

Содержание

Перечень сокращений	7
Введение	8
Глава 1. Основы технического регулирования и стандартизации в Российской Федерации	17
1.1. Общие замечания	17
1.2. Федеральный закон Российской Федерации № 184-ФЗ «О техническом регулировании»	20
1.3. Основы стандартизации в Российской Федерации	27
1.3.1. Основные положения системы стандартизации в Российской Федерации (ГОСТ Р 1.0–2012)	27
1.3.2. Правила разработки национальных стандартов (ГОСТ Р 1.2–2014)	30
1.3.3. Стандарты организаций (ГОСТ Р 1.4–2004)	30
1.4. Основы стандартизации в области защиты информации	31
1.4.1. Основные термины в сфере защиты информации (ГОСТ Р 50922–2006)	31
1.4.2. Защита информации в организации (ГОСТ Р 53114–2008)	33
1.4.3. Система стандартов по защите информации (ГОСТ Р 52069.0–2013)	35
1.4.4. Факторы, воздействующие на информацию (ГОСТ Р 51275–2006)	38
1.4.5. Оценка соответствия (ГОСТ 17000–2012)	39
Контрольные вопросы и задания к главе 1	44
Глава 2. Нормативные документы ФСТЭК России	46
2.1. Основные нормативные документы в области защиты информации	46
2.2. Защита от несанкционированного доступа к информации.	
Термины и определения	53
2.3. Концепция защиты СВТ и АС от НСД к информации	55
2.4. Показатели защищенности СВТ от НСД к информации	58
2.5. Классификация автоматизированных систем и требования по защите информации	61
2.6. Межсетевые экраны. Показатели защищенности от НСД	65

2.7. Контроль отсутствия НДВ в программном обеспечении	67
2.8. Требования к защите персональных данных	71
2.9. Требования о защите информации в государственных информационных системах	76
2.10. Требования о защите информации в ИС общего пользования	80
2.11. Требования к обеспечению защиты информации в АСУ ТП	84
2.12. Новое поколение нормативных документов ФСТЭК	89
2.12.1. Общие замечания	89
2.12.2. Пакет документов по профилям защиты	90
2.12.3. Требования к средствам антивирусной защиты	93
2.12.4. Требования к средствам обнаружения вторжений	97
2.12.5. Требования к средствам контроля съемных машинных носителей	100
2.12.6. Требования к средствам доверенной загрузки	104
2.13. Заключительные замечания	106
Контрольные вопросы и задания к главе 2	108

Глава 3. Национальные и международные стандарты в области информационной безопасности 110

3.1. Государственный стандарт по защите информации от НСД ГОСТ Р 50739–95	110
3.2. Национальный стандарт по менеджменту инцидентов ИБ ГОСТ Р ИСО/МЭК ТО 18044–2007	112
3.3. Национальный стандарт по менеджменту безопасности ИТП ГОСТ Р ИСО/МЭК 13335-1–2006	115
3.4. Национальный стандарт по менеджменту безопасности сетей ГОСТ Р ИСО/МЭК 13335-5–2006	122
3.5. Стандарты серии 27000 по менеджменту ИБ	123
3.5.1. История создания стандартов серии 27000	123
3.5.2. Национальный стандарт ГОСТ Р ИСО/МЭК 27000–2012 — термины по СМИБ	128
3.5.3. Национальный стандарт ГОСТ Р ИСО/МЭК 27001–2006 — требования к СМИБ	130
3.5.4. Национальный стандарт ГОСТ Р ИСО/МЭК 27002–2012 — свод норм и правил СМИБ	132
3.5.5. Национальный стандарт ГОСТ Р ИСО/МЭК 27003–2012 — реализация СМИБ	136
3.5.6. Национальный стандарт ГОСТ Р ИСО/МЭК 27004–2011 — измерения в СМИБ	141
3.5.7. Национальный стандарт ГОСТ Р ИСО/МЭК 27005–2010 — менеджмент риска ИБ	143
3.5.8. Национальные стандарты в области аудита СМИБ (ГОСТ 27006–2008, ГОСТ 27007–2014)	146

3.5.9. Национальный стандарт по СМИБ в телекоммуникационных организациях (ГОСТ 27011–2014)	148
3.6. Стандарты серии 27033 по безопасности сетей	150
3.6.1. Общие замечания	150
3.6.2. Национальный стандарт ГОСТ Р ИСО/МЭК 27033-1–2011 — обзор и концепции безопасности сетей	153
3.6.3. Национальный стандарт ГОСТ Р ИСО/МЭК 27033-3–2014 — эталонные сетевые сценарии	160
3.7. Стандарты по безопасности сетей электросвязи (ГОСТ Р 52448–2005, ГОСТ Р 53110–2008)	166
3.8. Защита от угроз, реализуемых через скрытые каналы (ГОСТ Р 53113.1, ГОСТ Р 53113.2)	171
3.9. Стандарты по уязвимостям ИС (ГОСТ Р 56545, ГОСТ Р 56546)	175
3.10. Комплекс стандартов по информационной безопасности Банка России (ИББС)	178
Контрольные вопросы и задания к главе 3	182
Глава 4. Национальные стандарты Российской Федерации на основе «Общих критериев»	184
4.1. История создания «Общих критериев» и национальных стандартов на их основе	184
4.2. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1–2012	189
4.3. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2–2013	196
4.4. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3–2013	200
4.5. Национальный стандарт ГОСТ Р ИСО/МЭК 18045–2013	209
4.6. Национальный стандарт ГОСТ Р ИСО/МЭК 51583–2014	213
4.7. Национальный стандарт ГОСТ Р ИСО/МЭК 19791–2008	219
4.8. Национальный стандарт ГОСТ Р ИСО/МЭК 15446–2008	227
4.9. Национальные стандарты по биометрической аутентификации серии ГОСТ Р 52633	231
4.10. Краткий обзор некоторых стандартов	234
Контрольные вопросы и задания к главе 4	239
Список литературы	240
Список документов ФСТЭК	245
Список национальных стандартов	248
Список стандартов Банка России	253

*Памяти моих друзей Валерия Борякова
и Геннадия Ярового посвящаю*

Нет, никто никогда не заменит погибшего товарища. Старых друзей наскоро не создашь. Нет сокровища дороже, чем столько общих воспоминаний, столько тяжких часов, пережитых вместе, столько ссор, примирений, душевных порывов. Такая дружба — плод долгих лет. Сажая дуб, смешно мечтать, что скоро найдешь приют в его тени.

Так устроена жизнь. Сперва мы становимся богаче, ведь много лет мы сажали деревья, но потом настают годы, когда время обращает в прах наши труды и вырубает лес. Один за другим уходят друзья, лишая нас прибежища.

И, скорбя об ушедших, втайне еще и грустишь о том, что сам стареешь.

Антуан де Сент-Экзюпери. Планета людей

Перечень сокращений

АС	— автоматизированная система
АСЗИ	— АС в защищенном исполнении
АСУТП	— автоматизированная система управления производственными и технологическими процессами
ГИС	— государственная информационная система
ЗБ	— задание по безопасности
ИБ	— информационная безопасность
ИКТ	— информационно-коммуникационные технологии
ИС ОП	— информационная система общего пользования
ИСПДн	— информационная система персональных данных
ИТ	— информационная технология
ИТТ	— информационная и телекоммуникационная технология
КСЗ	— комплекс средств защиты
МЭ	— межсетевой экран
НДВ	— недекларированная возможность
НСД	— несанкционированный доступ
ОО	— объект оценки
ОУД	— оценочный уровень доверия
ПД	— персональные данные
ПЗ	— профиль защиты
ПО	— программное обеспечение
ПРД	— правила разграничения доступа
ПС	— программное средство
РД	— руководящий документ
РИД	— результаты интеллектуальной деятельности
САВЗ	— средство антивирусной защиты
СВБА	— средства высоконадежной биометрической аутентификации
СВТ	— средство вычислительной техники
СДЗ	— средства доверенной загрузки
СЗИ	— средство защиты информации
СК	— скрытый информационный канал
СКЗИ	— средство криптографической защиты информации
СКН	— средства контроля съемных машинных носителей информации
СМИБ	— система менеджмента ИБ
СОВ	— система обнаружения вторжений
СОИБ	— система обеспечения информационной безопасности
СоПД	— составной пакет доверия
СП	— сообщение о проблеме
СРД	— система разграничения доступа
ССЗИ	— система стандартов по защите информации
ТДБ	— требования доверия к безопасности
ТОО	— технический отчет об оценке
УЗ	— уровень значимости информации
ФБО	— функциональные возможности безопасности объекта
ФТБ	— функциональные требования безопасности

Введение

Развитие человечества знаменуется системой эпохальных открытий и перемен, коренным образом изменяющих характер жизни общества. В развитии средств создания, хранения, обработки и передачи информации также можно выделить ключевые этапы:

1. Изобретение в XV в. печатного станка.
2. Появление телефона, так как он позволил создать новую коммуникационную технологию.
3. Возникновение радио, послужившее прообразом сегодняшних спутниковых коммуникаций.
4. Появление персональных компьютеров.
5. Период компьютерных коммуникаций, развития средств доступа к информации, Интернета и мировой информационной инфраструктуры.

