применения электронной подписи идет по пути гармонизации, выработки единой методологии и технических требований, что должно позволить создать на мировом уровне универсальную правовую и технологическую инфраструктуру электронной подписи. Необходимо отметить, что в иностранной юридической доктрине по данному вопросу преобладает точка зрения, которая состоит в том, что в связи с глобальным характером «online economy» национальное законодательство должно быть сведено к нескольким унифицированным законам, стать последовательно международным и прозрачным. Данная позиция совпадает с основными принципами и подходами, зафиксированными в Окинавской хартии, которая ставит перед правительствами государств задачу создания «предсказуемой, транспарентной и не дискриминационной политики и нормативной базы, необходимой для информационного общества».

Данные принципы нашли наиболее полное отражение в Директиве Европейского Парламента по электронным подписям 1999г. Директива исходит, прежде всего, из целей и задач обеспечения нормального функционирования внутреннего рынка Европейского Союза, свободного перемещения товаров и капитала, а также свободного передвижения физических лиц на всей территории Евросоюза.

Директива устанавливает рамочное регулирование применения электронных подписей и оказания услуг по выдаче сертификатов ключей электронной подписи. Она не распространяется на заключение и испол-

нение договоров или иных обязательств, которые подчиняются требованиям национального законодательства государств-участников Евросоюза. Основные требования Директивы в отношении законодательства государств-участников состоят в следующем.

Предоставление услуг по выдаче сертификатов ключей электронной подписи не должно зависеть от предварительного разрешения. Однако может вводиться добровольная аккредитация поставщиков данных услуг.

Признавать средства электронной подписи, отвечающие общепризнанным стандартам средств электронной подписи, опубликованным в Официальном Журнале Европейского Союза, соответствующими требованиям Директивы в отношении надежных (квалифицированных) сертификатов.

Гарантировать, что средства электронной подписи, которые соответствуют современным требованиям, могут свободно обращаться на внутреннем рынке. Возможно предъявление дополнительных требований к использованию электронных подписей в государственном (публичном) секторе. Такие требования не могут составлять препятствия трансграничным услугам для граждан.

Не ограничивать предоставление услуг с территории другого государства-участника в отношениях.

Гарантировать, что электронные подписи, созданные с помощью надежных средств электронной подписи и имеющие соответствующие подтверждение их надежности:

– удовлетворяют юридическим требованиям к подписи в отношении данных в электронной форме, так же как и собственноручная подпись удовлетворяет такие требования в отношении информации на бумажном носителе;

– допускаются в качестве судебных доказательств.

Обеспечить, чтобы юридическая сила электронных подписей и допустимость последних в качестве доказательств не отрицались только на том основании, что подписи являются электронными, или не созданы при помощи надежных средств создания электронной цифровой подписи, или не имеют соответствующего сертификата.

Предусмотреть положения об ответственности поставщика услуг по выдаче сертификатов ключей электронной подписи в случае выпуска сертификата для использования в отношении неопределенного круга лиц или предоставлении гарантий на основе такого сертификата.

Предусмотреть возможность указывать в сертификате ограничения на его использование, в том числе, лимит стоимости операций, для совершения которых может использоваться сертификат.

Гарантировать защиту частных лиц в отношении использования персональной информации, предоставляемой для получения сертификатов ключей электронной подписи.

Государства-участники должны принять соответствующие Директиве законы и подзаконные акты. Последние должны содержать отсылку к данной Директиве.

Одновременно с этим, приложения, содержащиеся в Директиве определяют:

– Требования, предъявляемые к квалифицированным сертификатам.

– Требования, предъявляемые к поставщику сертификационных услуг (удостоверяющему центру), выпускающему квалифицированные сертификаты.

– Требования к надежным средствам создания электронной подписи.

– Рекомендации к процедуре безопасной проверки подписи.

– Кроме этого, в 2003 г. комиссия Европейского парламента опубликовала решение, направленное на дальнейшее решение вопросов единого методологического и технологического подхода к вопросу использования электронной подписи в Евросоюзе. Данное решение предлагает использовать в практической деятельности по применение электронной подписи технические стандарты, разработанные CEN (Европейский комитет по стандартизации) и ETSI (Европейский институт стандартов телекоммуникации) в рамках EESSI (Европейская инициатива по стандартизации электронной подписи).

Большинство европейских стран предъявляют требования по аккредитации удостоверяющих центров, издающих квалифицированные сертификаты (а только использование таких сертификатов обеспечивает равнозначность собственноручной подписи электронной и аналогично положению ФЗ «Об ЭЦП» в части требования к сертификату открытого ключа).

Причем аккредитация УЦ основана на условии применения адекватной концепции безопасности УЦ и УЦ используют только проверенные и аттестованные в конкретной стране программно-технические средства для создания электронной подписи.

Следует также заметить, что хотя Директива и определяет применение электронной подписи как таковой, однако технические спецификации, международные рекомендации и стандарты (CEN, ETSI, IETF, ISO, ITU-T) разработаны только для алгоритмов электронной цифровой подписи.

В большинстве информационно развитых стран деятельность по использованию электронной подписи регулируется государством, через уполномоченный орган.

Можно привести следующие примеры.

Уполномоченный государственный орган Германии – Государственный орган по регулированию и надзору в области телекоммуникаций и почтовой связи (.RegTP), выполняющий функции по аккредитации поставщиков сертификационных услуг (удостоверяющих центров), осуще-

ствляет надзор за аккредитованными центрами, выпускает сертификаты ключей центров и управляет национальным удостоверяющим центром высшего уровня (корневым удостоверяющим центром).

Управление политикой в области применения ЭЦП в Канаде осуществляется Секретариатом Государственного Казначейства. Секретариат Казначейства Канады осуществляет контроль за соблюдением политики, анализирует отчеты, предоставляемые ответственными должными лицами Комитету по исполнению политики Правительства Канады в области PKI.

Комитет по исполнению Политики Правительства Канады в области ЭЦП состоит из представителей Департаментов, выпускающих сертификаты открытых ключей или управляющих удостоверяющими центрами, управляющего информационными технологиями, «Канадского Федерального PKI Моста» и др. организаций. Управляющий информационными технологиями возглавляет Комитет по исполнению политики Правительства Канады в области ЭЦП; отвечает за аккредитацию «Канадского Федерального PKI Моста», публичных удостоверяющих центров и др. Политика Правительства в области ЭЦП предусматривает применение технологии открытых ключей и использование цифровых подписей, основанных на криптографии, в качестве основного способа электронной аутентификации, идентификации и защиты информации в государственном управлении и бизнесе.

С целью координации развития PKI в Федеральном правительстве США в 2000 г. создано Федеральное агентство по PKI политике (The Federal PKI Policy Authority). Федеральное агентство создано при Федеральном Совете Управляющих по информационным технологиям (Federal Chief Information Officers Council) и функционирует под руководством Комитета по архитектуре и взаимодействию. Оно координирует взаимодействие ведомств по вопросам PKI политики. Федеральное агентство разрабатывает Политику функционирования Федерального Удостоверяющего центра. Использование Федерального Удостоверяющего центра позволяет доверять цифровым сертификатам, выпущенным разными ведомствами, при условии, что такие сертификаты соответствуют Политике и кросс-сертифицированы Федеральным Удостоверяющим центром. Последний обслуживает прежде всего интересы федеральных правительственных организаций, однако способствует взаимодействию структур, не принадлежащих к числу федеральных правительственных организаций: компаний, правительств штатов и местных органов власти, иностранных правительств. Более подробно опыт США в области построения инфраструктуры открытых ключей расст\мотрен в Приложении № 6 к настоящему отчету.

6.11.3. Основные концепции безопасности PKI

Уровень безопасности системы зависит от того, какие меры приняты для обеспечения безопасности системы. Нет такого понятия, как полностью защищенная система, так как принятые в системе операции по обеспечению безопасности могут быть слишком упрощенными [27].

Когда речь заходит о безопасности данных в Интернете, подразумевается принятие специальных мер для достижения следующих целей:

1) *Анонимность/ Секретность/ Конфиденциальность*: Уверенность в том, что данные пользователя недоступны посторонним лицам. Например, уверенность в том, что «никто не читает вашу почту».

2) *Подлинность*: Уверенность в том, что полученные вами данные вами пришли из того места, из которого вы их и ожидали получить. Например, если вы получаете данные с электронной подписью, вы должны быть уверены в том, что они отправлены именно тем человеком, чья подпись там стоит.

3) *Целостность данных*: Уверенность в том, что данные не были изменены на пути от отправителя к получателю.

4) *Контроль доступа*: Предотвращение доступа к тому или иному ресурсу лиц, не имеющих на это прав, а также предотвращение неправильного использования ресурса.

5) *Неотрекаемость*: Механизм, гарантирующий невозможность отказа от факта получения или отправления сообщений или данных. Это понятие является частью проверки подлинности данных.

Одним из решений поставленных целей является использование ЭЦП и шифрование.

6.11.4. Основные сведения об Удостоверяющем Центре

Удостоверяющий Центр (УЦ) – основа автоматизированных систем защищенного документооборота на технологии открытых ключей (PKI).

Схема организации УЦ должна обеспечивать правило: абонент удостоверяющего центра с определенной степенью доверия доверяет любому субъекту, предъявившему сертификат открытых ключей, подписанных (заверенных) в Центре Сертификации – центр доверия всех пользователей (абонентов) системы «Удостоверяющий Центр».

По Федеральному закону от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи», Удостоверяющий Центр в России должен быть юридическим лицом, при этом должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей [29].

Удостоверяющий центр:

– изготавливает сертификаты ключей подписей;

– создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

– приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;

– ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;

– проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;

– выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

– осуществляет, по обращениям пользователей сертификатов ключей подписей, подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;

– может предоставлять участникам информационных систем иные, связанные с использованием электронных цифровых подписей, услуги.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

– вносить сертификат ключа подписи в реестр сертификатов ключей подписей;

– обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;

– приостанавливать действие сертификата ключа подписи по обращению его владельца;

– уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

– иные, установленные нормативными правовыми актами или соглашением сторон, обязательства.

6.11.5. Система удостоверяющих центров

Основные принципы:

Успешная реализация Федеральной программы «Электронная Россия», развитие государственных и коммерческих информационных сис-

тем невозможны без использования средств надежной и оперативной аутентификации пользователей этих систем и контроля целостности исходящих от них электронных документов.

Одним из наиболее совершенных механизмов аутентификации участников информационных систем и контроля целостности электронных документов является электронная цифровая подпись (ЭЦП). В соответствии с федеральным законом «Об электронной цифровой подписи» для подтверждения подлинности ЭЦП должны использоваться сертификаты открытых ключей подписи, выдаваемые удостоверяющими центрами. Удостоверяющие центры составляют основу инфраструктуры открытых ключей (ИОК). Технология ИОК является наиболее эффективной и широко применяемой в мировой практике использования ЭЦП и других услуг информационной безопасности, например, защиты информации от разглашения и несанкционированной модификации.

Таким образом, для создания возможности эффективной работы общероссийской системы электронных торгов необходима развитая инфраструктура удостоверяющих центров. На сегодняшний день в России такой системы нет, поэтому необходимо ее создание.

В мире существует целый ряд органов стандартизации, созданных государственными и коммерческими организациями, а также их объединениями, заинтересованными в развитии ИОК. Утверждённые этими организациями стандарты и рекомендации соответствуют единым принципам и по базовым моментам соответствуют друг другу. Эти документы, а также накопленный богатый опыт их применения целесообразно использовать для создания российской инфраструктуры открытых ключей, что важно в связи с перспективой участия России в международных организациях и ввиду возникающей возможности воспользоваться получившими широкое распространение и активно развиваемыми технологическими решениями, включая открытые платформы разработки программного обеспечения.

Для того чтобы технология ИОК дала максимальный эффект, необходимо урегулировать ряд аспектов, в том числе вопросы правовых отношений и совместимости технологических практик применения открытых ключей различными субъектами. Иными словами, цифровые сертификаты, изданные одними субъектами электронных отношений для собственных нужд, должны быть, при соблюдении определенных соглашений, признаны другими [30].

При формировании системы УЦ (СУЦРФ) необходимо учитывать административно-хозяйственные особенности, географическую распределённость возможных участников и их отраслевую принадлежность.

Первоначально в Федеральном центре, а в последствии и на уровне Федеральных округов может возникнуть необходимость кросс-сертификации электронных коммуникаций между одноранговыми УЦ.

Иерархические ведомственные системы УЦ на уровне Федеральных округов объединяются доверительными связями, создавая горизонтальный уровень (уровни) кросс-сертификации. В случае неприемлемости условий удостоверения подписей между двумя аналогичными структурами, т.е. при недостатке доверия к конкурирующей организации, у субъектов отношений есть выбор использовать окружной УЦ, либо обратиться в независимый УЦ, созданный как отдельная компания, либо как часть подчиненной ведомственной структуры какого-либо федерального органа, например, УЦ Минсвязи или Торгово-промышленной палаты.

Вместе с тем целесообразно создать централизованный механизм доверительных связей между пользователями различных информационных систем. Наиболее полно соответствует этой задаче мостовая модель, при которой ведомственные УЦ организуют доверительные отношения с федеральным мостовым УЦ, основываясь на стандартах и регламентах, представленных УФО.

При использовании системы УЦ с налаженными «мостовыми» связями, абонент одного УЦ сможет передать юридически значимые электронные документы в другой город и в подразделение другого ведомства с достаточной уверенностью в их своевременной доставке и пригодности.

Рассмотрим компоненты архитектуры мостового УЦ (рис. 6.1).

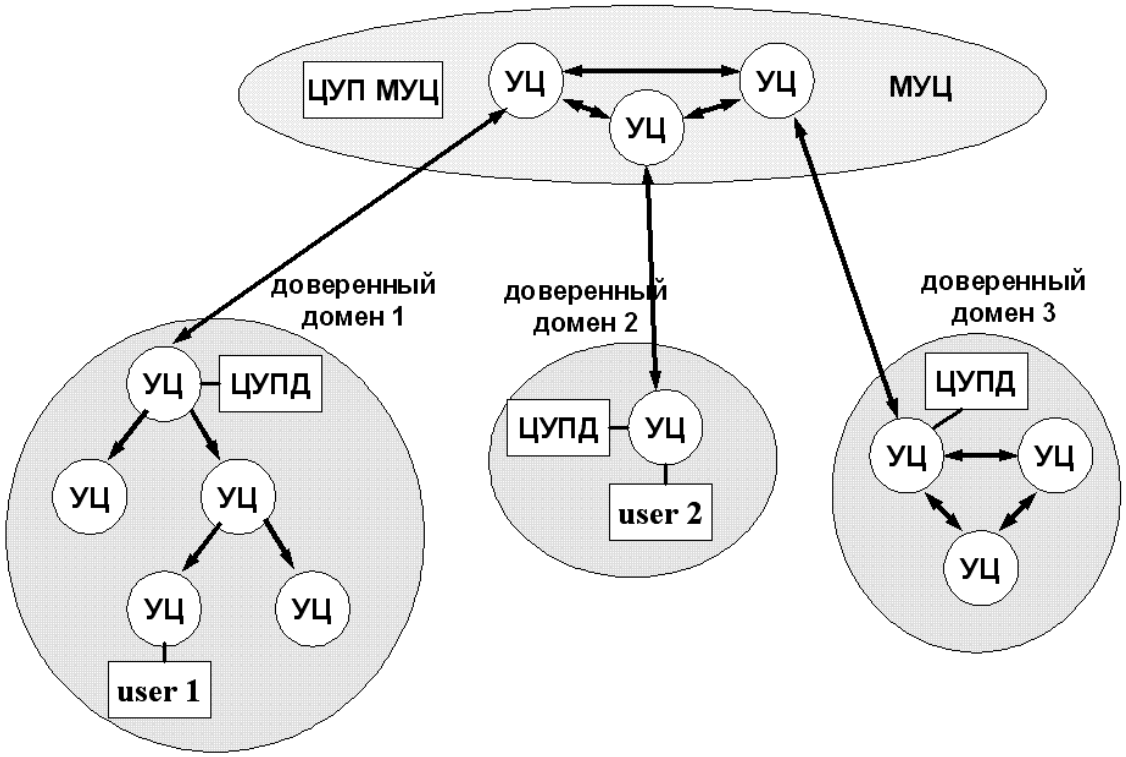


Рис. 6.1. Пример архитектуры мостовой ИОК

СУЦРФ может состоять из следующих компонентов:

– Центр управления политиками (ЦУП) мостового УЦ: устанавливает общие политики Мостового УЦ, проверяет политики доверенных доменов и участвует в кросс-сертификации с доменами ИОК организаций.

– Доверенные домены организаций: В данном контексте это домены ИОК организаций, которые кросс-сертифицировались с мостовым УЦ, и которые функционируют под управлением одного органа управления политиками.

– Центр управления политиками доверенного домена (ЦУПД): этот орган устанавливает политики внутри домена ИОК организации, и контролирует их исполнение;

– Органы сертификации (УЦ):

а) Мостовой УЦ (Bridge УЦ – МУЦ): Это совокупность сильносвязных кросс-сертифицированных УЦ, функционирующих под управлении ЦУП. Его целевое назначение состоит в обеспечении мостов доверия между доверенными доменами ИОК. ЦУП вводит в мостовую инфраструктуру УЦ принципалы через кросс-сертификацию с МУЦ.

б) УЦ принципал (Principal УЦ, РУЦ): Это УЦ внутри доверенного домена, который кросс-сертифицируется с МУЦ. В каждом домене может быть только один УЦ принципал. УЦ принципал обычно совмещен с органами управления политиками домена и/или является точкой доверия домена.

Модели построения доверительных отношений

Выше уже упоминалось, что цифровые сертификаты, изданные одними субъектами электронных отношений, должны быть, при соблюдении определенных соглашений, признаны другими субъектами. Если сертификаты изданы одним удостоверяющим центром, то проблем не возникает. Но в том случае, когда сертификаты изданы разными УЦ, возникает вопрос: как поступать пользователю? Стоит ли доверять информации, указанной в сертификате. Для решения данной проблемы используются три модели построения доверительных отношений.

Модель 1 (иерархическая)

Данная модель характеризуется прямой иерархией доверительных отношений, регистрируемых на уровне единого (федерального, отраслевого, корпоративного и т.п.) корневого удостоверяющего центра (УЦ), который выпускает сертификаты УЦ уровнем ниже. Они в свою очередь выпускают сертификаты УЦ следующего уровня и т.д. до сертификатов конечных пользователей. Таким образом, все образующие домен сертификаты в данной модели связаны в строгом иерархическом порядке и образуют древовидную структуру.

Такая модель существенно упрощает вопросы по обеспечению взаимодействия пересылаемых информационных блоков ЭЦП и сертификатов внутри корневого домена, проверка подлинности приходящего сертификата происходит по ясно выстроенной иерархической «цепочке доверия» – пути следования сертификата.

Иерархическая архитектура имеет следующие преимущества:

– иерархическая архитектура аналогична существующим федеральным и ведомственным организационно-управляющим структурам;

– иерархическая архитектура может быть легко наложена на иерархическое дерево имен;

– иерархическая архитектура определяет простой алгоритм поиска, построения и верификации цепочек сертификатов для всех взаимодействующих сторон.

Вместе с тем использование только иерархической архитектуры без сочетания с другими моделями имеет следующие ограничения:

– для обеспечения взаимодействия конечных пользователей они должны входить в домен одного корневого УЦ;

– компрометация секретного ключа корневого УЦ приостанавливает работу всего домена и требует защищенной доставки нового сертификата до каждого конечного пользователя.

Модель 2 (браузерная)

В данной модели пользователь входит сразу в несколько иерархических доменов ИОК, для чего используются т.н. «списки доверенных удостоверяющих центров», публикуемые той или иной организацией для облегчения проверки сертификатов пользователей из других доменов. В данных списках представляются те УЦ, которым можно доверять при определенных условиях (нередко разные типы бизнес-взаимодействия подразумевают использование услуг разных УЦ).

Для данной модели, ввиду удобства использования получившей широкое распространение среди пользователей сети Интернет, характерно наличие рисков при определении списков доверенных УЦ, обеспечении защиты доверенных списков (публикуемых обычно через веб-браузеры) от несанкционированного изменения.

Модель 3 (сетевая)

В сетевой архитектуре каждый из удостоверяющих центров является независимым, и для установления доверия между центрами, каждая пара центров формирует кросс-сертификат, содержащий два объекта: сертификат открытого ключа первого УЦ, подписанный вторым УЦ, и сертификат второго УЦ, подписанный первым УЦ. В результате взаимной сертификации формируется сетевая (ячеистая) топология доверия, основанная на связи двух ячеек (удостоверяющих центров). В сетевой схеме для взаимной проверки сертификатов двух пользователей может возникнуть несколько путей.

Сетевая архитектура имеет следующие преимущества:

– она более гибкая, чем иерархическая;

– конечный пользователь должен доверять, только центру, издавшему его сертификат;

– возможна непосредственная кросс-сертификация различных УЦ, пользователи которых часто взаимодействуют между собой, что сокращает процесс верификации цепочек;

Вместе с тем использование только сетевой архитектуры имеет следующие недостатки:

– алгоритм поиска и построения цепочек сертификатов для всех взаимодействующих сторон очень сложный;

– пользователь не может предоставить цепочку, которая обеспечивает проверку его сертификата всеми остальными пользователями.

Одним из способов реализации сетевой архитектуры является «мост», через который проходят отношения доверия в виде кросс-сертификатов (рис. 6.2).

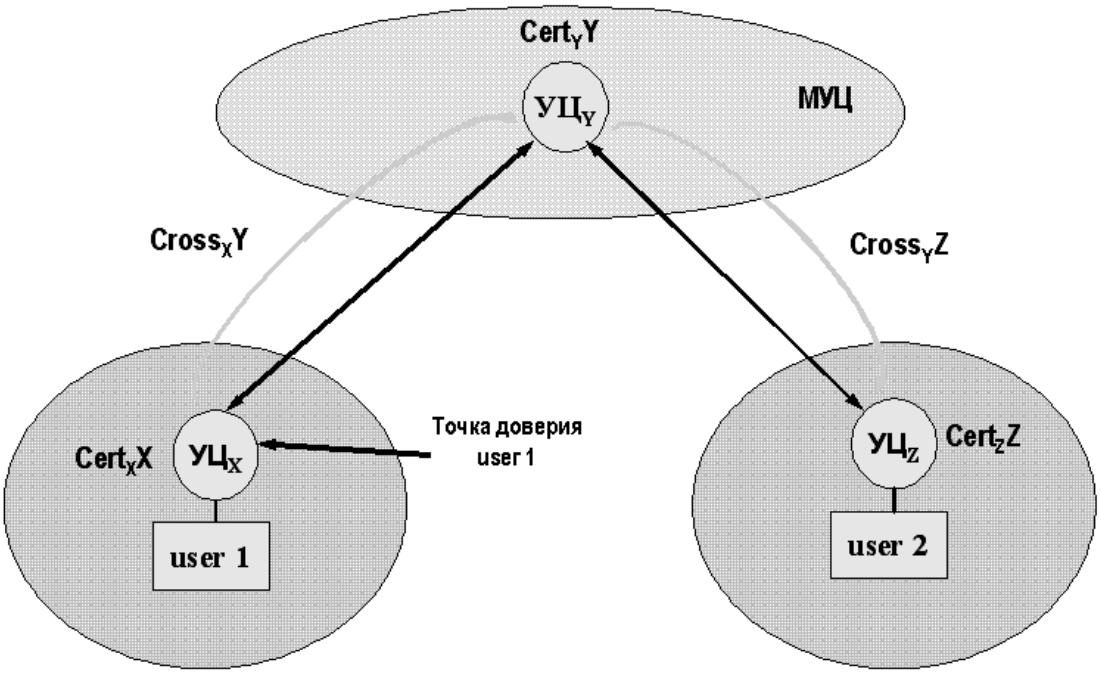


Рис. 6.2. Принцип «моста доверия»

В данном примере если user1, из одного домена ИОК, желает проверить сертификат user2 из другого домена ИОК, то он строит путь сертификации от своей точки доверия через мостовой УЦ (МУЦ) в другой домен используя его как «мост доверия». В данном случае путь сертификации будет иметь вид:

$Cert_X(X) \rightarrow Cert_X(Y) \rightarrow Cert_Y(Z) \rightarrow Cert_Z$ (user2).

Особенности сразу видны из данного примера:

– точки доверия остаются внутри домена ИОК;

– отношения доверия представляют собой кросс-сертификаты;

– домены объединяемых через мост организаций имеют ту архитектуру ИОК, которая им необходима для эффективного функционирования.

Если предположить, что нужно организовать взаимодействие между *n* независимыми доменами ИОК, количество кросс-сертификационных отношений в данном случае будет равно *n*, тогда как в случае с кросс-

сертификацией отдельных доменов – n^2-n. Таким образом, имеет место линейный, а не квадратичный рост числа кросс-сертификационных отношений.

Методы проверки статуса сертификата

Необходимо рассмотреть несколько способов проверки статуса сертификата.

1) Наиболее широкое распространение получил метод использования списка отозванных сертификатов (CRL). Список Отозванных Сертификатов (СОС) формируется с определенной периодичностью, в СОС включаются те сертификаты, которые имеют статус отозванные или приостановленные.

Период публикаций списков отзыва нужно выбирать из соображений компромисса между затратами на публикацию списка и риском того, что клиент не узнает об отзыве сертификата.

В список добавляются только сертификаты, срок действия которых еще не истек, сертификаты с истекшим сроком действия обнаруживаются при обновлении списка и удаляются из него.

2) Для того, чтобы уменьшить размер файла CRL необходимо рассмотреть такой метод как публикация изменения в списках, отозванных сертификатов (delta – CRL) и списков, отозванных удостоверяющих центров (ARL). Несмотря на то, что проверка статуса сертификатов по CRL и delta – CRL является наиболее распространенными способами, они имеют существенные недостатки.

В интервал между опубликованными CRL и проверкой сертификата, может возникнуть ситуация, когда сертификат пользователя в данной момент недействителен, но еще не находится в списке отозванных сертификатов.

3) OCSP – промышленный стандарт протокола и формата представления информации о статусе сертификата для его проверки в on-line режиме. OCSP облегчает проверку статуса сертификата путем централизации хранения CRL и доступа к ним. Специальный модуль – OCSP респондер – берет на себя функцию предоставления приложений информации о статусе сертификата, запрашивая CRL непосредственно у Удостоверяющего Центра, не дожидаясь его официального опубликования.

Данный метод проверки дает более адекватные данные о статусе сертификата, но в его основе лежит все теже CRL, сама технология создания которого допускает возможность их неактуальности.

4) Проверка сертификата в режиме реального времени. В данном методе используется идея запрашивать каталоги сертификатов, хранящиеся в Удостоверяющем Центре напрямую, получая точную информацию о реальном статусе сертификата на момент запроса. Таким образом, пользователь лишается доступа к защищенному ресурсу сразу, как только его сертификат отозван.

7. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

7.1. Общие понятия

Основными объектами защиты информации являются:

Информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией.

- Средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ).

Технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют *объект ТСПИ*.

7.2. Технические каналы утечки информации. Структура, классификация и основные характеристики

Наибольший интерес с точки зрения образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие выход за пределы *контролируемой зоны* (КЗ), т.е. зоны с пропускной системой. Кроме со-

единительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС (рис. 1.1).

Зона с возможностью перехвата разведывательным оборудованием побочных электромагнитных излучений, содержащих конфиденциальную информацию, называется *опасной зоной*. Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется *опасной зоной 1*.