Каждый из этапов сопровождался определенными проблемами. В допечатную эпоху основными способами распространения информации были устная речь и тиражирование рукописей, поэтому главной проблемой была доступность информации. В эпоху книгопечатания, наоборот, издавалось огромное количество информации в печатном виде, и главной проблемой был поиск нужной информации.

Эпоха электронных ресурсов и Интернета характеризуется огромным количеством информации в электронном виде и мощными средствами поиска. Вместе с тем возросли и проблемы: необходимость оценки истинности и подлинности информации, защиты от несанкционированного доступа, использование информации в качестве оружия в информационных войнах.

В современном информационном обществе информационные и коммуникационные технологии являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности. Информация и поддерживающие ее процессы, системы и сети являются важными деловыми активами, которые, подобно другим активам организации, имеют ценность и, следовательно, должны быть защищены надлежащим образом.

Информация может существовать в различных формах: быть напечатанной или написанной на бумаге, храниться в электронном виде, передаваться

по почте или с использованием электронных средств связи, а также устно. Независимо от формы представления информации, средств ее распространения или хранения, она всегда должна быть адекватно защищена.

Информационная безопасность достигается реализацией комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств. Указанные меры и средства контроля и управления необходимо создавать, реализовывать, подвергать мониторингу, анализировать и улучшать.

Организация должна определить свои требования к информационной безопасности. Существуют три основных источника требований к безопасности. Один из источников складывается из оценки рисков организации с учетом целей ее бизнеса. Посредством оценки рисков идентифицируются угрозы активам организации, оцениваются уязвимости, вероятности возникновения угроз, а также возможные последствия.

Вторым источником являются правовые, законодательные, нормативные и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг, а также их социокультурная среда.

Третим важным источником является также определенный набор принципов, целей и требований бизнеса для обработки информации, которые разработала организация для поддержки своей деятельности.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлены следующими причинами:

- ◆ высокими темпами роста парка персональных компьютеров, находящихся в эксплуатации в различных сферах человеческой деятельности;
- ◆ резким увеличением объемов информации, накапливаемой, хранимой на электронных носителях (в виде электронных документов) и обрабатываемой с помощью средств вычислительной техники;
- ◆ концентрацией информации и сосредоточением в единых базах данных информации различного назначения и различной принадлежности;
- ◆ бурным развитием аппаратно-программных средств, не удовлетворяющих требованиям безопасности;
- ◆ резким расширением круга пользователей, имеющих непосредственный доступ к компьютерным сетям и хранилищам данных;
- ◆ развитием электронной почты и электронного документооборота в компьютерных сетях на предприятиях;

- ◆ внедрением электронных технологий в различные виды профессиональной деятельности на финансовых и товарных рынках (электронная коммерция, сетевые банковские и финансовые услуги);
- ◆ широким распространением сетевых технологий, созданием единого информационно-коммуникационного мирового пространства на базе сети Интернет, которая по своей идеологии не обеспечивает достаточного уровня информационной безопасности;
- ◆ несоответствием бурного развития средств обработки информации и теории информационной безопасности, стандартов и правовых норм.

Учитывая масштабы проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней, а также высокий уровень зависимости создаваемых в стране информационных систем от импортной продукции, особенно актуальным становится вопрос обеспечения должного уровня информационной безопасности страны в современном глобальном информационном мире. Президентом Российской Федерации В. В. Путиным 24.07.2013 г. утвержден концептуальный документ № Пр-1753 «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.». Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

- ◆ в качестве информационного оружия;
- ◆ в террористических целях;
- ◆ для вмешательства во внутренние дела суверенных государств;
- ◆ для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных компьютерных программ.

В соответствии с новым вариантом документа «Стратегия национальной безопасности Российской Федерации», утвержденным Указом Президента от 31.12.2015 г. № 687, под угрозой национальной безопасности страны понимается совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам. Обеспечение национальной безопасности достигается путем реализации органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов.

Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах, а реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления. В «Стратегии...» отмечено, что все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории. Появляются новые формы противоправной деятельности с использованием информационных, коммуникационных и высоких технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе.

В документе «Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 гг. и на перспективу до 2025 г.», утвержденном Распоряжением Правительства Российской Федерации от 01.11.2013 г. № 2036-р, среди факторов, ограничивающих развитие информационных технологий в России, отмечены, в частности, следующие:

- ◆ обострившийся в последние годы дефицит кадров;
- ◆ недостаточный уровень подготовки специалистов.

Ежегодно из образовательных организаций высшего образования страны выпускается до 25 тыс. специалистов, что не дает достаточной базы для удовлетворения потребностей отрасли в квалифицированных кадрах. При этом сегодня только 15 % выпускников вузов, обучавшихся по инженерным специальностям, пригодны к немедленному трудуоустройству в сфере информационных технологий.

В число основных задач по развитию отрасли информационных технологий России в «Стратегии...» включены:

- ◆ обеспечение информационной безопасности;
- ◆ развитие человеческого капитала, в том числе за счет развития профильного образования и популяризации профессий отрасли.

В новом варианте «Стратегии национальной безопасности Российской Федерации» наука, технологии и образование отнесены к стратегическим национальным приоритетам, от степени реализации которых напрямую зависит состояние национальной безопасности. Одним из главных направлений обеспечения национальной безопасности в области науки, технологий и образования согласно «Стратегии...» является повышение уровня

технологической безопасности, в том числе в информационной сфере. В ст. 113 «Стратегии...» прямо отмечено, что при ее реализации особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов.

К сожалению, с каждым годом растет количество преступлений в сфере информационно-коммуникационных технологий. В докладе начальника бюро специальных технических мероприятий (БСТМ) МВД России А. Н. Мошкова на 17-м национальном форуме информационной безопасности («Инфофорум–2015») было отмечено, что количество зарегистрированных компьютерных преступлений в 2014 г. превысило 11 тыс. В докладе заместителя начальника Главного управления безопасности и защиты информации «Банка России» А. М. Сычева отмечено, что в 2014 г. выявлено 379 тыс. несанкционированных операций с использованием 87 тыс. пластиковых карт. По данным лаборатории Касперского, в 2014 г. ежедневно детектировалось 325 тыс. образцов нового вредоносного программного обеспечения (в 1994 г. каждый час появлялся 1 новый вирус).

На «Инфофоруме–2016» (состоялся 4 и 5 февраля 2016 г.) А. Н. Мошковым было сделано сообщение о раскрытии в России международного преступного киберсообщества, готовившего глобальную операцию по хищению денег из банков, находящихся в первой сотне российского рейтинга. На момент задержания преступникам уже удалось похитить несколько сотен миллионов рублей, но была предотвращена кража еще 1,5 млрд рублей. В 2015 г. на 66 % больше, чем в 2014-м, зарегистрировано преступлений, связанных с вредоносным программным обеспечением. Также за год в два раза возросло число киберпреступлений, наказание за которые определяется ст. 159 Уголовного кодекса (УК) РФ «Мошенничество». За 2015 г. в судебные органы направлено 11 223 дела в области компьютерных преступлений.

Меры нормативно-правовой поддержки регулирования вопросов защиты информации в Российской Федерации определяются на основании:

- ◆ международных договоров и соглашений;
- ◆ законов Российской Федерации;
- ◆ указов и распоряжений Президента Российской Федерации;
- ◆ нормативных документов Правительства Российской Федерации;
- ◆ технических регламентов;
- ◆ национальных стандартов и стандартов организаций;
- ◆ нормативных правовых актов уполномоченных федеральных органов исполнительной власти.

Проблема борьбы с компьютерными преступлениями и защита информационных ресурсов, включая всю инфраструктуру информационных систем,

стала глобальной и требует соответствующего международного взаимодействия, в том числе разработки единых стандартов в области информационной безопасности.

Россия подписала соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (вступило в силу 14.03.2002 г.). В нем признаются в качестве уголовно наказуемых следующие деяния:

- ◆ осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;
- ◆ создание, использование или распространение вредоносных программ;
- ◆ нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации;
- ◆ незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства.

Благодаря усилиям группы правительенных экспертов ООН в августе 2015 г. была достигнута договоренность ведущих кибердержав мира о необходимости принятия важного документа «Правила поведения в области обеспечения международной информационной безопасности». Об этом сообщил на «Инфофоруме–2016» специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области ИБ, посол РФ по особым поручениям, д-р исторических наук, профессор А. В. Крутских.

В соответствии с «Правилами...» государства, в частности, обязуются:

- ◆ не использовать ИКТ и информационные и коммуникационные сети для осуществления действий, которые противоречат задачам поддержания международного мира и безопасности;
- ◆ не использовать ИКТ и сети для вмешательства во внутренние дела других государств и в целях подрыва их политической, экономической и социальной стабильности;
- ◆ сотрудничать в борьбе с преступной или террористической деятельностью с использованием ИКТ и сетей и сдерживать распространение информации террористического, сепаратистского или экстремистского характера, а также разжигающей ненависть на национальной, расовой или религиозной почве;
- ◆ прикладывать усилия к обеспечению безопасности на всех этапах поставок продукции и предоставления услуг в сфере ИКТ;

- ◆ подтверждать права и обязанности каждого государства в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии.

Все государства должны в полной мере сотрудничать с другими заинтересованными сторонами и способствовать углублению осознания своей ответственности за обеспечение информационной безопасности, включая формирование культуры ИБ и поддержку усилий по защите объектов критической информационной инфраструктуры.

К сожалению, в настоящее время вышеуказанные нормы ответственного поведения государств являются добровольными и не имеют обязательного юридического характера.

На пленарном заседании национального форума информационной безопасности «Инфофорум–2016» референт аппарата Совета Безопасности Российской Федерации Д. Г. Грибков осветил некоторые основные положения новой Доктрины информационной безопасности РФ. Предыдущая Доктрина была принята в 2000 г. и не соответствует новым угрозам безопасности в современном глобальном информационном обществе. О начале работ над новым вариантом Доктрины было объявлено еще на «Инфофоруме–2015», и спустя год появился проект документа, который планируется принять в 2016 г.

В соответствии с проектом базовыми составляющими национальных интересов Российской Федерации в информационной сфере являются:

- ◆ соблюдение конституционных прав и свобод человека и гражданина в области получения и использования информации, а также сохранение и укрепление культурных, исторических, духовно-нравственных ценностей многонационального российского народа;
- ◆ обеспечение устойчивого развития и бесперебойного функционирования информационной инфраструктуры государства;
- ◆ развитие отечественной отрасли ИКТ;
- ◆ информационное обеспечение государственной политики РФ;
- ◆ формирование международного правового режима в целях укрепления равноправного стратегического партнерства в области ИБ и обеспечение национального суверенитета в глобальном информационном пространстве.

Основные направления обеспечения информационной безопасности в проекте увязаны со стратегическими национальными приоритетами и формулируются в привязке к следующим областям:

- ◆ Оборона страны.

- ◆ Государственная и общественная безопасность.
- ◆ Экономика.
- ◆ Наука, технологии, образование.
- ◆ Стратегическая стабильность, равноправное стратегическое партнерство.

Комплексный подход к обеспечению ИБ предполагает также совершенствование деятельности по следующим важнейшим направлениям:

- ◆ Информационное обеспечение государственной политики.
- ◆ Обеспечение устойчивого и безопасного функционирования единой сети электросвязи РФ.
- ◆ Защита информации государственных органов и различных организаций.
- ◆ Подготовка кадров в области ИБ.
- ◆ Формирование культуры ИБ граждан.

Если исходить из положений новой Доктрины, становится ясной ключевая роль образовательных учреждений в подготовке кадров в области ИБ и повышении общей информационной культуры и культуры информационной безопасности граждан, в первую очередь молодого поколения. Важнейшим условием повышения уровня информационной безопасности является подготовка высококвалифицированных специалистов в области защиты информации, обладающих необходимыми компетенциями и знаниями требований нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК), ФСБ, международных и национальных стандартов.

Цель данного учебного пособия — рассмотреть важнейшие открытые нормативно-методические документы ФСТЭК и стандарты в области информационной безопасности (кроме документов по криптографической защите) по состоянию на начало 2016 г. С различной степенью подробности в пособии рассмотрено более 100 документов.

В главе 1 рассматриваются основные положения Федерального закона Российской Федерации № 184-ФЗ «О техническом регулировании» и национальных стандартов, устанавливающих основы стандартизации в России.

Глава 2 посвящена рассмотрению основных нормативных и методических документов Гостехкомиссии России и документов ФСТЭК нового поколения, основанных на принципах международного стандарта «Общие критерии».

Главы 3 и 4 посвящены рассмотрению основных национальных и международных стандартов в области информационной безопасности, принятых в Российской Федерации, в том числе стандартов нового поколения,

построенных на основе международного стандарта «Общие критерии» и его российского аналога ГОСТ Р ИСО/МЭК 15408.

Учебное пособие написано на основе опыта преподавания в Самарском экономическом, Самарском государственном и Самарском аэрокосмическом университетах (ныне объединенный Самарский национальный исследовательский университет им. акад. С. П. Королева) ряда дисциплин по направлению подготовки «Информационная безопасность»:

- ◆ «Методы и стандарты оценки защищенности компьютерных систем»;
- ◆ «Нормативная база, российские и международные стандарты по информационной безопасности»;
- ◆ «Вычислительные сети. Контроль безопасности в компьютерных сетях»;
- ◆ «Организационное и правовое обеспечение информационной безопасности».

Кроме того, автор читал циклы лекций в рамках различных курсов повышения квалификации для специалистов в области информационной безопасности и информационных технологий. По тематике пособия автором опубликован ряд научных статей и учебных пособий с грифом УМО в области информационной безопасности, ссылки на которые даны в списке литературы.

Отзывы, пожелания и замечания можно присылать на кафедру безопасности информационных систем Самарского национального исследовательского университета им. акад. С. П. Королева по адресу: 443086, г. Самара, Московское шоссе, 34, а также по адресу электронной почты автора: rodichev@samsu.ru.

Благодарности

Выражаю признательность своим коллегам М. Н. Осипову, А. И. Моисееву, а также рецензентам А. Г. Абросимову и В. С. Кузьмичеву за ценные советы и поддержку при сборе материала и написании пособия.

Искренне благодарен руководителю проектной группы «Компьютерная и научно-популярная литература» Юлии Сергиенко за доброе и внимательное отношение и профессионализм, а также всем сотрудникам издательского дома «Питер» за творческое отношение по правке исходного текста рукописи и подготовке пособия к изданию.

Глава 1. Основы технического регулирования и стандартизации в Российской Федерации

1.1. Общие замечания

Основным правовым документом в области технического регулирования и стандартизации является Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». Он вступил в силу 1 июля 2003 г. В связи с этим утратили силу ряд ранее принятых законов и постановлений Правительства в области стандартизации и сертификации продукции и услуг. Среди таких документов следует отметить законы Российской Федерации от 10.06.1993 г. № 5151-1 «О сертификации продукции и услуг» и от 10.06.1993 г. № 5154-1 «О стандартизации».

Одной из причин принятия закона явилась подготовка к вступлению Российской Федерации во Всемирную торговую организацию (ВТО), что потребовало реформирования существующей системы технического регулирования в соответствии с требованиями ВТО. В государствах — членах ВТО обязательные для применения требования к продукции устанавливаются в технических регламентах, утверждаемых органами власти, а национальные стандарты являются добровольными для применения. В России до принятия закона разделения требований на обязательные и применяемые на добровольной основе не существовало. Большинство требований носило обязательный характер и устанавливалось в государственных стандартах и нормативных документах федеральных органов исполнительной власти. Федеральный закон «О техническом регулировании» закладывает основу принципиально новой системы сертификации и стандартизации в Российской Федерации. Основной упор в нем делается на сужение сферы

обязательной стандартизации и подтверждения соответствия и расширение добровольности таких действий.

Закон регулирует отношения, возникающие при:

- ◆ разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- ◆ разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- ◆ оценке соответствия.

Основная цель закона — создание двухуровневой системы нормативных документов: технических регламентов, которые будут содержать обязательные требования безопасности, и добровольных стандартов, содержащих требования к качеству (до принятия закона все действующие в нашей стране ГОСТы были обязательны для исполнения).

Утверждение технического регламента в качестве обязательного к исполнению и применению документа и перевод стандартов в категорию добровольно применяемых норм явились своего рода революцией в сложившемся ранее процессе технического регулирования. Закон кардинально изменил всю систему технических требований, порядок их разработки и утверждения, порядок государственного контроля и подтверждения соответствия требованиям обязательных и добровольных норм.

Закон меняет правовой статус стандартов: из обязательных они превращаются в добровольно применяемые. Иными словами, стандарты, даже государственные, перестают быть обязательными для субъектов хозяйствующей деятельности. Сам термин «государственный стандарт» выходит из обращения. Вместо него введены новые понятия: «национальный стандарт», «международный стандарт», «региональный стандарт», «стандарт организации». Выведен из обращения также термин «отраслевой стандарт». Изменения правового статуса документов по стандартизации и самого понятия «стандартизация» обусловлены ориентацией российского законодателя на международную практику и сложившийся практический международный опыт в этой сфере деятельности.

Федеральным органом исполнительной власти Российской Федерации в области технического регулирования является Федеральное агентство по техническому регулированию и метрологии (Росстандарт, сайт агентства www.gost.ru), созданное Указом Президента Российской Федерации от 20.05.2004 г. № 649 «Вопросы структуры федеральных органов исполнительной власти». Деятельность агентства соответствует Положению,

утвержденному Постановлением Правительства Российской Федерации от 17.06.2004 г. № 294.