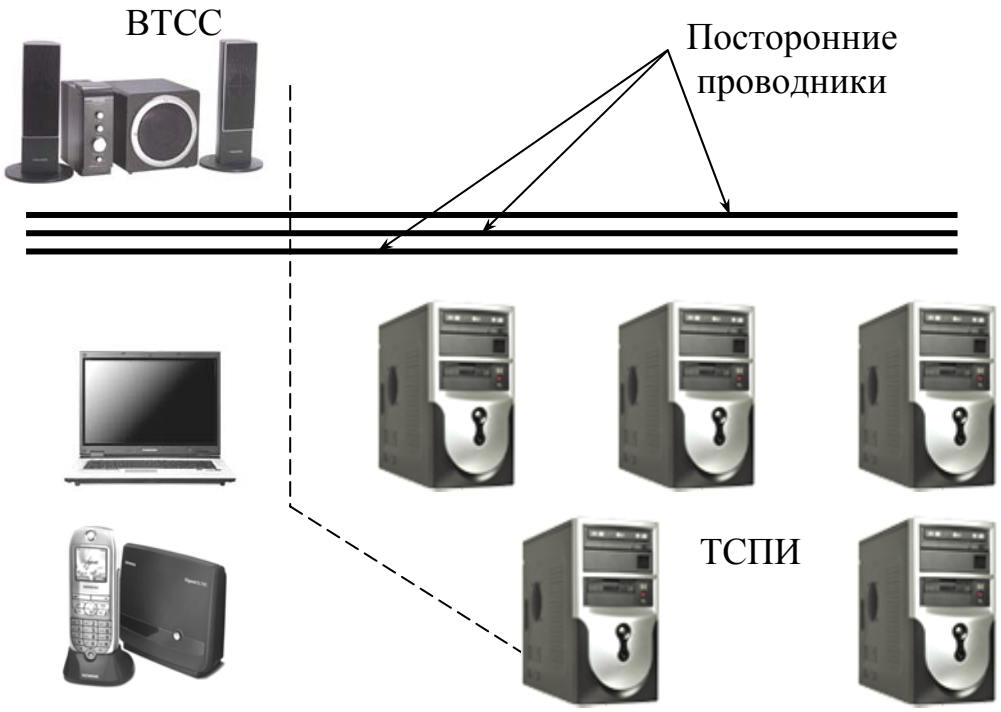


Рис. 7.1. Источники образования возможных каналов утечки информации

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают сосредоточенными и распределёнными. Сосредоточенная случайная антенна представляет собой техническое средство с сосредоточенными параметрами (телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д.). Распределённые случайные антенны образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

Информационные сигналы могут быть электрическими, электромагнитными, акустическими и т.д. Они имеют в большинстве случаев колебательный характер, а информационными параметрами являются амплитуда, фаза, частота, длительность.

Перехват и измерения параметров сигналов осуществляют технические средства обработки информации и технические средства разведки (ТСР).

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал (рис. 7.2). В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте [1].



Рис. 7.2. Технический канал утечки информации (ТКУИ)

В зависимости от физической природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. К таким средам относятся воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т.п.

Противодействие промышленному и экономическому шпионажу является непрерывным и адекватным новым типам угроз процессом развития методов, средств и способов защиты информации.

Классификация каналов утечки информации представлена на рис. 7.3.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации.

Технические каналы утечки информации, обрабатываемой ТСПИ

1. Электромагнитные:

- электромагнитные излучения элементов ТСПИ;
- электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты.

2. Электрические:

- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
- просачивание информационных сигналов в линии электропитания;

- просачивание информационных сигналов в цепи заземления;
- съем информации с использованием закладных устройств.

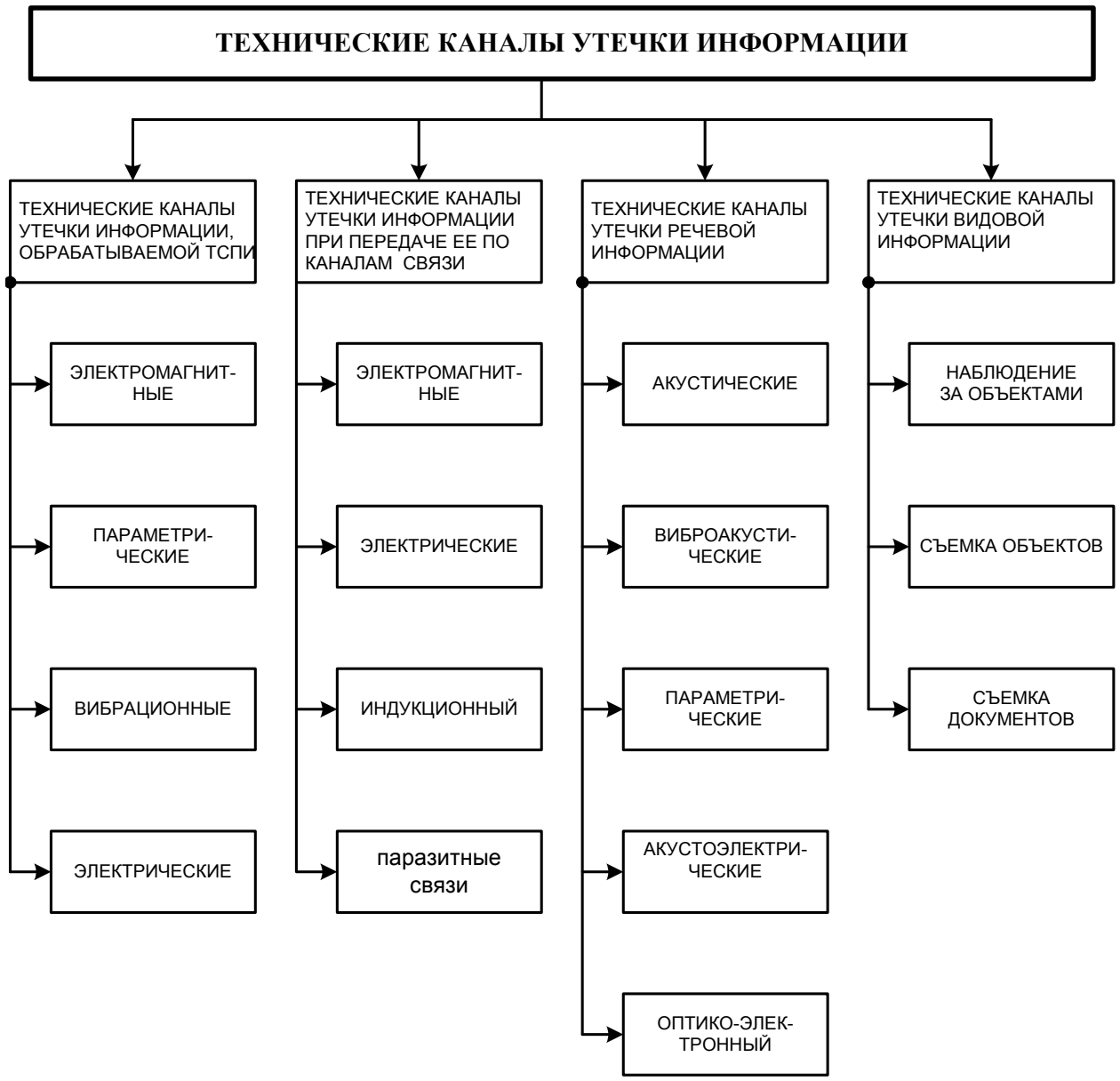


Рис. 7.3. Технические каналы утечки информации

3. Параметрические:

- перехват информации путем «высокочастотного облучения» ТСПИ.

4. Вибрационные:

- соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы:

- электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

2. Электрические каналы:

подключение к линиям связи.

3. Индукционный канал:

эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1. Акустические каналы:

- среда распространения – воздух.

2. Виброакустические каналы:

- среда распространения – ограждающие строительные конструкции.

3. Параметрические каналы:

- результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4. Акустоэлектрические каналы:

- преобразование акустических сигналов в электрические.

5. Оптико-электронный (лазерный) канал:

- облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1. Наблюдение за объектами.

Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2. Съемка объектов.

Для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

3. Съемка документов.

Съемка документов осуществляется с использованием портативных фотоаппаратов

7.3. Аттестация объектов информатизации по требованиям безопасности информации

7.3.1. Общие сведения

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 и создана Гостехкомиссией России в 1995 г. в

соответствии с Постановлением Правительства Российской Федерации «О сертификации средств защиты информации» от 26 июня 1995 г. №608.

Под объектом информатизации, аттестуемым по требованиям безопасности информации, понимают совокупность информационных ресурсов, средств и систем обработки информации (автоматизированные системы различного уровня и назначения), используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, и выделенные (защищаемые) помещения. Выделенное помещение – это специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера. Если в помещении обсуждается конфиденциальная информация, то оно называется защищаемым.

На указанных объектах могут быть установлены вспомогательные технические средства и системы, не участвующие в обработке защищаемой информации, но посредством наводок на которые возможна утечка защищаемой информации. Они также испытываются при проведении аттестации.

Аттестация объектов информатизации – это комплекс организационно-технических мероприятий, в результате выполнения которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект информатизации соответствует требованиям стандартов и иных нормативных и методических документов по безопасности информации, утвержденных ФСТЭК (Гостехкомиссией) России. К нормативно-техническим документам относятся Нормы противодействия акустической речевой разведке (предельные возможности инженерно-технической разведки по добыванию информации), Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от ее утечки по техническим каналам (СТР), а также нормы и требования по защите информации от утечки по каналу ПЭМИН.

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в «Аттестате соответствия».

Нормативно-правовую базу составляют основные документы:

1. «Об информации, информационных технологиях и защите информации». Федеральный закон от 27.07.2006 г. № 149-ФЗ.

2. Постановление Правительства Российской Федерации от 26.06. 1995 г. № 608 «О сертификации средств защиты информации».

3. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. 25.1.1994 г. Гостехкомиссией России).

4. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2002 г.)

5. РД Защита от несанкционированного доступа к информации. Термины и определения.

6. РД Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

7. РД Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

8. РД Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. Государственную тайну составляют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

В некоторых случаях обработки конфиденциальной информации аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Сведения конфиденциального характера – сведения, входящие в следующий перечень:

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

– сведения, составляющие тайну следствия и судопроизводства;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и так далее);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен органами государственной власти в соответствии с

Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

– сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Аттестация предусматривает комплексную проверку объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации:

1. от несанкционированного доступа (в том числе от компьютерных вирусов);

2. от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие);

3. от утечки или воздействия за счет встроенных специальных устройств.

Аттестация объектов информатизации, обрабатывающих сведения, составляющие государственную тайну, проводится специально аккредитованными ФСТЭК России органами по аттестации объектов информатизации согласно положению по аттестации объектов информатизации.

Аттестацию собственных объектов информатизации, обрабатывающих конфиденциальную информацию (не являющуюся государственной тайной), организация может выполнить самостоятельно при наличии лицензии, подготовленных специалистов, соответствующей нормативной и методической литературы, а также контрольно-измерительной аппаратуры и средств контроля защищенности информации.

Порядок проведения аттестации состоит из следующих этапов:

1. подача и рассмотрение заявки на аттестацию;

2. предварительное ознакомление с аттестуемым объектом;

3. испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте;

4. разработка программы и методики испытаний;

5. проведение аттестационных испытаний ОИ;

6. оформление, регистрация и выдача «Аттестата соответствия»;

7. рассмотрение апелляций;

8. осуществление госконтроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации.

Этапы аттестационных испытаний включают в себя:

1. Анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации, раз-

работанной документации и ее соответствия требованиям нормативной документации по защите информации.

2. Определение правильности категорирования объектов ЭВТ и классификации АС, выбора и применения сертифицированных средств и систем защиты информации.

3. Проверка уровня подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации.

4. Проведение комплексных аттестационных испытаний ОИ в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации.

5. Оформление протоколов испытаний и заключения по результатам испытаний с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты в соответствие с установленными требованиями, рекомендациями по контролю за функционированием ОИ.

«Аттестат соответствия» оформляется и выдается не более, чем на 3 года после утверждения заключения по результатам аттестационных испытаний. Ведение сводных информационных баз аттестованных объектов информатизации осуществляется территориальными управлениями ФСТЭК России. Ответственность за выполнение установленных условий функционирования ОИ, технологии обработки защищаемой информации и требований по безопасности информации несет владелец аттестованного объекта информатизации.

Аттестация объекта информатизации на соответствие требованиям по безопасности информации требует совместной работы заказчика и исполнителя. Например, для аттестации автоматизированной системы заказчик разрабатывает и перед аттестацией объекта представляет исполнителю следующие документы:

1. приказ об организации автоматизированного рабочего места (АРМ);
2. приказ об организации работ по защите информации.
3. акт ввода в эксплуатацию АРМ;
4. акт классификации автоматизированной системы;
5. акт категорирования автоматизированной системы;
6. перечень режимных помещений;
7. схему расположения ОТСС на объекте информатизации с привязкой к границе контролируемой зоны и средствам технической разведки;
8. описание технологического процесса обработки информации в АС;
9. перечень лиц, имеющих право доступа к объекту информатизации;
10. перечень программного обеспечения АС;
11. инструкцию по организации антивирусной защиты в АС;
12. матрицу доступа;

13. инструкцию по организации парольной защиты в АС;

14. технический паспорт на объект информатизации;

15. данные по уровню подготовки кадров в области защиты информации;

16. инструкцию администратора безопасности АС;

17. инструкцию по эксплуатации средств защиты АС;

18. перечень защищаемых ресурсов в АС;

19. инструкцию пользователю по обеспечению защиты конфиденциальной информации, обрабатываемой на объекте информатизации.