Основными задачами агентства являются:

- ◆ реализация функций национального органа по стандартизации;
- ◆ обеспечение единства измерений;
- ◆ осуществление государственного контроля (надзора) за соблюдением требований технических регламентов и обязательных требований стандартов;
- ◆ создание и ведение федерального информационного фонда технических регламентов и стандартов и единой информационной системы по техническому регулированию;
- ◆ оказание государственных услуг в сфере стандартизации, технического регулирования и метрологии.

На международном уровне систему стандартов создают Международная организация по стандартизации ISO (ИСО) и Международная электротехническая комиссия IEC (МЭК).

Кроме закона № 184-ФЗ «О техническом регулировании» существует ряд нормативных документов по техническому регулированию и стандартизации, в частности:

- ◆ Постановление Правительства РФ от 15.08.2003 г. № 500 «О федеральном информационном фонде технических регламентов и стандартов и единой информационной системе по техническому регулированию»;
- ◆ «Концепция развития национальной системы стандартизации Российской Федерации на период до 2020 г.» (одобрена Распоряжением Правительства РФ от 24.09.2012 г. № 1762-р);
- ◆ Постановление Правительства РФ от 19.11.2008 г. № 858 «О порядке разработки и утверждения сводов правил»;
- ◆ ГОСТ Р 1.12–2004 «Стандартизация в РФ. Термины и определения»;
- ◆ ГОСТ Р 1.0–2012 «Стандартизация в РФ. Основные положения»;
- ◆ ГОСТ Р 1.4–2004 «Стандарты организаций. Общие положения»;
- ◆ ГОСТ Р 1.1–2005 «Технические комитеты по стандартизации. Порядок создания и деятельности»;
- ◆ ГОСТ Р 1.2–2014 «Стандарты национальные РФ. Правила разработки, утверждения, обновления и отмены»;
- ◆ ГОСТ Р 1.5–2012 «Стандарты национальные. Правила построения, изложения, оформления и обозначения»;

- ◆ ГОСТ 1.1–2002 «Межгосударственная система стандартизации. Термины и определения».

В соответствии с Постановлением Госстандарта РФ от 30.01.2004 г. № 4 «О национальных стандартах Российской Федерации» со дня вступления в силу Федерального закона № 184-ФЗ «О техническом регулировании» национальными стандартами признаются государственные и межгосударственные стандарты, принятые Госстандартом России до 01.07.2003 г. Впредь до вступления в силу соответствующих технических регламентов установленные ранее требования к продукции подлежат обязательному исполнению только в части, соответствующей целям:

- ◆ защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;
- ◆ охраны окружающей среды, жизни или здоровья животных и растений;
- ◆ предупреждения действий, вводящих в заблуждение приобретателей.

Распоряжениями Правительства РФ от 6.11.2004 г. № 1421-р и от 8.11.2005 г. № 1889-р была утверждена Программа разработки технических регламентов на 2004–2006 гг., которая предусматривала разработку 84 регламентов. Указанные распоряжения были отменены Распоряжением Правительства РФ от 27.01.2011 г. № 86-р.

1.2. Федеральный закон Российской Федерации № 184-ФЗ «О техническом регулировании»

Предметом правового регулирования закона являются отношения между субъектами технического регулирования по вопросам:

- ◆ установления обязательных технических норм и правил;
- ◆ подтверждения соответствия продукции требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;
- ◆ стандартизации;
- ◆ аккредитации органов по сертификации и испытательных лабораторий;
- ◆ государственного контроля за соблюдением требований технических регламентов и ответственности в случаях несоответствия их требованиям;
- ◆ информирования о технических регламентах и документах по стандартизации;
- ◆ финансирования работ в области технического регулирования.

Закон № 184-ФЗ «О техническом регулировании» вводит ряд новых понятий.

Декларирование соответствия — форма подтверждения соответствия продукции требованиям технических регламентов.

Декларация о соответствии — документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов.

Международный стандарт — стандарт, принятый международной организацией.

Национальный стандарт — стандарт, утвержденный национальным органом Российской Федерации по стандартизации.

Региональный стандарт — стандарт, принятый региональной организацией по стандартизации.

Сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Схема подтверждения соответствия — перечень действий участников подтверждения соответствия, результаты которых рассматриваются ими в качестве доказательств соответствия продукции и иных объектов установленным требованиям.

Форма подтверждения соответствия — определенный порядок документального удостоверения соответствия продукции или иных объектов, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Орган по сертификации — юридическое лицо или индивидуальный предприниматель, аккредитованные в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации 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.

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.

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 продукции и связанным с требованиями к продукции 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, подлежащим ратификации в порядке, установленном законодательством Российской Федерации, или в соответствии с международным договором Российской Федерации, ратифицированным 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.

Техническое регулирование осуществляется в соответствии с принципами:

- ◆ применения единых правил установления требований к продукции, выполнению работ или оказанию услуг;
- ◆ соответствия технического регулирования уровню развития национальной экономики, материально-технической базы, а также уровню научно-технического развития;

- ◆ независимости органов по аккредитации и сертификации от изготовителей, продавцов, исполнителей и приобретателей, в том числе потребителей;
- ◆ единства системы и правил аккредитации;
- ◆ единства правил и методов исследований (испытаний) и измерений при проведении процедур обязательной оценки соответствия;
- ◆ единства применения требований технических регламентов независимо от видов или особенностей сделок;
- ◆ недопустимости ограничения конкуренции при аккредитации и сертификации;
- ◆ недопустимости совмещения одним органом полномочий по государственному контролю (надзору), за исключением осуществления контроля за деятельностью аккредитованных лиц, с полномочиями по аккредитации или сертификации;
- ◆ недопустимости совмещения одним органом полномочий по аккредитации и сертификации;
- ◆ недопустимости внебюджетного финансирования государственного контроля (надзора) за соблюдением требований технических регламентов;
- ◆ недопустимости одновременного возложения одних и тех же полномочий на два и более органа государственного контроля (надзора) за соблюдением требований технических регламентов.

Закон устанавливает следующие цели принятия технических регламентов:

- ◆ защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;
- ◆ охраны окружающей среды, жизни или здоровья животных и растений;
- ◆ предупреждения действий, вводящих в заблуждение приобретателей, в том числе потребителей;
- ◆ обеспечения энергетической эффективности и ресурсосбережения.

Принятие технических регламентов в иных целях не допускается.

Технический регламент должен содержать правила и формы оценки соответствия. Разработчиком проекта технического регламента может быть любое лицо. В качестве основы для разработки проектов технических регламентов могут быть полностью или частично использованы международные и национальные стандарты. На основании заключения экспертной комиссии федеральный орган исполнительной власти по техническому регулированию в течение десяти дней со дня поступления такого заключения принимает решение о принятии технического регламента или об отклонении его

проекта. Технический регламент вступает в силу не ранее чем через шесть месяцев со дня его официального опубликования.

Закон устанавливает следующие цели стандартизации:

- ◆ повышение уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества, повышение уровня экологической безопасности, безопасности жизни и здоровья животных и растений;
- ◆ обеспечение конкурентоспособности и качества продукции, добровольного подтверждения соответствия продукции (работ, услуг);
- ◆ содействие соблюдению требований технических регламентов;
- ◆ создание систем классификации и кодирования технико-экономической и социальной информации.

Закон устанавливает следующие принципы стандартизации:

- ◆ добровольного применения документов в области стандартизации;
- ◆ максимального учета при разработке стандартов законных интересов заинтересованных лиц;
- ◆ применения международного стандарта как основы разработки национального стандарта;
- ◆ недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг;
- ◆ недопустимости установления таких стандартов, которые противоречат техническим регламентам;
- ◆ обеспечения условий для единообразного применения стандартов.

Добровольность – это не только главный принцип стандартизации, но и основной элемент, определяющий правовой статус документов в области стандартизации в Российской Федерации как документов, которые не имеют обязательного характера и применяются исключительно на добровольной основе.

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;
- ◆ предварительные национальные стандарты.

Национальный стандарт и предварительный национальный стандарт применяются на добровольной основе. Разработчиком национального стандарта может быть любое лицо.

Статья 16 закона устанавливает правила разработки и утверждения национальных стандартов. Разработка и утверждение национальных стандартов осуществляются в следующей последовательности:

- ◆ организация разработки стандарта;
- ◆ разработка первой редакции проекта стандарта и ее публичное обсуждение;
- ◆ разработка окончательной редакции проекта стандарта и ее экспертиза (научно-техническая, правовая, патентная, терминологическая и метрологическая);
- ◆ подготовка проекта стандарта к утверждению, утверждение стандарта, его регистрация, опубликование и введение в действие.

В соответствии со ст. 17 закона организациями могут разрабатываться и утверждаться (руководителем организации) стандарты организаций.