Исполнитель (лицензиат) в результате проведенных работ разрабатывает следующие документы:

1. согласованную с заказчиком программу аттестационных испытаний объекта информатизации на соответствие требованиям по безопасности информации;

2. протокол оценки защищенности ОТСС АРМ от утечки конфиденциальной информации по каналу ПЭМИ и контроля защищенности информации, обрабатываемой ОТСС, от ее утечки за счет наводок информативного сигнала на линии и коммуникации;

3. протокол контроля эффективности принятых мер защиты информации ОТСС от утечки конфиденциальной информации по каналу ПЭМИН;

4. протокол проведения аттестационных испытаний объекта информатизации на соответствие требованиям по защите информации от несанкционированного доступа;

5. предписание на эксплуатацию объекта информатизации;

6. заключение по результатам аттестационных испытаний на соответствие требованиям по безопасности информации объекта вычислительной техники;

7. акты установки и настройки технических средств защиты информации;

8. аттестат соответствия АС требованиям по безопасности информации.

При аттестации проводятся мероприятия по выявлению и оценке свойств каналов утечки информации. Безопасный уровень сигналов каналов утечки определяется возможностями средств технической разведки. Так как средства технической разведки постоянно совершенствуются, то безопасный уровень сигналов в каналах утечки постоянно снижается. В нормативных документах приведен перечень работ по выявлению каналов утечки информации, который предусматривает:

- специальные проверки (СП);
- специальные обследования (СО);
- специальные исследования (СИ).

В свою очередь, специальные исследования объединяют в себе в общем случае следующие исследования:

- специальные исследования акустических, виброакустических и акустоэлектрических каналов;
- специальные исследования побочных электромагнитных излучений и наводок устройств обработки информации;
- специальные исследования линий электропитания устройств обработки информации.

Специальные проверки представляют собой проверки технических средств и систем (ТСС) объекта защиты с целью выявления закладных устройств и технических доработок по изменению свойств ТСС. При проведении специальных проверок применяются специализированные технические средства.

Специальные обследования (поисковые мероприятия) на объекте в наиболее распространенном случае состоят из:

- радиообнаружения;
- осмотра помещения;
- обследования электрических и электронных приборов;
- проверки проводных коммуникаций.

Специальные исследования **объединяют в себе в общем случае следующие исследования:**

специальные исследования акустических, виброакустических и акустоэлектрических каналов утечки информации;

специальные исследования побочных электромагнитных излучений и наводок устройств обработки информации;

специальные исследования линий электропитания устройств обработки информации.

7.3.2. Мероприятия по выявлению и оценке свойств каналов утечки информации

Подробно и конкретно комплекс вопросов по выявлению каналов утечки информации рассмотрен в [2]. Краткое изложение и основные положения приведенного ниже материала соответствуют этому источнику.

Наличие каналов утечки информации определяется физическими свойствами среды распространения сигналов и характеристиками источников информации. Каналы утечки информации на объектах существуют всегда, но опасность они представляют только тогда, когда их информационные сигналы могут быть зафиксированы за пределами контролируемой зоны и расшифрованы. Для безопасности информации необходимо, чтобы уровень сигналов в каналах утечки был ниже воспринимаемого средствами технической разведки или же позволял маскирование сигналов. Сказанное не относится к информационным каналам с шифрованием сигналов.

Безопасный уровень сигналов каналов утечки определяется возможностями средств технической разведки. Так как средства технической разведки постоянно совершенствуются, то безопасный уровень сигналов в каналах утечки постоянно снижается.

Для обоснованного выбора действий по нейтрализации каналов утечки информации необходимо их выявить, произвести оценку реальной угрозы утечки информации и выработать необходимый комплекс защитных мер. Важное значение для оценки реальной угрозы утечки информации имеет определение уровня сигналов в каналах утечки.

7.3.2.1. Специальные проверки

Специальная проверка состоит из нескольких последовательно выполняемых действий:

- прием-передача проверяемого технического средства представителям исследовательских лабораторий сертификационных центров;
- составление программы проведения специальной проверки технического средства;
- проведение проверки;
- анализ результатов проверки, составление отчетных протоколов.

Кроме технического средства, представители организации обязаны предоставить для разработки программы проверки:

- данные о техническом средстве;
- сведения о его планируемом применении;
- данные о месте размещения технического средства.

Данные о техническом средстве должны содержать сведения о его назначении и полной комплектации, способ приобретения с указанием сведений об организации-поставщике.

Данные о планируемом применении должны содержать сведения:

- планируется ли техническое средство для обработки закрытой информации;
- есть ли высший гриф секретности у обрабатываемой или обсуждаемой информации;
- в составе какой информационной системы планируется работа технического средства;
- к каким коммуникационным системам планируется подключение технического средства.

Сведения о планируемом размещении технического средства должны содержать:

- описание объекта информатизации, на котором планируется использовать техническое средство;
- перечень охраняемых сведений объекта информатизации;
- минимальное расстояние до границы контролируемой зоны;

- наличие посольств, представительств и мест пребывания иностранных граждан с указанием расстояния до контролируемой зоны;
- возможность и периодичность пребывания иностранных делегаций на объекте.

Типовой перечень операций проведения специальных технических проверок состоит из:

- дозиметрического контроля изделия в упаковке для обнаружения радиоактивных меток и радиоизотопных источников питания;
- токовихревого контроля узлов технических средств обработки информации, не содержащих металлических включений;
- контроля упаковки, которая по назначению не должна иметь полупроводниковых приборов, нелинейным локатором для выявления специального электронного устройства, выполняющего роль маяка для определения местоположения технического средства;
- проведения радиоконтроля для выявления активных закладных устройств передачи информации по радиоканалу;
- проверки возможности съема информации методом высокочастотного навязывания;
- разборки технического средства с последующим осмотром его узлов для выявления отклонения от схемотехнических и конструкторских решений;
- измерений импедансов некоторых узлов технических средств для выявления отклонений от нормы из-за возможно внедренных аппаратных закладок;
- рентгенотелевизионного и визуально-оптического контроля внешнего вида и внутренней структуры узлов и элементов технических средств (сложные виды контроля проводятся по специальным методикам);
- рентгенографии или рентгеноскопии неразборных узлов и элементов технических средств с целью выявления схемных изменений.

Итогом анализа исходных данных, схемотехнических особенностей и иных необходимых сведений с учетом классификации электронного устройства должен явиться перечень каналов утечки информации и возможно внедренных аппаратных закладных устройств.

По результатам проведения специальной проверки руководитель проверяющей группы делает вывод о наличии или отсутствии закладных электронных устройств и оформляет акт с перечислением проверенных элементов, видов технических проверок и фамилий и инициалов проводивших отдельные виды проверок лиц. Акт оформляется в единственном экземпляре и хранится у исполнителя. Заключение составляется в двух экземплярах (для исполнителя и заказчика). Акт и заключение утверждаются руководителем организации-исполнителя.

7.3.2.2. Специальные обследования

Под специальными обследованиями выделенных помещений понимают комплекс поисковых мероприятий по выявлению возможно установленных электронных устройств съема информации в ограждающих конструкциях, предметах интерьера, бытовых приборах и проводных коммуникациях. Поисковые мероприятия проводятся в местах, где возможна утечка конфиденциальной информации (кабинетах руководства, помещениях для переговоров, в загородных резиденциях, саунах, автомобилях) для своевременного обнаружения прослушивающих устройств и ликвидации угрозы перехвата информации. Специальные обследования, как правило, проводятся с применением специальных технических средств.

Задачи поисковых мероприятий:

- определение состояния информационной безопасности объекта;
- поиск каналов утечки информации;
- поиск установленных приборов и систем перехвата и передачи информации;
- выдача рекомендаций по оптимальным способам блокирования каналов утечки информации.

При поиске каналов утечки информации производятся следующие виды работ:

1. Радиомониторинг – контроль радиоэфира в районе объекта поиска для выявления различных классов подслушивающих устройств (ПУ), использующих в качестве канала передачи радиоэфир. При радиомониторинге возможно выявить лишь «активные» ПУ, т.е. излучающие радиосигнал на момент проведения проверки.

- Применяемое оборудование: комплекс радиоконтроля, который позволяет обнаружить и локализовать микрорадиопередатчики, составить карты загрузки радиоэфира (базы данных принятых радиосигналов и их характеристик). Эти карты послужат исходным материалом при проведении последующих проверок на объекте.

2. Физический поиск средств перехвата информации является наиболее трудоемкой составляющей поискового мероприятия, в результате которого могут быть обнаружены практически любые типы заносных и закладных ПУ, а также косвенные признаки их установки. При этом тщательно осматриваются вероятные места установки ПУ (полости и щели в плинтусах, стенах, за батареями отопления, труднодоступные места на шкафах, карнизах, полости подвесного потолка и т.д.). Особое внимание уделяется предметам «неизвестного происхождения», которые возможно быстро заменить.

- Применяемое оборудование: досмотровые зеркала, фонарь, эндоскоп.

3. Проверка электронной техники заключается в обнаружении ПУ, установленных в бытовой и офисной аппаратуре, расположенной в проверяемом помещении. Выявление ПУ, производится визуально (при разборке) и при помощи специальных поисковых приборов.

• Применяемое оборудование: комплект специальных инструментов, детектор электромагнитного поля с частотомером. Для более серьезных проверок можно добавить портативный рентгеновский аппарат.

4. Проверка кабельных коммуникаций предназначена для обнаружения ПУ, использующих силовые и слаботочные проводные линии в качестве канала передачи информации или в качестве источника питания ПУ. Отдельным видом работ при этом является проверка телефонных линий. Помимо канала передачи и источника питания ПУ, телефонная линия является носителем информации и поэтому требует отдельного исследования на наличие телефонных ПУ (радиопередатчиков, диктофонных адаптеров и т.д.).

• Применяемое оборудование: анализатор проводных линий, анализатор параметров телефонной линии, проводной приемник, усилитель НЧ-сигналов, комплект специальных инструментов и принадлежностей, контрольно-измерительные приборы (мегомметр, мультиметр).

5. Проверка предметов интерьера заключается в тщательном обследовании мебели, книг, картин, сувениров, папок с бумагами, видеокассет и т.д. Особое внимание уделяют всякого рода укрепляющим брускам-подставкам и способам их крепления, поскольку ПУ, закамуфлированное под элементы мебели, крепится, как правило, на шипах или подобных элементах.

• Применяемое оборудование: нелинейный локатор, селективный металлодетектор, эндоскоп, досмотровые зеркала и специальные инструменты. Может применяться рентгеновская аппаратура.

6. Проверка ограждающих конструкций – поиск ПУ, стационарно установленных в стенах и строительных конструкциях. Производится проверка конструкций на наличие акустических и вибрационных каналов утечки информации. Обнаруживаются «активные» и «пассивные» (не работающие на момент проверки) ПУ.

• Применяемое оборудование: нелинейный локатор, селективный металлодетектор, тестовый микрофон и стетоскоп.

По окончании работ предоставляется «Отчет о результатах работ» с детальным описанием выявленных каналов утечки информации и подробными рекомендациями по их блокированию

Рассмотрим выполнение наиболее важных поисковых мероприятий.

Радиообнаружение. Современные программно-аппаратные комплексы (например, RS turbo) за счет зондирующего акустического сигнала позволяют проводить обнаружение и локализацию сравнительно простых радиозакладных устройств с постоянной несущей частотой и передачей

по открытому каналу. Несмотря на небольшую вероятность применения такие радиозакладные устройства исключать из рассмотрения нельзя.

Универсальными методами обнаружения радиозакладных устройств являются сравнительный радиоконтроль и энергетическая локализация с помощью индикаторов электромагнитного поля.

Применяемое оборудование: комплекс радиоконтроля, который позволяет обнаружить и локализовать микрорадиопередатчики, составить карты загрузки радиоэфира (базы данных принятых радиосигналов и их характеристик). Эти карты послужат исходным материалом при проведении последующих проверок на объекте.

Осмотр помещения. Осмотр помещения подразделяется на первичный осмотр и техническую проверку [2].

Первичный осмотр проводится как визуальный контроль помещения и находящихся в нем предметов. Если имеется план или фотографии, то производят сверку фактического размещения предметов с документально зафиксированным. Электронные приборы временно удаляют или размещают в определенном месте. Мебель отодвигают от стен и осматривают содержимое ящиков. Регистрируют наименования предметов, серийные номера, номера печатей и пломб.

Осматривая стены и потолок, обращают внимание на крепления плиток, наличия на них царапин, на наличие посторонних предметов в межпотолочном пространстве.

Осветительные приборы снимают, разбирают и осматривают. Обследуют ниши и подводящие провода электророзеток.

С помощью эндоскопов и осмотровых зеркал обследуют вентиляционные короба.

В местах установки отопительных батарей обследуют ниши, места ввода труб в стены, межсекционные пространства.

Проверяют также предметы, находящиеся на стенах, мебель, складки обивки мягкой мебели, сувениры, игрушки и т.п.

Техническую проверку предметов мебели и интерьера проводят при помощи нелинейного локатора и портативного рентгеновского аппарата на подготовленной для этой цели площадке. После проверки подозрительные предметы желательно промаркировать специальными невидимыми при обычном освещении метками.

Последним этапом аппаратурной проверки является обследование ограждающих конструкций нелинейным локатором.

Линии проверяют на наличие модулированных высокочастотных сигналов, а слаботочные линии – на наличие информационных низкочастотных сигналов.

При проверке линий их отключают от распределительных щитков, подключают к локатору коммуникаций и нагружают на эквивалентное

сопротивление. По результатам локации определяют наличие или отсутствие закладных устройств.

Применяемое оборудование: анализатор проводных линий, анализатор параметров телефонной линии, проводной приемник, усилитель НЧ-сигналов, комплект специальных инструментов и принадлежностей, контрольно-измерительные приборы (мегомметр, мультиметр).

7.3.2.3. Специальные исследования

Под специальными исследованиями согласно ГОСТ Р 51624-00 понимают выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

Оценка соответствия защиты информации требованиям нормативных документов невозможна без объективных измерений уровня информационных сигналов в крайних точках канала утечки. В одних случаях определяется уровень сигналов утечки информации непосредственно у источника и расчетным путем производится его оценка на границе контролируемой зоны, в других случаях измерение сигналов утечки информации производится на границе контролируемой зоны, чем обеспечиваются более объективные результаты. Без такой оценки невозможно выявление опасности каналов утечки информации – основной задачи специальных исследований.