Одним из важнейших элементов технического регулирования наряду с применением технических регламентов и стандартов является подтверждение соответствия. Закон устанавливает следующие принципы подтверждения соответствия:

- ◆ доступности информации о порядке подтверждения соответствия заинтересованным лицам;
- ◆ недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов;

- ◆ установления перечня форм и схем обязательного подтверждения соответствия в отношении определенных видов продукции в соответствующем техническом регламенте;
- ◆ уменьшения сроков обязательного подтверждения соответствия и затрат заявителя;
- ◆ недопустимости принуждения к добровольному подтверждению соответствия;
- ◆ защиты имущественных интересов заявителей, соблюдения коммерческой тайны в отношении сведений, полученных при подтверждении соответствия;
- ◆ недопустимости подмены обязательного подтверждения соответствия добровольной сертификацией.

Подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной 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, предварительным национальным стандартам, стандартам организаций, сводам правил, системам добровольной сертификации, условиям договоров.

Объекты сертификации, сертифицированные в системе добровольной сертификации, могут маркироваться знаком соответствия системы добровольной сертификации.

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

Обязательное подтверждение соответствия осуществляется в формах:

- ◆ принятия декларации о соответствии (декларирование соответствия);
- ◆ обязательной сертификации.

Декларирование соответствия осуществляется по одной из следующих схем:

- ◆ принятие декларации о соответствии на основании собственных доказательств;
- ◆ принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и/или аккредитованной испытательной лаборатории (третья сторона).

Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем. Соответствие продукции требованиям технических регламентов подтверждается сертификатом соответствия, выдаваемым заявителю органом по сертификации. В соответствии с законом необходимым условием деятельности органов по сертификации и испытательных лабораторий (центров) является их аккредитация.

Глава 6 закона посвящена организации государственного контроля за соблюдением требований технических регламентов.

За нарушение требований технических регламентов изготовитель несет ответственность в соответствии с законодательством Российской Федерации (Гражданский кодекс РФ, Кодекс РФ об административных правонарушениях, Уголовный кодекс РФ).

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

Технические регламенты, стандарты и другие документы национальной системы стандартизации составляют Федеральный информационный фонд технических регламентов и стандартов, который является государственным информационным ресурсом.

1.3. Основы стандартизации в Российской Федерации

1.3.1. Основные положения системы стандартизации в Российской Федерации (ГОСТ Р 1.0–2012)

Национальный стандарт Российской Федерации ГОСТ Р 1.0–2012 «Стандартизация в Российской Федерации. Основные положения» введен в действие 01.07.2013 г. взамен ранее принятому стандарту ГОСТ Р 1.0–2004.

Стандарт устанавливает основные положения по организации и проведению в Российской Федерации работ в области стандартизации, цели и принципы стандартизации, требования к документам в области стандартизации, правила их опубликования, распространения и применения, а также задачи международного сотрудничества в области стандартизации.

Стандарт устанавливает следующие принципы осуществления национальной стандартизации в Российской Федерации:

- ◆ добровольности применения заинтересованным лицом документов в области стандартизации и обязательности соблюдения указанным лицом требований, содержащихся в этих документах, в случае объявления об их использовании, а также в случае определения обязательности исполнения требований стандартов в рамках контрактных (договорных) обязательств;
- ◆ применения в установленном порядке на территории Российской Федерации международных и региональных стандартов, региональных сводов правил, стандартов иностранных государств и сводов правил иностранных государств;
- ◆ максимального учета мнения заинтересованных лиц при разработке документов в области стандартизации;
- ◆ обеспечения преемственности работ по стандартизации;
- ◆ обеспечения условий для единообразного применения документов в области стандартизации;
- ◆ открытости (прозрачности) процедур разработки документов в области стандартизации;
- ◆ обеспечения доступности документов в области стандартизации и информации о них для заинтересованных лиц;
- ◆ однозначности понимания требований, включаемых в документы в области стандартизации;
- ◆ соответствия документов в области стандартизации нормативным правовым актам Российской Федерации;
- ◆ прогрессивности и оптимальности требований документов в области стандартизации;
- ◆ недопустимости разработки национальных стандартов Российской Федерации на объекты и аспекты стандартизации, стандартизованные на межгосударственном уровне;
- ◆ недопустимости разработки и применения национальных стандартов Российской Федерации, которые создают излишние препятствия международной торговле;
- ◆ унификации процессов разработки, хранения стандартов, а также процессов внесения в них изменений и обеспечения доступа к документам в области стандартизации;
- ◆ обеспечения системности и комплексности информационных ресурсов в области стандартизации с использованием информационных технологий;

- ◆ обеспечения актуальности и достоверности информационных ресурсов в области стандартизации.

Раздел 5 стандарта посвящен организации работ по стандартизации и функциям национального органа по стандартизации – Федерального агентства по техническому регулированию и метрологии.

В разделах 6 и 7 описаны требования к документам в области стандартизации, порядок их опубликования и распространения.

Стандарт определяет также основные задачи международного сотрудничества в области стандартизации, а именно:

- ◆ гармонизация системы стандартизации Российской Федерации с международными, региональными прогрессивными национальными системами стандартизации других стран;
- ◆ совершенствование фонда документов в области стандартизации, используемых в Российской Федерации;
- ◆ гармонизация национальных стандартов Российской Федерации с международными, региональными стандартами и национальными стандартами других стран;
- ◆ повышение качества отечественной продукции и ее конкурентоспособности на мировом рынке;
- ◆ содействие внедрению инноваций, проведению технологической модернизации и продвижению отечественной продукции на мировой рынок;
- ◆ активное привлечение представителей отечественной промышленности к разработке международных и региональных стандартов;
- ◆ разработка международных и межгосударственных стандартов на основе национальных стандартов Российской Федерации;
- ◆ улучшение нормативного обеспечения торгово-экономического и научно-технического сотрудничества Российской Федерации с другими странами и участие Российской Федерации в международном разделении труда;
- ◆ обеспечение защиты национальных интересов Российской Федерации при разработке международных и региональных стандартов;
- ◆ обеспечение единства измерений при взаимодействии с другими странами.

1.3.2. Правила разработки национальных стандартов (ГОСТ Р 1.2–2014)

Национальный стандарт Российской Федерации ГОСТ Р 1.2–2014 «Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления и отмены» введен в действие с 1.01.2015 г. взамен ГОСТ Р 1.2–2004. Стандарт устанавливает правила разработки и утверждения национальных стандартов Российской Федерации, проведения работ по их обновлению, а также правила отмены действующих стандартов.

Разрабатывают национальные стандарты на основе программы разработки национальных стандартов в такой последовательности:

- ◆ организация разработки стандарта;
- ◆ разработка первой редакции проекта стандарта и ее публичное обсуждение;
- ◆ разработка окончательной редакции проекта стандарта и ее экспертиза;
- ◆ подготовка проекта стандарта к утверждению, утверждение стандарта, его регистрация, опубликование и введение в действие.

Требования, устанавливаемые в национальном стандарте, должны соответствовать современному уровню развития техники и не должны противоречить техническим регламентам Таможенного союза, федеральным законам, техническим регламентам, иным нормативным правовым актам Российской Федерации, относящимся к данному объекту и/или аспекту стандартизации. Национальные стандарты Российской Федерации разрабатывают на основе применения международных стандартов.

В разделе 4 подробно описаны правила разработки и утверждения национальных стандартов в соответствии с приведенной ранее последовательностью. Утвержденный стандарт должен быть официально опубликован незамедлительно, не позднее даты его введения в действие.

В разделе 5 описаны правила проведения работ по обновлению национальных стандартов, а в разделе 6 – правила отмены национальных стандартов.

Официальное опубликование обновленного стандарта и информации об отмене стандарта осуществляют национальный орган Российской Федерации по стандартизации (Росстандарт).

1.3.3. Стандарты организаций (ГОСТ Р 1.4–2004)

Национальный стандарт Российской Федерации ГОСТ Р 1.4–2004 «Стандарты организаций. Общие положения» введен в действие с 01.07.2005 г.

и устанавливает объекты стандартизации и общие положения при разработке и применении стандартов организаций.

Стандарты организаций, в том числе коммерческих, общественных, научных, саморегулируемых, а также объединений юридических лиц разрабатываются этими организациями в случаях и на условиях, указанных в ст. 17 закона № 184-ФЗ «О техническом регулировании».

Стандарты организации могут разрабатываться на применяемые в данной организации продукцию, процессы и оказываемые в ней услуги, а также на продукцию, созданную и поставляемую данной организацией на внутренний и внешний рынок, на работы, выполняемые данной организацией на стороне, и оказываемые ею на стороне услуги в соответствии с заключенными договорами.

Стандарты организации не должны противоречить требованиям технических регламентов, а также национальных стандартов. Порядок разработки, утверждения, учета, изменения и отмены стандартов организаций устанавливается организациями самостоятельно. Стандарты организации утверждает руководитель (заместитель руководителя) организации приказом и/или личной подписью на титульном листе стандарта в установленном в организации порядке. В случае утверждения стандарта организации приказом дату введения стандарта в действие устанавливают в приказе.

При необходимости проект стандарта может быть направлен организацией-разработчиком в специализированные организации для проведения экспертизы. Стандарт организации, разработанный и утвержденный одной организацией, может использоваться другой организацией в своих интересах только по договору с утвердившей его организацией.

Организация, разработавшая и утвердившая стандарт организации на продукцию, поставляемую на внутренний или внешний рынок, может при необходимости готовить предложения о разработке национального стандарта на основе этого стандарта.

1.4. Основы стандартизации в области защиты информации

1.4.1. Основные термины в сфере защиты информации (ГОСТ Р 50922–2006)

Национальный стандарт Российской Федерации ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» введен с 01.02.2008 г. взамен ГОСТ Р 50922–96.

Стандарт устанавливает основные термины, применяемые при проведении работ по стандартизации в области защиты информации, и рекомендует использовать их в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе. Далее приведены некоторые из терминов с соответствующими определениями.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов, регулирующих отношения субъектов по защите информации, применение этих документов, а также надзор и контроль за их исполнением.

Техническая ЗИ — ЗИ, заключающаяся в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Физическая ЗИ — ЗИ путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Криптографическая ЗИ — ЗИ с помощью ее криптографического преобразования.

Система ЗИ — совокупность органов и/или исполнителей, используемых ими техники ЗИ, а также объектов ЗИ, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области ЗИ.

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

Оценка соответствия требованиям по ЗИ — прямое или косвенное определение степени соблюдения требований по ЗИ, предъявляемых к объекту ЗИ.

Сертификация на соответствие требованиям по безопасности информации — форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Средство контроля эффективности ЗИ — средство ЗИ, предназначенное или используемое для контроля эффективности ЗИ.

Угроза — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уязвимость (информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа к информации и/или воздействия на информацию или ресурсы ИС.

Средство защиты информации — техническое, программное, программенно-техническое средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Эффективность защиты информации — степень соответствия результатов защиты информации цели защиты информации.

До принятия рассматриваемого стандарта действовали рекомендации по стандартизации: Р 50.1.053–2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (дата введения 01.01.2006 г.) и Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения» (дата введения 01.06.2006 г.). Термины, установленные настоящими рекомендациями, должны применяться совместно с ГОСТ Р 50922.

1.4.2. Защита информации в организации (ГОСТ Р 53114–2008)

Национальный стандарт Российской Федерации ГОСТ Р 53114–2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» введен с 01.10.2009 г. Стандарт устанавливает основные термины, применяемые при проведении работ по стандартизации в области обеспечения информационной безопасности в организации.

Информационная сфера — совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Критически важная система информационной инфраструктуры — информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критическим объектом или процессом или его информационное обеспечение, нарушение или прерывание функционирования которой может привести к чрезвычайной ситуации со значительными негативными последствиями.

Критический объект — объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб.

Объект защиты информации — информация, или носитель информации, или информационный процесс, который необходимо защищать в соответствии с целью ЗИ.

Инцидент ИБ — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

В стандарте указаны следующие виды инцидентов:

- ◆ утрата услуг, оборудования или устройств;
- ◆ системные сбои или перегрузки;
- ◆ ошибки пользователей;
- ◆ несоблюдение политики или рекомендаций по ИБ;
- ◆ нарушение физических мер защиты;
- ◆ неконтролируемые изменения систем;
- ◆ сбои программного обеспечения и технических средств;
- ◆ нарушение правил доступа.

Аудит информационной безопасности организации — систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ и установлению степени выполнения в организации критериев ИБ.

Оценка соответствия ИБ организации установленным требованиям — деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований ИБ.

Аттестация АС в защищенном исполнении — процесс комплексной проверки выполнения заданных функций АС по обработке защищаемой информации на соответствие требованиям стандартов или нормативных документов в области ИБ.

Критерий обеспечения ИБ организации — показатель, на основании которого оценивается степень достижения цели (целей) ИБ организации.

Меры обеспечения информационной безопасности — совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения ИБ.

Организационные меры обеспечения информационной безопасности — меры обеспечения ИБ, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

1.4.3. Система стандартов по защите информации (ГОСТ Р 52069.0–2013)

Стандарт ГОСТ Р 52069.0–2013 «Защита информации. Система стандартов. Основные положения» введен в действие с 01.09.2013 г. взамен ГОСТ Р 52069.0–2003. Он устанавливает цель, задачи и структуру системы стандартов по защите (некриптографическими методами) информации, объекты и аспекты стандартизации в данной области и является основополагающим национальным стандартом Российской Федерации в области защиты информации. Положения стандарта применяются при проведении работ по стандартизации в области противодействия техническим разведкам, технической защиты информации, обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

Система стандартов по защите информации является составной частью национальной системы стандартизации Российской Федерации.

Основными задачами по формированию и развитию ССЗИ являются:

- ◆ установление основополагающих принципов построения, требований к составу и содержанию системы документов в области ЗИ;
- ◆ обеспечение единства терминологии в области ЗИ;
- ◆ упорядочение объектов и аспектов стандартизации в области ЗИ;
- ◆ обеспечение единства организационных и методических подходов к проведению работ по ЗИ;
- ◆ установление системы требований по ЗИ и методов контроля выполнения этих требований;
- ◆ установление общих технических требований к средствам ЗИ и услугам по ЗИ;
- ◆ установление требований к методам и методикам испытаний и оценки качества СЗИ;
- ◆ установление требований к метрологическому, информационному и другим видам обеспечения ЗИ.

Основными объектами стандартизации ССЗИ являются:

- ◆ ЗИ как область деятельности:
 - противодействие техническим разведкам;
 - техническая ЗИ;
 - обеспечение безопасности информации в ключевых системах информационной инфраструктуры;

- ◆ объекты ЗИ (промышленные объекты, объекты науки, энергетики, жизнеобеспечения, органов управления, информатизации, продукция);
- ◆ угрозы безопасности информации и уязвимости объектов ЗИ;
- ◆ организация и содержание работ по ЗИ;
- ◆ методы (процессы, работы, технологии) ЗИ и методы контроля состояния ЗИ;
- ◆ техника ЗИ (средства ЗИ, средства контроля эффективности ЗИ);
- ◆ услуги по ЗИ.

Основными аспектами стандартизации в ССЗИ являются:

- ◆ термины и определения в области ЗИ;
- ◆ классификация в области ЗИ (угроз, уязвимостей, работ и услуг по ЗИ, техники ЗИ);
- ◆ требования к системе документов в области ЗИ;
- ◆ общие технические требования по ЗИ, предъявляемые к объектам;
- ◆ общие требования к организации и содержанию работ по ЗИ;
- ◆ общие технические требования к СЗИ и системе контроля эффективности ЗИ и методам их испытаний;
- ◆ методы контроля организации и эффективности ЗИ, методы измерений при проведении контроля;
- ◆ общие требования к организации, содержанию работ и результатам оказания услуг по ЗИ.

Система стандартов по защите информации включает следующие виды документов в области стандартизации по ЗИ:

- ◆ национальные стандарты Российской Федерации, в том числе ограниченного распространения, государственные военные стандарты, национальные стандарты, оформленные на основе аутентичных переводов международных стандартов;
- ◆ межгосударственные стандарты;
- ◆ правила стандартизации, нормы и рекомендации в области стандартизации;
- ◆ общероссийские классификаторы технико-экономической и социальной информации;
- ◆ стандарты организаций;
- ◆ предварительные национальные стандарты;

- ◆ международные стандарты, региональные стандарты, региональные своды правил, стандарты иностранных государств и своды правил иностранных государств, принятые на учет национальным органом Российской Федерации по стандартизации, и их надлежащим образом заверенные переводы на русский язык.

Стандарты организаций по ЗИ разрабатываются организациями и утверждаются ими самостоятельно, исходя из необходимости применения этих стандартов для целей стандартизации по ЗИ, и не должны противоречить другим документам в области стандартизации по ЗИ, используемым на территории Российской Федерации.

Структура системы стандартов по ЗИ представлена на рис. 1.1.



Рис. 1.1. Структура системы стандартов по ЗИ

Система стандартов по защите информации включает подсистемы стандартов в области:

- ◆ противодействия техническим разведкам;
- ◆ технической защиты информации;
- ◆ обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

В каждой области подсистемы стандартов ССЗИ включают следующие комплексы стандартов:

- ◆ комплекс общесистемных стандартов по ЗИ;
- ◆ комплексы стандартов по ЗИ для различных классов объектов;

- ◆ комплексы стандартов по технике ЗИ;
- ◆ комплекс стандартов на услуги по ЗИ.

1.4.4. Факторы, воздействующие на информацию (ГОСТ Р 51275–2006)

Национальный стандарт Российской Федерации ГОСТ Р 51275–2006 «Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения» введен в действие с 01.02.2008 г. взамен ранее принятому стандарту ГОСТ Р 51275–99.

Стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

Стандарт вводит ряд понятий.