Конечным результатом специальных исследований должно быть вычисление отношения сигнал/шум и сравнение полученного значения с нормированными значениями.

До проведения специальных исследований необходимо провести детальный анализ особенностей всех технических средств ОИ, составить список исследуемых устройств и помещений и в обязательном порядке результаты зафиксировать в протоколах в качестве обоснования выбора опасных каналов утечки информации. Эта работа проводится совместно заказчиком и исполнителем.

В большинстве случаев выявление возможных характеристик опасных сигналов производится в тестовых режимах работы технического средства. Тестовые режимы позволяют установить необходимый уровень и форму опасного сигнала и гарантированно его выделить при измерении на фоне других сигналов по известным признакам.

Измерение опасных сигналов должно в обязательном порядке проводиться только средствами измерений, внесенными в Госреестр средств измерений и имеющими не просроченное «Свидетельство о поверке». В некоторых случаях измерительные системы и комплексы должны иметь сертификат ФСТЭК России.

Специальные исследования акустических и виброакустических каналов

Специальные исследования в области акустики проводятся в основном применительно к выделенным (защищаемым) помещениям (ВП, ЗП). Исследуемыми объектами являются ограждающие помещение конструкции, все каналы, трубопроводы и другие проводящие звук инженерные конструкции.

В протоколе специальных исследований (СИ) в области акустики и виброакустики в [2] рекомендуется отразить:

- *название организации*, выполняющей СИ, ссылку на его лицензии и название объекта СИ;
- *объекты контроля* и их краткое описание;
- *уровень защиты* для каждого из них (категория помещения);
- *размещение помещения*;
- *перечень граничащих с ВП помещений* во всех направлениях с приведением плана размещения по отношению к смежным помещениям;
- *перечень* ограждающих конструкций ВП.

Для ВП должны быть заранее известны границы контролируемых зон отдельно для акустических и виброакустических каналов. Должны быть также проанализированы особенности структуры ограждающих конструкций с целью выбора для исследований опасных участков, на которых возможна утечка акустической информации.

Действующая методика измерений акустических и виброакустических характеристик различных сред базируется на определении двух величин – звукового давления в воздушной среде и виброускорения на поверхности твердого тела [2]. Обе величины определяются специальными устройствами на основе шумомеров, на вход которых подаются сигналы от измерительных датчиков-микрофонов и акселерометров. Звуковые тест-сигналы формируются акустическими генераторами с регулируемыми по уровню и частотным характеристикам выходными акустическими сигналами.

Кроме комплектов измерительных приборов существуют программно-аппаратные комплексы для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическим и виброакустическим каналам, а также за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств, образованных за счет акустоэлектрических преобразований. Из таких комплексов наиболее известными являются «Трап», «Спрут», «Шепот» и «Гриф».

Программно-аппаратный комплекс «Спрут-7» состоит из трех подсистем:

– измерительной подсистемы;

– подсистемы источника тестового акустического сигнала;

– подсистемы управления.

Специальное программное обеспечение (СПО) предназначено для управления измерительным модулем и модулем источника тестового акустического сигнала, получения результатов измерений, их обработки, отображения и сохранения в необходимом формате.

Внешний вид главного окна программы управления показан на рис. 7.1.

Главное окно программы имеет две основные области:

– панель измерительного модуля;

– панель источника тестового акустического сигнала.

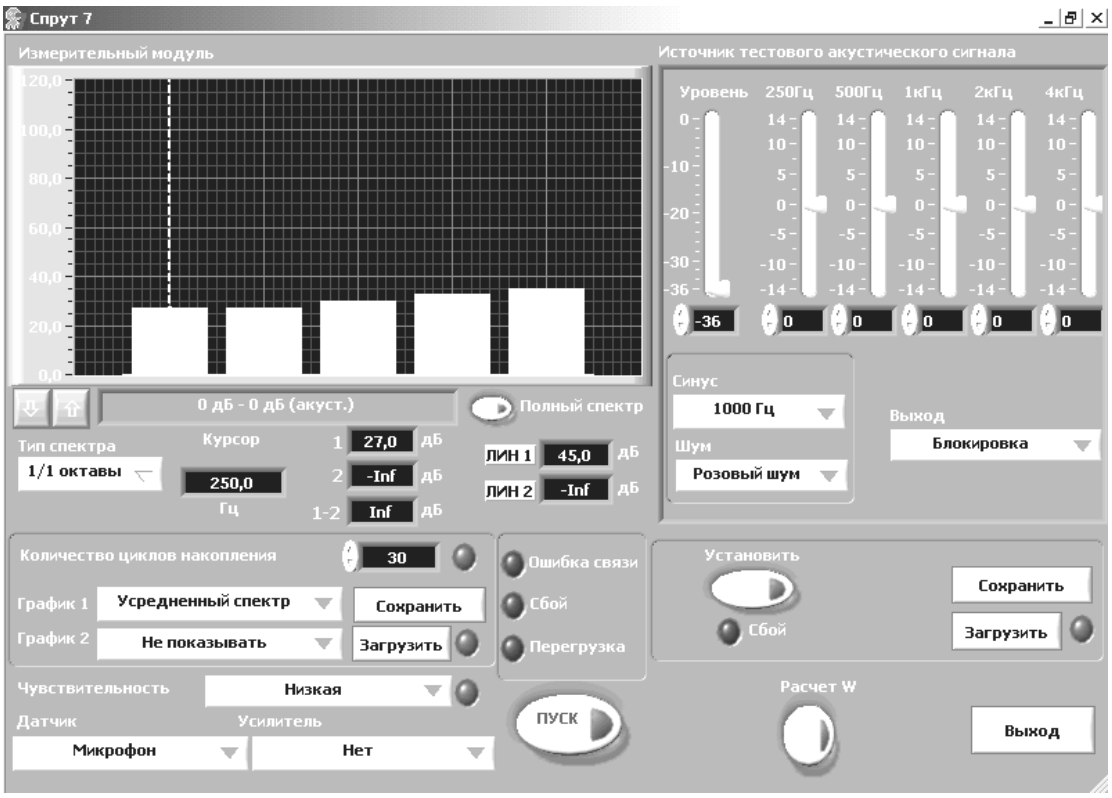


Рис. 7.1. Внешний вид главного окна СПО «СПРУТ-7»

Рассмотрим некоторые особенности акустических и виброакустических исследований ВП.

На рис. 7.2. схематично показано выделенное помещение с некоторыми важными потенциальными каналами утечки акустической и виброакустической информации, к которым относятся оконные и дверные проемы, стены и перегородки, перекрытия потолка и пола, система вентиляции, система отопления.

Согласно схеме помещения акустические исследования необходимо проводить для ограждающих конструкций (дверные проемы, стены и перегородки, перекрытия потолка и пола), а виброакустические – для инженерных конструкций (системы отопления и вентиляции), окон и железобетонных элементов ограждающих конструкций.

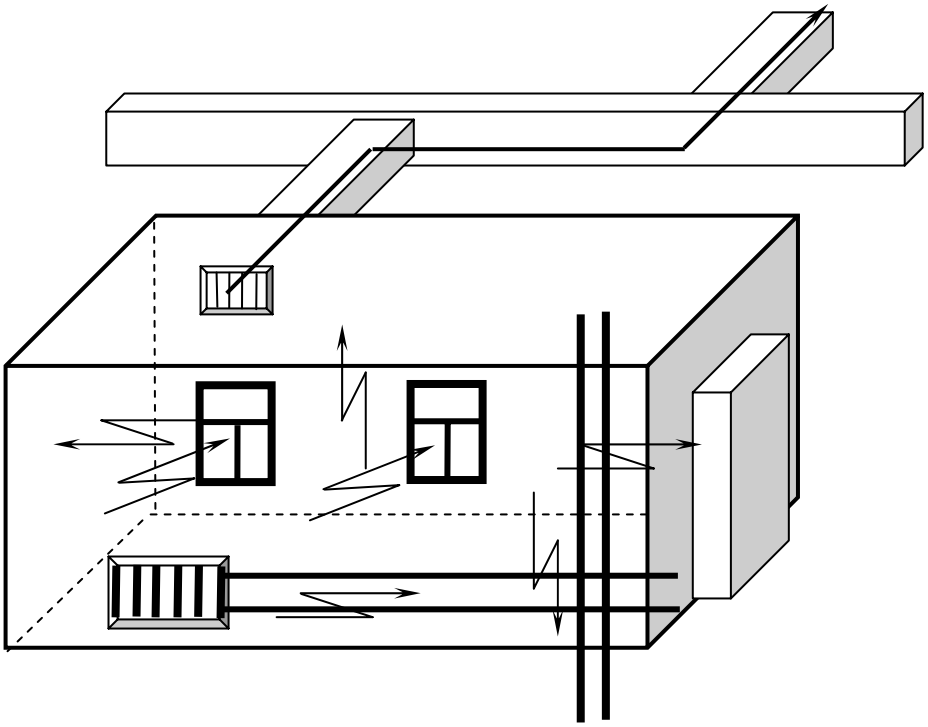


Рис. 7.2. Схема выделенного помещения

При акустических измерениях измерительные приборы располагаются согласно стандартной схемы – излучатель тестового сигнала (экранированная акустическая колонка) располагается на расстоянии 1,0 м от конструкции на высоте 1,5 м от пола; первый микрофон, измеряющий уровень падающей на конструкцию звуковой волны, располагается на расстоянии 0,5 м перед конструкцией; второй микрофон, измеряющий уровень прошедшей через конструкцию звуковой волны, устанавливается на расстоянии 0,5 м за конструкцией (рис. 7.3).

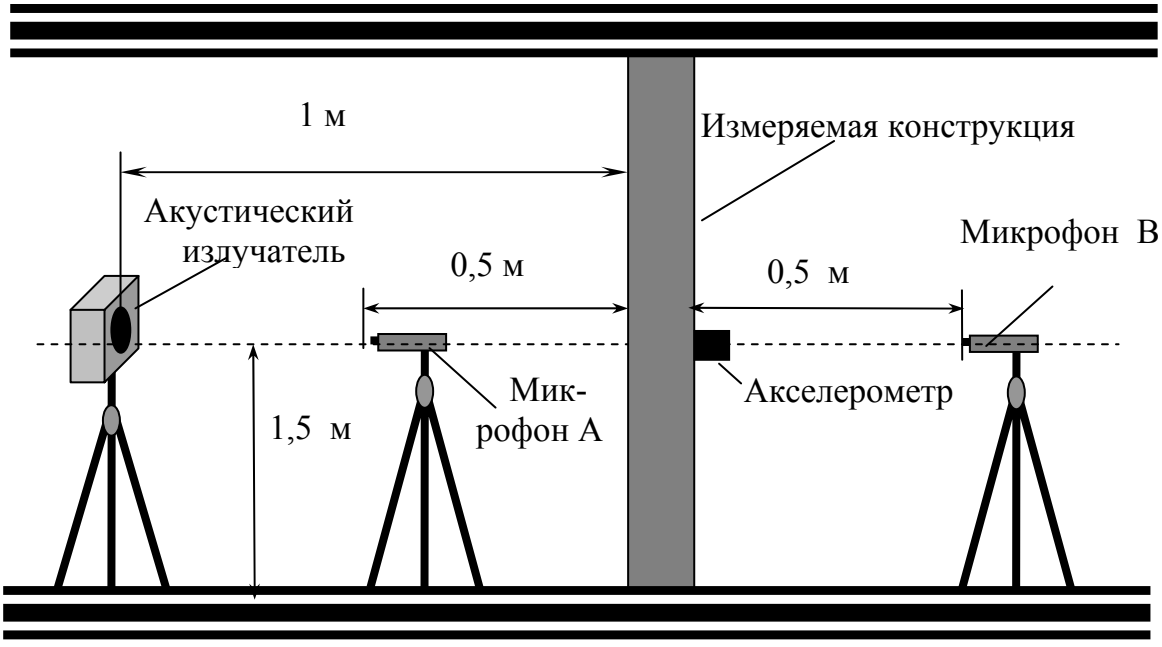


Рис. 7.3. Схема измерения акустических и виброакустических характеристик стены (перегородки)

Если стена однородна, то достаточно одного или двух замеров вдоль стены. Если же стена неоднородна или имеет трещины и отверстия, то число контрольных точек необходимо увеличить, располагая их через 1,5…2 м друг от друга [2]. Для неоднородной стены измерению подлежит каждый ее элемент в отдельности и выводы делаются по наиболее «слабому» элементу.

Аналогично выполняются измерения и по виброакустическому каналу как при первоначальных исследованиях, так и при проверке эффективности средств активной звуковой защиты.

Измеритель вибрационных ускорений (акселерометр) крепится плотно к стене с противоположной стороны с помощью специального клея или приспособлений. Крепление акселерометра к рыхлой штукатурке, обоям и прочим мягким покрытиям недопустимо, так как в этом случае результаты измерений будут ошибочны из-за гашения виброколебаний этими материалами.

На рис. 7.4. показана типовая схема измерения перекрытия пола. Расположение акустического излучателя согласно регламентирующим документам может быть иным, чем показано на схеме – допускается его установка на месте источника звука (рабочий стол руководителя, трибуна для выступлений и т.д.). При этом размещение датчиков не меняется.