Программная закладка — преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Недекларированные возможности (программного обеспечения) — функциональные возможности программного обеспечения, не описанные в документации.

Вредоносная программа — программа, используемая для несанкционированного доступа к информации и/или воздействия на информацию или ресурсы автоматизированной информационной системы.

Выявление и учет факторов, действующих или могущих действовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации. По признаку отношения к природе возникновения все факторы подразделяют на объективные и субъективные. По отношению к объекту информатизации факторы подразделяют на внутренние и внешние.

Объективные внутренние факторы:

- ◆ передача сигналов по проводным и оптико-волоконным линиям связи, в диапазоне радиоволн и оптическом диапазоне длин волн;
- ◆ излучения акустических сигналов, электромагнитные излучения и поля;
- ◆ побочные электромагнитные излучения;
- ◆ паразитное электромагнитное излучение;

- ◆ наводка в электрических цепях, линиях связи, цепях электропитания, цепях заземления, технических средствах;
- ◆ наличие акустоэлектрических преобразователей в элементах технических средств;
- ◆ дефекты, сбои и отказы, аварии технических средств и программного обеспечения.

Объективные внешние факторы:

- ◆ явления техногенного характера;
- ◆ природные явления;
- ◆ стихийные бедствия.

Субъективные внутренние факторы:

- ◆ разглашение защищаемой информации лицами, имеющими к ней право доступа;
- ◆ неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации;
- ◆ несанкционированный доступ к информации;
- ◆ недостатки организационного обеспечения защиты информации;
- ◆ ошибки обслуживающего персонала.

Субъективные внешние факторы:

- ◆ доступ к защищаемой информации с применением технических средств;
- ◆ несанкционированный доступ к защищаемой информации;
- ◆ блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- ◆ действия криминальных групп и отдельных преступных субъектов;
- ◆ искажение, уничтожение или блокирование информации с применением технических средств.

1.4.5. Оценка соответствия (ГОСТ 17000–2012)

Межгосударственный стандарт ГОСТ ИСО/МЭК 17000–2012 «Оценка соответствия. Словарь и общие принципы» принят Межгосударственным советом по стандартизации, метрологии и сертификации (Азербайджан, Армения, Киргизия, Россия) в январе 2012 г. Приказом Федерального агентства по техническому регулированию и метрологии от 25.12.2012 г. он введен в действие в качестве национального стандарта Российской Федерации

с 01.09.2013 г. Стандарт подготовлен на основе применения ГОСТ Р ИСО/МЭК 17000–2009, который был отменен. Он идентичен международному стандарту ISO/IEC 17000:2004 «Conformity assessment – Vocabulary and general principles» («Оценка соответствия. Словарь и общие принципы»).

Стандарт устанавливает общие термины и определения, относящиеся к оценке соответствия, включая аккредитацию органов по оценке соответствия. В приложении к стандарту дано описание функционального подхода к оценке соответствия, который используется в рамках как добровольных, так и обязательных систем оценки соответствия.

Стандарт вводит ряд терминов в области оценки соответствия.

Оценка соответствия — доказательство того, что заданные требования к продукции, процессу, системе, лицу или органу выполнены.

Оценка соответствия в соответствии со стандартом включает в себя следующие базовые виды деятельности:

- ◆ испытание;
- ◆ контроль;
- ◆ сертификацию;
- ◆ аккредитацию органов по оценке соответствия.

В стандарте различается деятельность трех сторон по оценке соответствия:

- ◆ деятельность по оценке соответствия первой стороной — деятельность по оценке соответствия, которую осуществляет лицо или организация, предоставляющая объект (например, разработчик или поставщик);
- ◆ деятельность по оценке соответствия второй стороной — деятельность по оценке соответствия, которую осуществляет лицо или организация, заинтересованная в объекте как пользователь;
- ◆ деятельность по оценке соответствия третьей стороной — деятельность по оценке соответствия, которую осуществляет лицо или орган, независимый от лица или организации, предоставляющей объект, и от пользователя, заинтересованного в этом объекте (например, аккредитованная испытательная лаборатория).

Орган по оценке соответствия — орган, оказывающий услуги по оценке соответствия.

Орган по аккредитации — полномочный орган, который проводит аккредитацию (обычно орган по аккредитации получает полномочия от правительства).

Система оценки соответствия — правила, процедуры и менеджмент, используемые для выполнения оценки соответствия. Системы оценки соответствия могут действовать на международном, региональном, национальном уровнях.

Схема оценки соответствия (программа оценки соответствия) – система оценки соответствия, относящаяся к определенным объектам оценки соответствия, к которым применяются одни и те же заданные требования, определенные правила и процедуры.

Процедура – установленный способ осуществления деятельности или процесса.

Испытание – определение одной или более характеристик объекта оценки соответствия согласно процедуре.

Контроль – проверка проекта, продукции или процесса и определение их соответствия заданным требованиям или, на основе профессионального суждения, общим требованиям. Контроль процесса может предусматривать проверку персонала, оборудования, технологии и методологии.

Аудит – систематический, независимый и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективного оценивания с целью установления степени выполнения заданных требований.

Подтверждение соответствия – выдача заявления, основанного на принятом после итоговой проверки решении о том, что выполнение заданных требований доказано.

Декларация – подтверждение соответствия первой стороной.

Сертификация – подтверждение соответствия третьей стороной, относящееся к продукции, процессам, системам или персоналу.

Согласно Постановлению Правительства Российской Федерации от 26.06.1995 г. № 608 руководство системами сертификации в России возложено на федеральные органы исполнительной власти: ФСБ, ФСТЭК, Минобороны, СВР. Эти органы в рамках своей компетенции создают свои правила и процедуры оценки соответствия (системы сертификации). Участниками сертификации являются заявитель (разработчик, изготовитель, поставщик), федеральный орган по сертификации, аккредитованный орган по сертификации, аккредитованная испытательная лаборатория.

Порядок проведения сертификации состоит из следующих этапов.

1. Заявитель подает в федеральный орган заявку на проведение сертификации.
2. Федеральный орган определяет аккредитованную испытательную лабораторию и орган по сертификации.
3. Испытательная лаборатория проводит сертификационные испытания.
4. Материалы испытаний передаются в орган по сертификации, который проводит их независимую экспертизу и дает техническое заключение.

5. На основании технического заключения федеральный орган дает заявителю заключение, а в случае положительного решения оформляет сертификат соответствия.

В ряде случаев, определенных требованиями нормативных документов федеральных органов и законов Российской Федерации, сертификация средств защиты информации является обязательной.

Аkkредитация — подтверждение соответствия третьей стороной, относящееся к органу по оценке соответствия и служащее официальным признанием его компетентности для выполнения конкретных задач по оценке соответствия.

Функциональный подход к оценке соответствия по стандарту представляет собой последовательность трех функций, которые удовлетворяют необходимости или потребности доказать, что заданные требования выполняются:

- ◆ выбор;
- ◆ определение;
- ◆ итоговая проверка и подтверждение соответствия.

В качестве заданных требований часто используются стандарты, так как они являются документами, отражающими широкий консенсус по вопросам, которые хотят решить в данной ситуации. В результате оценка соответствия часто рассматривается как деятельность, связанная со стандартами.

Оценка соответствия может быть применена к продукции (включая услуги), процессам, системам и персоналу, а также к органам, предоставляющим услуги по оценке соответствия. Каждая из категорий пользователей услуг по оценке соответствия имеет конкретные потребности. В результате наблюдается многообразие видов деятельности по оценке соответствия. Однако в основе всех них лежит общий подход (рис. 1.2).

На рисунке контур А обозначает функции оценки соответствия. Конкретные виды деятельности в каждой из функций могут меняться в зависимости от вида оценки соответствия. Контур В обозначает выход из функции и вход в следующую функцию. Характер выхода меняется в зависимости от конкретных видов деятельности. Сплошные стрелки связывают функции оценки соответствия и их выходы/входы. Пунктирные стрелки указывают на возможную необходимость или возможное требование проведения оценки соответствия.

Функция выбора предусматривает планирование и подготовку действий для сбора или представления всей информации, являющейся входными данными для следующей функции — определения. Для выбора объекта оценки соответствия необходимо принимать во внимание его особенности. Функция выбора может также включать в себя отбор наиболее подходящих процедур (например, методов испытания или контроля), применяемых для выполнения действий в рамках функции определения.