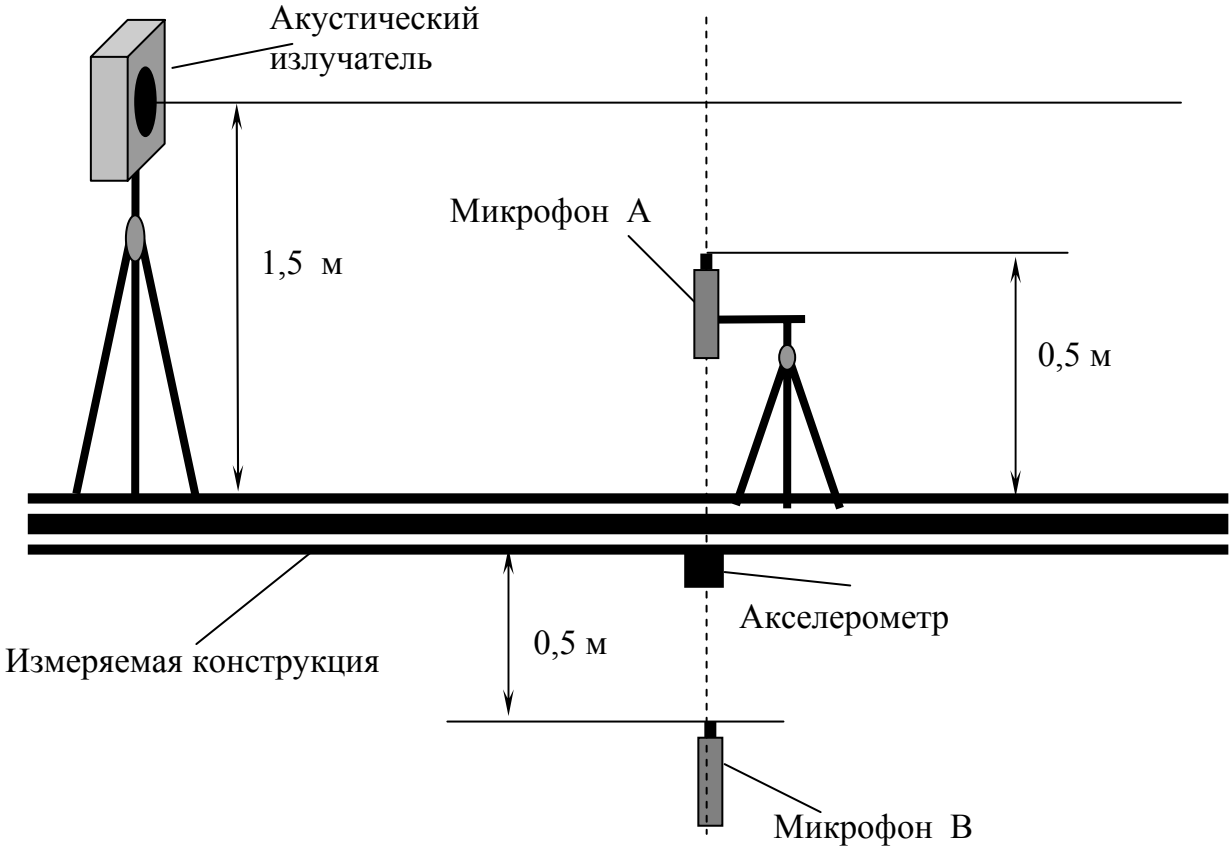


Рис. 7.4. Схема измерения акустических и виброакустических характеристик перекрытия пола

Схема измерения перекрытия потолка несколько отличается от схемы измерения перекрытий пола. Излучатель в обоих случаях размещается над полом, а микрофоны А и В по обе стороны ограждающей конструкции. При измерениях перекрытия потолка микрофон А размещается под потолком на расстоянии 0,5 м и развернут вертикально вниз (к источнику тест-сигнала). Микрофон В располагается над полом вышерасположенного помещения (т.е. над перекрытием потолка) на высоте 0,5 м и направлен вертикально вниз. Расположение микрофона В не зависит от наличия фальш-потолка.

Вибрационный канал утечки надо рассматривать (кроме окон) на границе контролируемой зоны, так как внутри зоны перехват информации обязаны исключить службы защиты информации заказчика.

На рис. 7.5. показана схема измерения акустических характеристик двойного дверного проема.

При акустических измерениях необходимо следить, чтобы полотна дверей были плотно прикрыты и имели звукопоглощающие уплотнения.

На рис. 7.6 показана схема измерений на окне. Следует заметить, что окна в общем случае могут служить оптическим, акустическим, виброакустическим и оптико-электронным каналами утечки речевой информации. Если окна расположены на нижних этажах, то проведение акустических измерений на звукоизоляцию оконных проемов не представляет особого труда. Они проводятся по рассмотренной схеме.

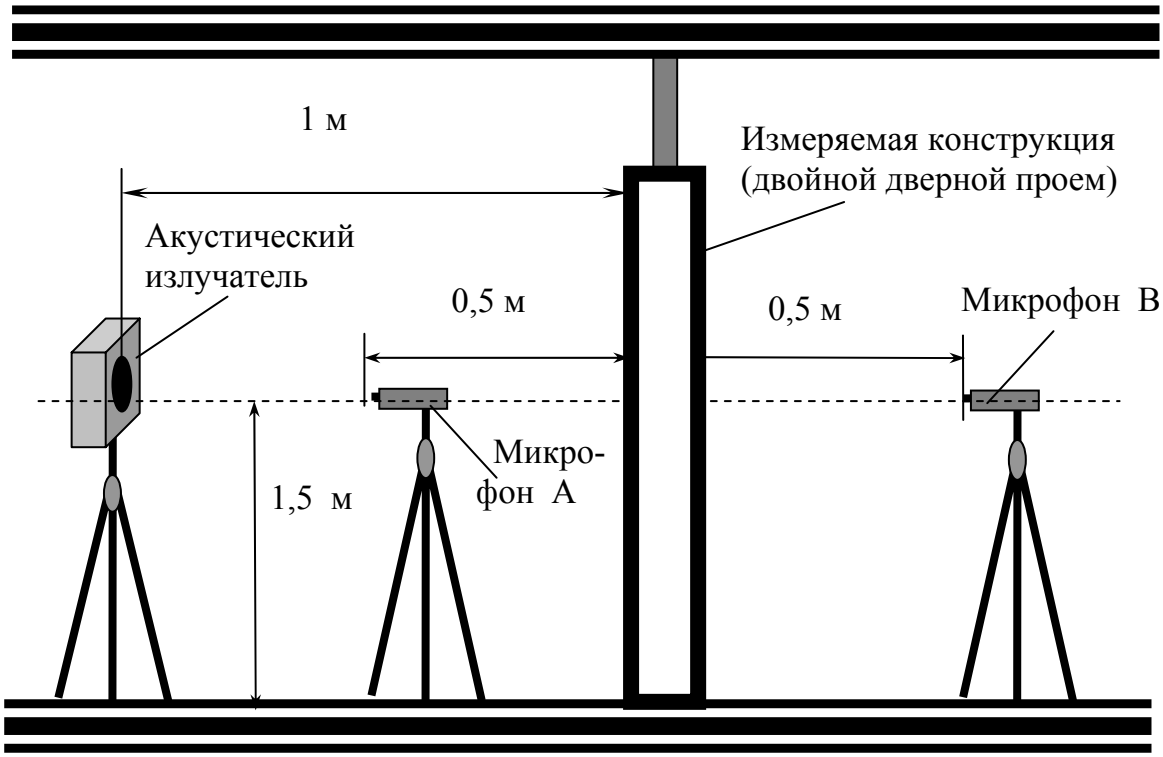


Рис. 7.5. Схема измерения акустических характеристик двойного дверного проема

Измерения защищенности по вибрационному каналу на остеклении окон с помощью оптико-электронной аппаратуры дистанционного прослушивания речи надо проводить с учетом некоторых особенностей, связанных с вертикальными размерами окон. Верхняя часть окон в большинстве случаев расположена значительно выше осевой линии акустического излучателя (выше 1,5 м от пола).

При проведении измерений в нижней и верхней частях окна на одинаковых предписанных расстояниях микрофона А (0,5 м) от плоскости стекол значение уровня падающей звуковой волны в верхней части окна будет на 3–8 дБ ниже, чем в нижней части [38].

При расчетных соотношениях сигнал/шум вблизи нормативных значений это может привести к ошибочным выводам. Поэтому для исключения подобной ситуации необходимо повторить измерения, поместив микрофон напротив центров верхних фрамуг.

В коробе распространяется сферическая звуковая волна со снижением звукового давления пропорционально третьей степени расстояния от источника звука. Поэтому расчеты защищенности в плоскости решетки и на расстоянии 0,5 *м* будут отличаться в несколько раз [2]. Уровень тестирующего сигнала зависит от характера решаемой задачи, общей рекомендацией является установка его не менее 10 дБ выше уровня шумов [2].

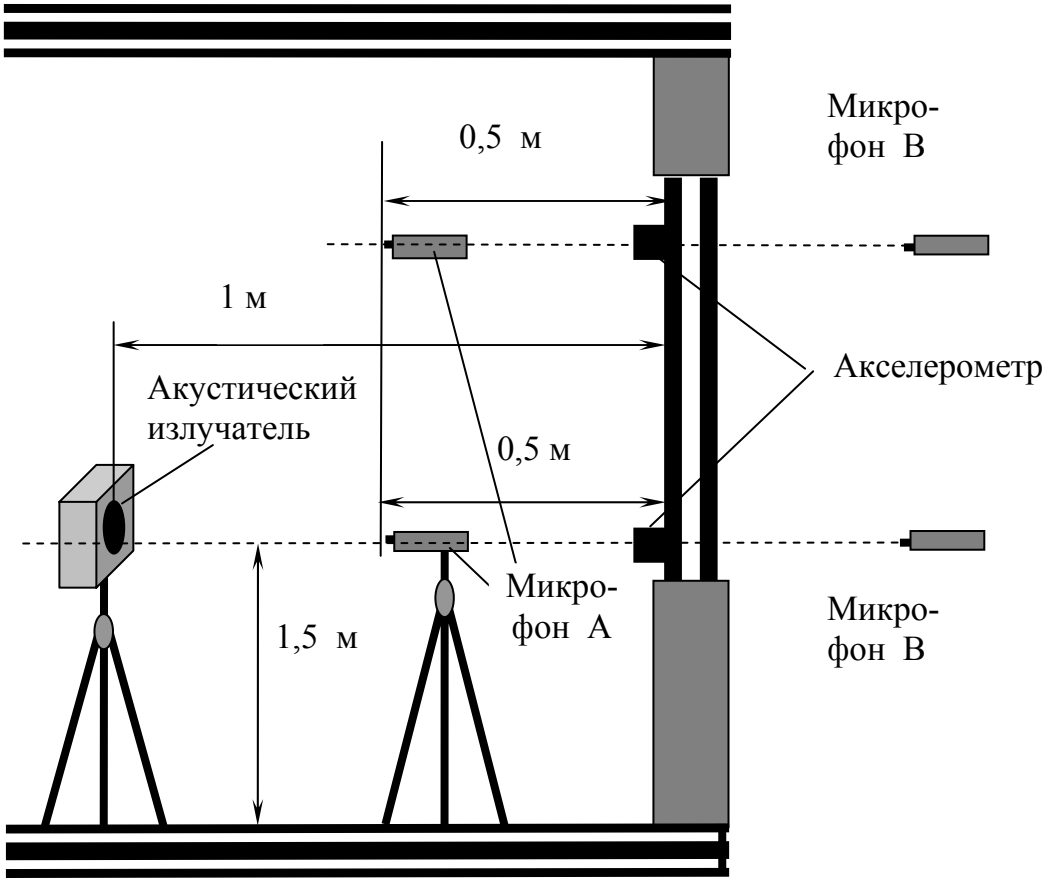


Рис. 7.6. Схема измерений на окне

Измерение в каналах вентиляционной системы производится по схеме, представленной на рис. 7.7. Излучатель располагается вблизи входа канала вентиляции на высоте 1,5 м от пола (расстояние от стены в 1 *м* не регламентируется). Микрофон А устанавливается на расстоянии в 0,5 м по нормали к плоскости вентиляционной решетки с ориентацией на нее. Микрофон В устанавливается в плоскости ближайшего по ходу вентиляционного канала окна также с ориентацией на решетку окна. Это связано с тем, что при непреднамеренном прослушиванием, например, во время ремонтно-профилактических работ, ухо постороннего может оказаться в этой же плоскости.

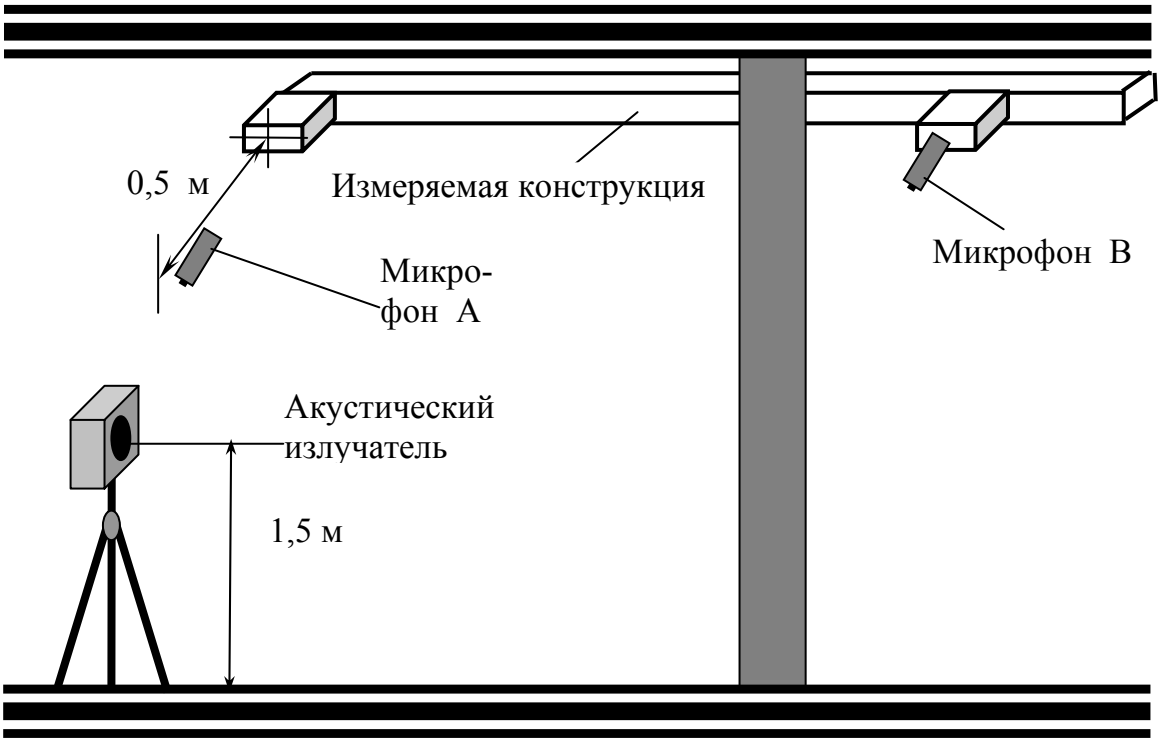


Рис. 7.7. Схема измерения в канале системы вентиляции

При измерениях на окнах при одиночных стеклах вполне достаточно давления 60…65 дБ, для стеклопакетов – 70…80 дБ. При измерениях на дверных проемах общего типа, в том числе и двойных, необходим уровень тестирующего сигнала 70…75 дБ, а для дверей с усиленной звукоизоляцией – до 90 дБ. Для стен и капитальных перегородок уровень тест-сигнала необходимо поднимать до допустимого максимума.

Измерения на системе отопления (рис. 7.8), представляющей собой виброакустический канал утечки речевой информации, на трубах отопления рекомендуется проводить в следующем порядке [2].

Акустический излучатель располагается относительно плоскости батареи, являющейся наиболее эффективным приемником звуковой волны. Микрофон А направляется на излучатель и располагается на расстоянии 0,5 м от плоскости батареи по ее центру.

Если границей контролируемой зоны являются ограждающие конструкции выделенного помещения, то акселерометр закрепляется поочередно на трубах на расстоянии 10…15 см от места выхода трубы из выделенного помещения.

Если же границей контролируемой зоны являются стены здания, в котором находится контролируемое помещение, то в связи со значительным затуханием вибрационного тест-сигнала до точки установки акселерометра прямой замер защищенности становится невозможным. В подобном случае надо размещать акселерометр на таком расстоянии от выделенного помещения, на котором тест-сигнал надежно измеряется, а результаты измерения защищенности от утечки удовлетворяют требованиям. На этом основании делается вывод, что на границе контролируемой зоны вследствие дальнейшего затухания тест-сигнала результаты будут еще лучше.

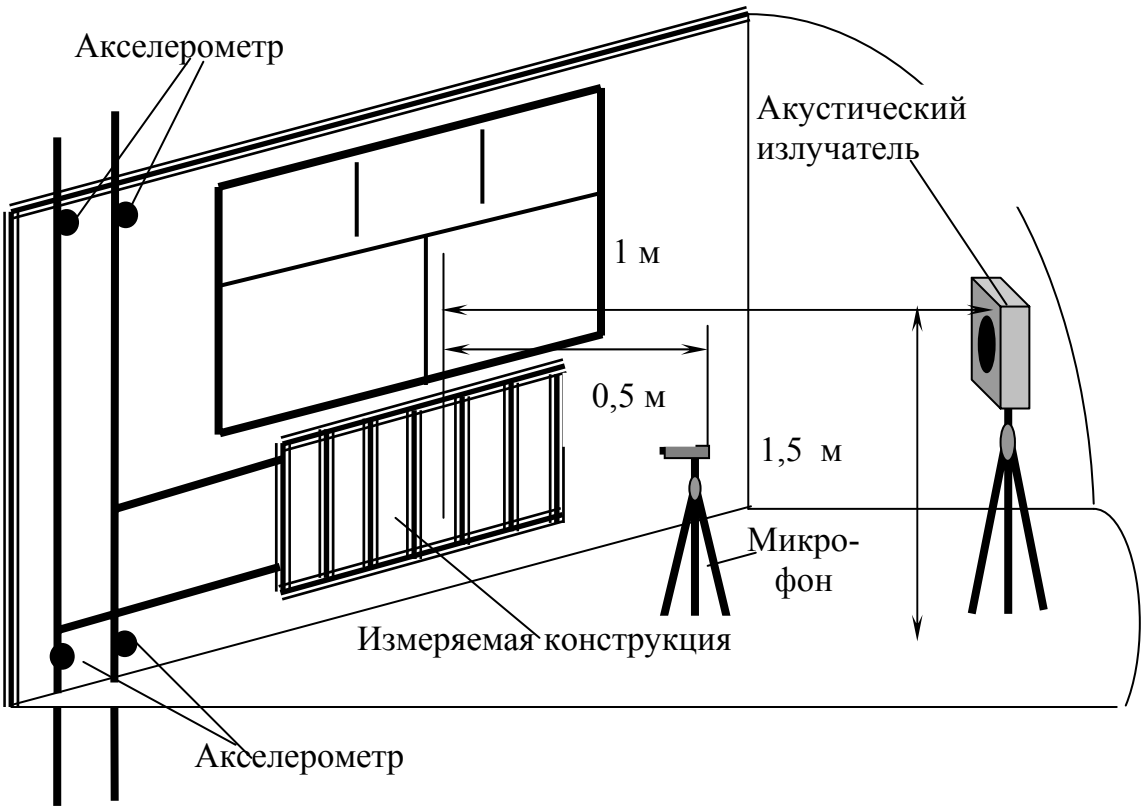


Рис. 7.8. Схема измерений на системе отопления

В случае невыполнения норм защищенности по акустическим и виброакустическим каналам утечки при исчерпанных возможностях средств пассивной защиты применяются средства активной защиты (САЗ), принцип работы которых заключается в зашумлении каналов утечки речевой информации.

Зашумление ограждающих конструкций их твердых материалов производится установкой вибропреобразователей на каждый элемент конструкции.

Трубы водоснабжения, отопления, канализации зашумляются достаточно просто. Если имеется система жестко связанных труб, то допускается установка одного вибропреобразователя, размещенного примерно посередине этой системы, а контрольные точки выбираются вблизи выхода труб из выделенного помещения.

Дверные проемы обычно зашумляются установкой акустической колонки в тамбуре двойной двери.

При защите систем вентиляции наиболее эффективна установка зашумляющей акустической колонки в канале на расстоянии не менее 1,5 *м* от плоскости его выхода в помещение. Этим обеспечивается необходимое зашумление при невысоких уровнях громкости колонки и отсутствии значительного шума в помещении.

Специальные исследования акустоэлектрических преобразований

Под акустоэлектрическим преобразованием понимают преобразование механической энергии акустического сигнала отдельными устройствами в электрический сигнал (напряжение, ток, заряд), модулированный по закону изменения акустического сигнала. Опасность акустоэлектрического канала утечки состоит в том, что наведенные электрические сигналы несмотря на свой низкий уровень могут распространяться по проводным линиям за пределы контролируемой зоны и перехватываться средствами технической разведки.

Акустоэлектрическим эффектом обладают многие элементы электронных технических средств обработки информации и вспомогательных технических средств. Прежде всего, это моточные изделия (трансформаторы, дроссели, реле и т.п.), в которых в соответствии с законом электромагнитной индукции, открытым Фарадеем, наводится ЭДС при движении проводников в магнитном поле под действием энергии звуковой волны. Магнитное поле всегда присутствует в ферромагнитных сердечниках за счет остаточной индукции.

Для прямого акустоэлектрического преобразования измерение величины сигналов речевого диапазона частот исследуемого технического средства (ТС) рекомендуется типовая схема (рис. 7.9) [2]. В конкретных реальных условиях можно применять не только указанные приборы, но и другие сертифицированные их аналоги с не уступающими характеристиками.

Исследуемое техническое средство может быть подключено к реальной отходящей линии, к имитатору или находиться в режиме холостого хода. К отходящей линии подключается измерительный нановольтметр непосредственно или бесконтактно через токовый трансформатор. Подключение измерительного нановольтметра необходимо выполнять по всем возможным вариантам: симметрично, несимметрично, по разбитым парам, по нескольким проводам (в случае применения токового трансформатора) и т.д.

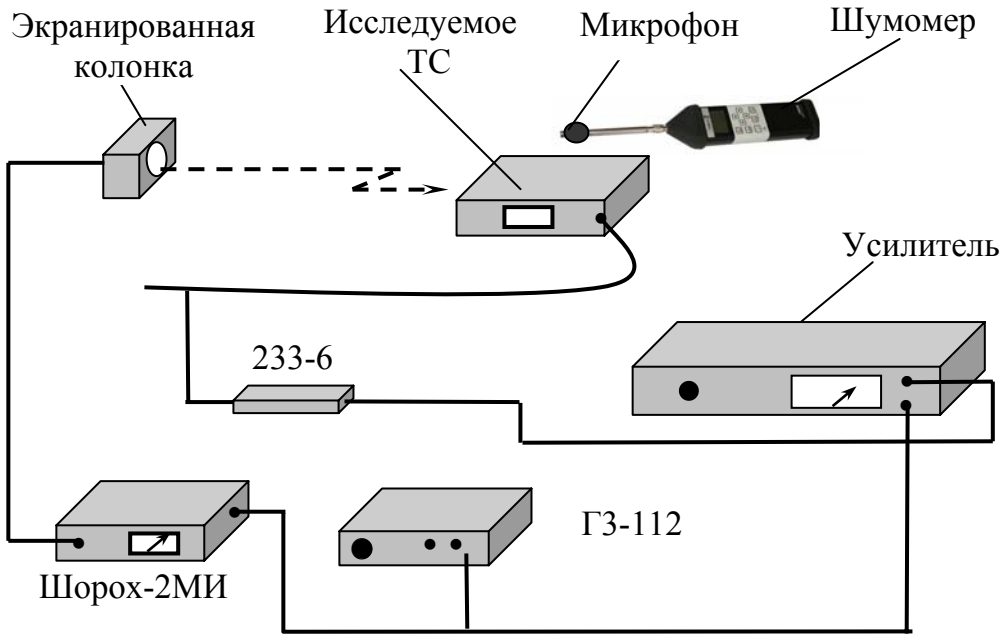


Рис. 7.9. Типовая схема измерения прямого акустоэлектрического преобразования

Для усиления слабого сигнала акустоэлектрического преобразования прямое подключение измерительного прибора производится через предусилитель типа 233-6 и усилитель. Токовый трансформатор может охватывать один или несколько проводов.

Экранированную акустическую колонку, создающую тестирующий звуковой сигнал с характеристиками, задаваемыми генератором Шорох-2МИ, обычно размещают на расстоянии 1 м от исследуемого технического средства. Такое расстояние выбирается из соображений обеспечения требуемого уровня звукового давления и допустимого уровня электромагнитных наводок от колонки на техническое средство.

Уровень тестирующего звукового сигнала непосредственно у технического средства измеряется шумомером.

Рекомендуется следующий порядок проведения измерений. После включения, прогрева и калибровки всех средств измерения оператор плавно изменяет частоту звукового генератора в заданном диапазоне частот при звуковом давлении 74…94 дБ. Как правило, огибающая сигнала АЭП характеризуется пиками и провалами. Рекомендуется фиксировать наибольшие пики.

Исследуемое техническое средство необходимо проверять во всех возможных режимах его работы и принимать за результат наибольшее значение опасного сигнала.

Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок

Побочные электромагнитные излучения и наводки (ПЭМИН) можно разделить на [2]:

- не предусмотренные в работе технические средства акустоэлектрические преобразования;
- паразитные связи и наводки;
- побочные низкочастотные излучения;
- побочные высокочастотные излучения.

Под низкочастотными излучениями понимают электромагнитные излучения с частотами слышимого звукового диапазона. Источниками таких излучений являются устройства и цепи, содержащие случайные и не случайные акустоэлектрические преобразователи с соединительными линиями.

К высокочастотным опасным излучениям относятся электромагнитные излучения от высокочастотных цепей, по которым циркулирует секретная или конфиденциальная информация. Источником таких излучений могут являться:

- усилители и логические элементы в режиме паразитной генерации;
- генераторы подмагничивания и стирания магнитофонов;
- гетеродины радио- и телевизионных приемников;
- элементы ВЧ-навязывания;
- устройства и узлы компьютерной техники.

Сигналы можно представлять функциями времени или в виде частотных спектров. При исследовании ПЭМИН сигналы обычно представляются в виде частотных спектров.

В реальных условиях существует только сплошной спектр импульсов. Амплитуды гармонических составляющих для последовательности импульсов значительно больше, чем амплитуда огибающей спектральной плотности для одиночного импульса. Однако нормами определен расчет защищенности по одному импульсу независимо от предыдущих и последующих

В случаях, когда технические средства применяются для обработки информации ограниченного доступа, наибольшую актуальность имеют вопросы, связанные с информативными ПЭМИ и наводками информативных сигналов на токопроводящие цепи. Под ними понимают ПЭМИ и наводки, которые содержат сведения об обрабатываемой информации и могут быть перехвачены заинтересованными лицами. Характер ПЭМИ определяется назначением, схемными решениями, элементной базой, мощностью устройства, а также материалами, из которых изготовлен корпус, и его конструкцией.

Согласно действующим нормативно-методическим документам, при проведении специальных исследований требуется измерять информативные ПЭМИ. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться при измерениях. Для того чтобы выделить ин-

формационные ПЭМИ, на исследуемом техническом средстве предусматривают специальные тестовые режимы его работы. Требования к тестам определяются в соответствующих ГОСТ и методиках.

В соответствии с методикой проведения специальных исследований технических средств по измерению их собственного электромагнитного излучения проводятся следующие операции:

1. Контролируемое устройство включается в тестовый режим.

2. На определенном расстоянии (обычно 0,5 м) от устройства устанавливаются поочередно антенны для приема электрической и магнитной составляющих поля, излучаемого анализируемым устройством (рис. 2.10).

3. Электрический сигнал с выхода антенны подается на вход приемно-регистрирующего измерительного устройства, с помощью которого по результатам измерений по определенной методике производится расчет опасных зон.

Для исследования ПЭМИН видеоподсистемы ПЭВМ широко используется стандартный тест «Зебра», который обеспечивает вывод на экран определенного числа белых и черных горизонтальных полос, содержащих одинаковое число строк развертки монитора.

Наибольшую опасность утечки информации через ПЭМИН представляют узлы и устройства ПЭВМ, обрабатывающие информацию в последовательном коде. Информативные излучения в параллельном коде на сегодняшний день расшифровке не поддаются, так как через электромагнитные излучения невозможно определить принадлежность излученного импульса к какому-то разряду кода.

Исследованию на ПЭМИН подлежат следующие устройства:

- видеоподсистема;
- накопители на жестких и гибких дисках;
- устройства CD, CD-R, CD-RW, DVD, DVD-RW;
- клавиатура;
- последовательные порты;
- принтеры.

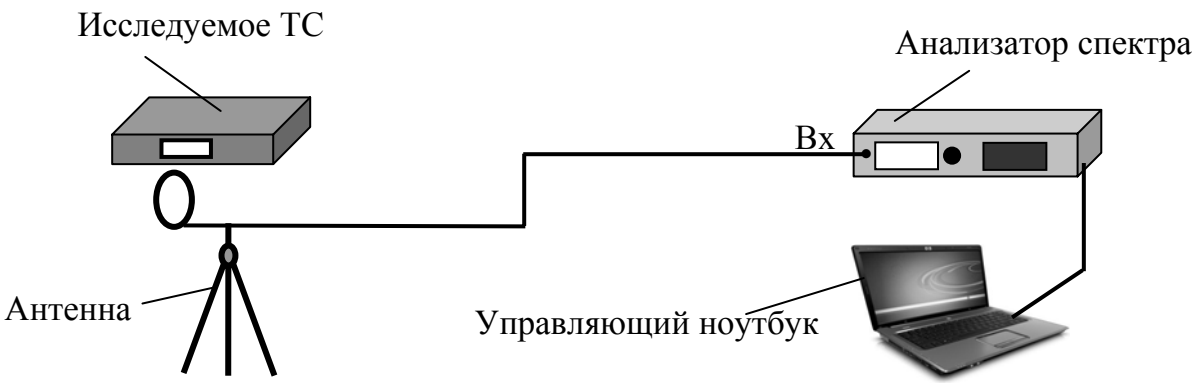


Рис. 7.10. Схема измерения ПЭМИ

Применяемые средства измерения могут быть различными, но обязательно поверенными и имеющими сертификат Гостехкомиссии. Укажем лишь на программно-аппаратные комплексы «Легенда» и «Сигурд», выполненные на базе анализаторов спектра «R&S» и «IFR».

Эти комплексы имеют управляющую и расчетную программы, способны опознавать заданные тест-программами опасные сигналы по форме их огибающих. Оба комплекса в результате специсследований определяют опасные зоны R_2, r_1 и r_1' и формируют отчетный протокол.

Внешний вид основного рабочего экрана управляющей программы «Легенда» представлен на рис. 7.11.

На рис. 7.11 цифрами обозначены следующие элементы основного рабочего экрана (главного окна):

1 – окно спектра (отображается спектр сигнала для выбранного диапазона частот);

2 – таблица исследований (отображаются все программы исследований, которые будут выполнены в автоматическом режиме);

3 – окно эталона (осциллограмма найденного в полуавтоматическом режиме эталона тестового сигнала);

4 – окно сигнала (осциллограмма сигнала, который будет сравниваться с эталоном);

5 – рабочая таблица промежуточных результатов.

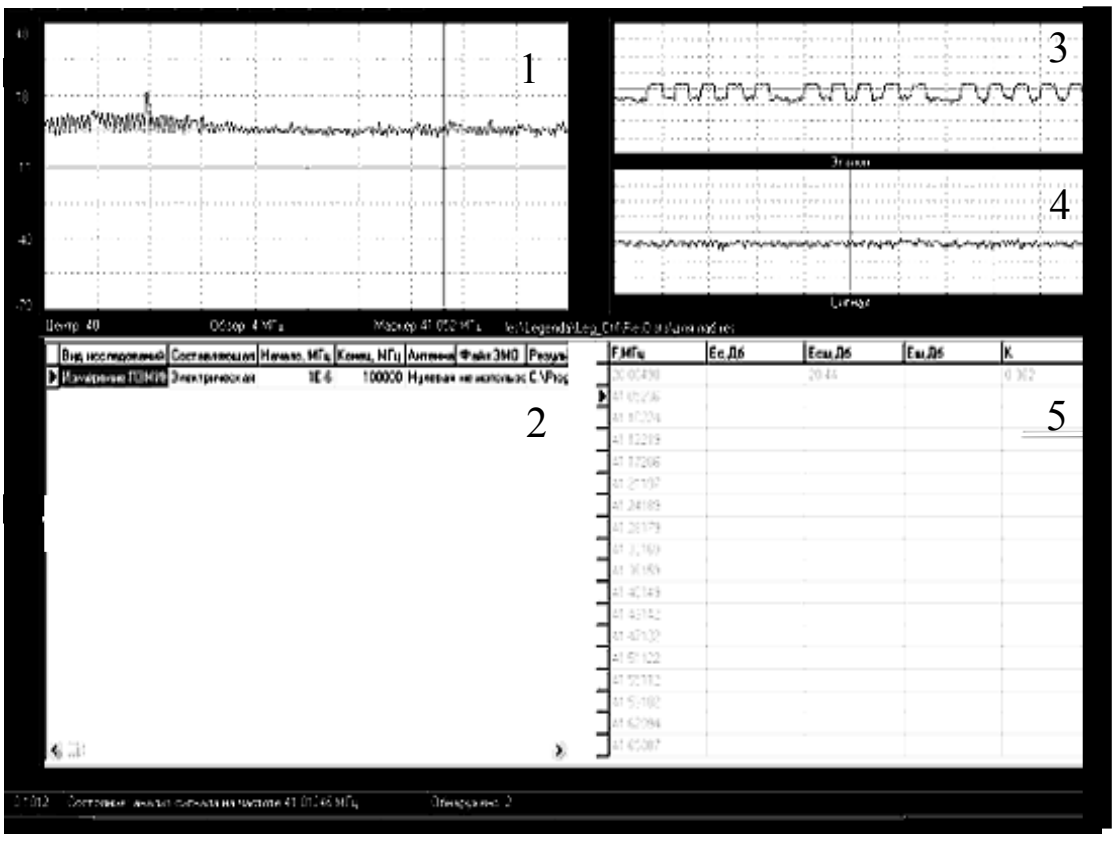


Рис. 7.11. Внешний вид экрана управляющей программы «Легенда»

7.3.2.4. Цели и задачи технического контроля эффективности мер защиты информации

Аттестация по требованиям безопасности информации предшествует разрешению на обработку подлежащей защите информации и официально подтверждает эффективность совокупности применяемых на конкретном объекте информатизации мер и средств защиты информации.

Комплекс специальных аттестационных мероприятий называется аттестационной проверкой и включает в себя *контроль эффективности защиты* – проверку соответствия качественных и количественных показателей эффективности мер технической защиты установленным требованиям или нормам эффективности защиты информации. *Показатель эффективности защиты информации* представляет собой меру или характеристику для ее оценки.

Нормы эффективности защиты информации соответствуют показателям, установленным нормативными документами.

Под *методом контроля эффективности защиты информации* понимают порядок и правила применения расчетных и измерительных операций при решении задач контроля эффективности защиты.

Различают два вида контроля защищенности объектов:

– аттестационный контроль,

– эксплуатационный контроль.

Аттестационный контроль проводится при вводе объекта в эксплуатацию и после его реконструкции или модернизации, а эксплуатационный – в процессе эксплуатации объекта. Проведение эксплуатационного контроля является обязательным и проводится не реже одного раза в год после проведения аттестационного контроля и получения аттестата соответствия. Для проведения аттестационного и эксплуатационного контроля применяются одни и те же средства.

Виды контроля эффективности защиты делятся на:

– организационный контроль – проверка соответствия мероприятий по технической защите информации требованиям руководящих документов;

– *технический контроль* – контроль эффективности технической защиты информации, проводимый с использованием технических средств контроля.

По способу проведения и содержанию технический контроль эффективности технической защиты информации относится к наиболее сложным видам контроля и может быть:

- *комплексным*, когда проверяется возможная утечка информации по всем опасным каналам контролируемого объекта;
- *целевым*, когда проводится проверка по одному из интересующих каналов возможной утечки информации;
- *выборочным*, когда из всего перечня технических средств на объекте для проверки выбираются только те, которые по результатам предва-

рительной оценки с наибольшей вероятностью имеют опасные каналы утечки защищаемой информации.

Аттестационный контроль всегда является комплексным.

В зависимости от вида выполняемых операций методы технического контроля делятся на:

- *инструментальные*, когда контролируемые показатели определяются непосредственно по результатам измерения контрольно-измерительной аппаратурой;
- *инструментально-расчетные*, при которых контролируемые показатели определяются частично расчетным путем и частично измерением значений некоторых параметров физических полей аппаратными средствами;
- *расчетные*, при которых контролируемые показатели рассчитываются по методикам, содержащимся в руководящей справочной литературе.

С целью исключения утечки информации не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на средствах и информационных системах, находящихся в процессе обработки информации.

Технический контроль состояния защиты информации в автоматизированных системах управления различного назначения осуществляется в полном соответствии со специально разработанными программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством, которому подчиняется объект контроля.

Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что на объекте отсутствуют технические каналы утечки информации.

Контроль состояния защиты информации заключается в проверке соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием *технических и программных средств контроля.*

Средство контроля эффективности защиты информации – техническое, программное средство, вещество и/или материал, используемые для контроля эффективности защиты информации.

Технический контроль определяет действенность и надежность принятых мер защиты объектов информатизации от воздействия технических средств разведки.

Технический контроль предназначен для:

- выявления возможных каналов утечки конфиденциальной информации;
- проверки соответствия и эффективности принятых мер защиты нормативным требованиям;
- разработки рекомендаций по совершенствованию принятых защитных мероприятий.

Технический контроль проводится по отдельным физическим полям, создаваемых объектами информатизации, и состоит из:

- сбора исходных данных, характеризующих уязвимости объекта информатизации по отношению к воздействиям технической разведки;
- определения возможных типов и средств технической разведки;
- предварительного расчета зон разведдоступности;
- определения состава и подготовки к работе контрольно-измерительной аппаратуры;
- измерения нормируемых технических параметров защищаемого объекта по отдельным физическим полям на границе контролируемой зоны;
- определения эффективности принятых мер защиты и в отдельных случаях разработки необходимых мер усиления защиты.

Для проведения технического контроля требуется наличие норм эффективности защиты, методик (методов) проведения контроля и соответствующей контрольно-измерительной аппаратуры.

Все контролируемые нормативные показатели разделяются на *информационные и технические* [5].

Информационные показатели относятся к вероятности обнаружения, распознавания и измерения технических характеристик объектов с заданной точностью.

Техническими показателями эффективности принятых мер защиты являются количественные показатели, характеризующие энергетические, временные, частотные и пространственные характеристики информационных физических полей объекта. Примерами таких характеристик могут быть напряженности электрического и магнитного полей ПЭМИ средств вычислительной техники, уровень сигналов наводок в силовых и слаботочных линиях за пределами контролируемой зоны, уровни акустических сигналов за пределами ограждающих конструкций и т.д. Нормой эффективности принятых мер защиты считается максимально допустимое значение контролируемых параметров на границе контролируемой зоны (в местах возможного нахождения технических средств разведки).

Инструментально-расчетные методы применяются тогда, когда комплект контрольно-измерительной аппаратуры не позволяет получить сразу конечный результат или не обладает достаточной чувствительностью.

Расчетные методы технического контроля применяются в случае отсутствия необходимой контрольно-измерительной аппаратуры, а также при необходимости быстрого получения предварительных ориентировочных результатов о зонах разведдоступности, например, перед инструментальными аттестациями рабочих мест.

При проведении технического контроля требуется контрольно-измерительная аппаратура, которая в большинстве случаев обеспечивает получение объективных характеристик контролируемых параметров или исходных данных для получения инструментально-расчетных характеристик. Контрольно-измерительная аппаратура по возможности должна быть портативной, что важно для аттестующих организаций, иметь достаточную чувствительность, соответствующую чувствительности аппаратуры разведки, быть надежной в эксплуатации.

Как правило, при проведении контроля расчетно-инструментальным методом проводится большое число измерений на дискретных интервалах и соответственно большое число сложных расчетов, что приводит к быстрой утомляемости испытателей. Поэтому современная тенденция развития контрольно-измерительной аппаратуры заключается в разработке для целей контроля программно-аппаратных комплексов, обеспечивающих полную автоматизацию измерения параметров физических полей и расчета нормируемых показателей защищенности объекта.

По результатам контроля состояния и эффективности защиты информации составляется заключение с приложением протоколов контроля.

Список литературы

1. Хореев А.А. Технические каналы утечки акустической (речевой) информации / Специальная техника. №1, 1998.

2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: учеб. пособие. М.: Горячая линия – Телеком, 2005. 416 с.

3. Шелупанов А.А., Зайцев А.П., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. М.: Горячая линия – Телеком. 543 с.

Учебное издание

Составители:
А.А. Шелупанов, д.т.н., профессор,
А.П. Зайцев, к.т.н., профессор,
Р.В. Мещеряков, к.т.н., доцент,
Е.М. Давыдова, к.т.н.,
В.Д. Зыков, к.т.н., А.А. Конев, к.т.н.,
Н.А. Новгородова, Г.А. Праскурин,
М.А. Сопов, Е.В. Колесник, Е.А. Колесник

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Издание пятое, переработанное и дополненное

Печатается без редактирования по текстам, предоставленным составителями

Издательство «В-Спектр»
Подписано к печати 18.06.2011.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 16,525. Усл. печ. л. 14,3.
Тираж 250 экз. Заказ 15.

Тираж отпечатан в издательстве «В-Спектр»
ИНН/КПП 7017129340/701701001, ОГРН 1057002637768
634055, г. Томск, пр. Академический, 13-24, Тел. 49-09-91.
E-mail: bvm@sibmail.com