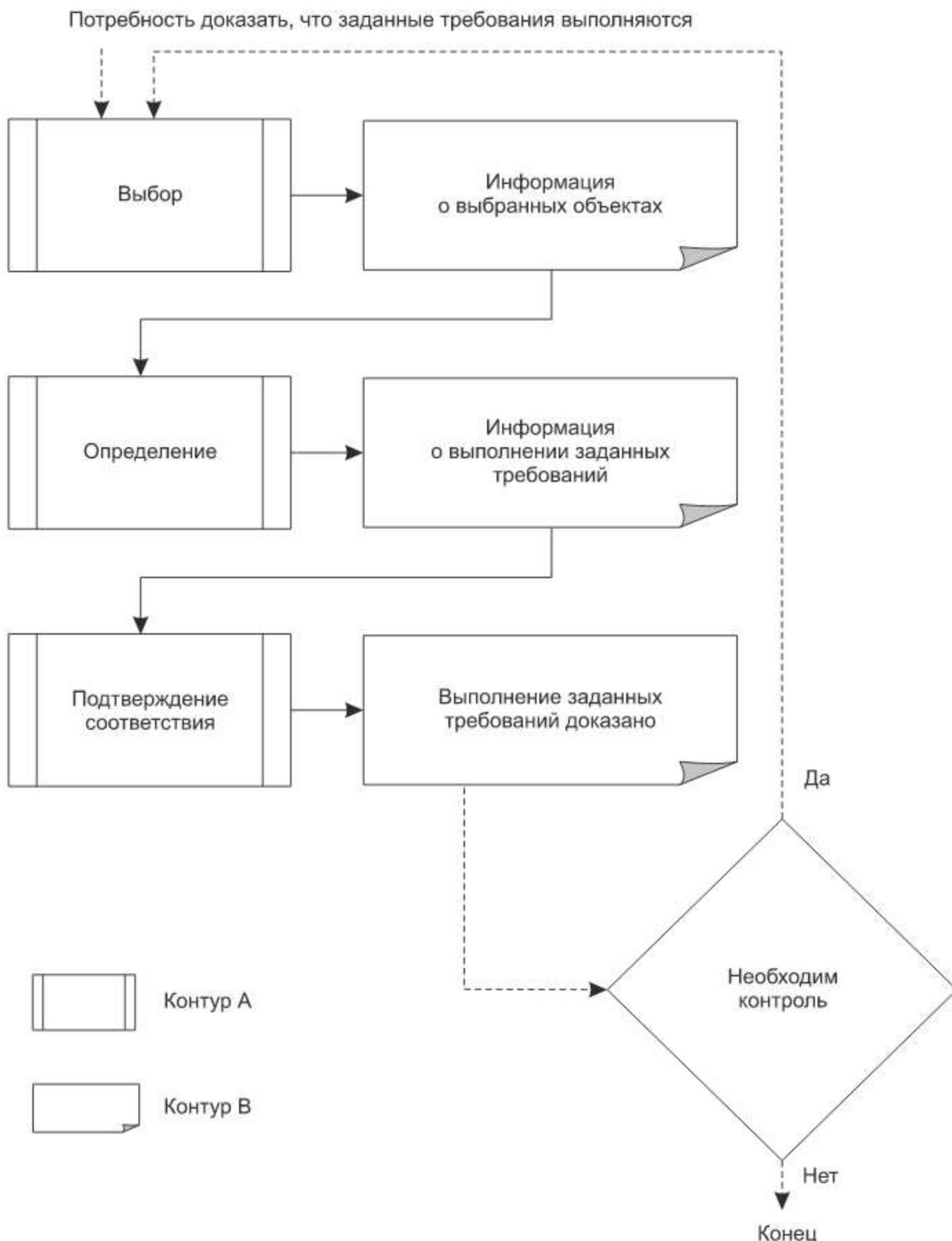


Рис. 1.2. Функциональный подход к оценке соответствия

Действия по определению предпринимаются с целью получения полной информации о выполнении заданных требований объектом оценки соответствия или его образцом.

Итоговая проверка (подтверждение соответствия) является завершающей стадией перед принятием решения о том, было ли в достаточном объеме доказано выполнение объектом оценки соответствия заданных требований. Если выполнение заданных требований не было доказано, то в отчете может содержаться заключение о несоответствии.

Оценка соответствия может быть закончена, когда подтверждено соответствие. Однако в некоторых случаях может потребоваться систематическое повторение оценки. Например, объект оценки соответствия может со временем измениться, что может отрицательно повлиять на продолжение выполнения заданных требований.

При каждом повторном инспекционном контроле не требуется полного повторения первичной оценки. Действия в рамках всех функций, представленных на рис. 1.2, во время инспекционного контроля могут быть сокращены или могут отличаться от действий при первичной оценке. Выбор заданных требований также может быть разным. Например, при любом повторном инспекционном контроле может быть выбрана отдельная группа заданных требований или часть объекта оценки.

Функция итоговой проверки и подтверждения соответствия применяется как при первичной оценке, так и при инспекционном контроле.

Контрольные вопросы и задания к главе 1

1. Каковы основные этапы информатизации общества?
2. Каковы основные проблемы современного информационного общества при использовании информации?
3. Каковы основные причины актуальности проблемы защиты информации в современном обществе?
4. Каковы основные угрозы в области международной информационной безопасности?
5. Каковы основные виды уголовно наказуемых преступлений в информационной сфере?
6. В чем заключаются цели принятия федерального закона «О техническом регулировании»?
7. Какой орган государственной власти осуществляет деятельность по стандартизации и техническому регулированию?
8. Каковы основные функции Росстандарта РФ?

9. В чем отличие стандарта Российской Федерации от технического регламента?
10. Дайте определения терминам «национальный стандарт» и «технический регламент».
11. Назовите основные принципы технического регулирования.
12. Назовите основные принципы стандартизации.
13. Назовите основные этапы разработки стандарта.
14. В чем заключается подтверждение соответствия? Назовите виды подтверждения соответствия.
15. Назовите формы подтверждения соответствия.
16. Каков порядок разработки и утверждения стандартов организаций?
17. Назовите основные стандарты Российской Федерации, закладывающие основы стандартизации.
18. Дайте определение термину «защита информации».
19. Дайте определение терминам «правовая ЗИ», «техническая ЗИ», «физическая ЗИ», «криптографическая ЗИ».
20. Что такое критически важная система информационной инфраструктуры?
21. Каковы основные задачи системы стандартизации в области ЗИ?
22. Перечислите виды документов в области стандартизации по ЗИ.
23. Какова структура стандартов в области ЗИ?
24. Что такое программная закладка?
25. Назовите основные факторы, воздействующие на защищаемую информацию.
26. Какие базовые виды деятельности предусматривает оценка соответствия?
27. В чем состоит функциональный подход к оценке соответствия?
28. В чем заключается разница в деятельности по оценке соответствия первой, второй и третьей сторон?
29. Дайте определения понятиям «декларация», «сертификация» и «аккредитация».
30. Какие федеральные органы исполнительной власти создают системы сертификации, на каком основании?

Глава 2. Нормативные документы ФСТЭК России

2.1. Основные нормативные документы в области защиты информации

Федеральные органы исполнительной власти Российской Федерации в соответствии с их компетенциями в области обеспечения информационной безопасности разрабатывают и утверждают нормативно-технические, методические документы и национальные стандарты, регламентирующие различные аспекты деятельности по защите информации, а также устанавливающие требования к системам обработки информации, критерии и методы оценки их защищенности.

В качестве основных открытых документов (кроме документов в области криптографической защиты) можно привести следующие.

1. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30.03.1992 г.
2. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия, 1992.
3. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Гостехкомиссии от 30.03.1992 г.
4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Гостехкомиссии от 30.03.1992 г.
5. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа

- в автоматизированных системах и средствах вычислительной техники. Утверждено решением председателя Гостехкомиссии от 30.03.1992 г.
6. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии от 25.11.1994 г.
 7. Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии от 27.10.1995 г. № 199.
 8. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Гостехкомиссии от 25.07.1997 г.
 9. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утверждено решением председателя Гостехкомиссии от 25.07.1997 г.
 10. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Гостехкомиссии от 04.06.1999 г. № 114.
 11. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г.
 12. Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г.
 13. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003 г.
 14. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 г.
 15. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие приказом Гостехкомиссии России от 19.06.2002 г. № 187.
 16. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2.

Функциональные требования безопасности. Введен в действие приказом Гостехкомиссии России от 19.06.2002 г. № 187.

17. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Введен в действие приказом Гостехкомиссии России от 19.06.2002 г. № 187.
18. Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
19. ГОСТ Р ИСО/МЭК 15408-1–2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
20. ГОСТ Р ИСО/МЭК 15408-2–2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».
21. ГОСТ Р ИСО/МЭК 15408-3–2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».
22. ГОСТ Р ИСО /МЭК 27033-1–2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
23. ГОСТ Р ИСО/МЭК 27033-3–2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления».
24. ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
25. ГОСТ Р ИСО/МЭК 27001–2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
26. ГОСТ Р ИСО/МЭК 27002–2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

27. ГОСТ Р ИСО/МЭК 27003–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
28. ГОСТ Р ИСО/МЭК 27004–2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
29. ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
30. ГОСТ Р ИСО/МЭК 27006–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
31. ГОСТ Р ИСО/МЭК 27007–2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности».
32. ГОСТ Р ИСО/МЭК 27011–2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».
33. Р 50.1.053–2005 «Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации».
34. Р 50.1.056–2005 «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения».
35. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».
36. ГОСТ Р 53114–2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».
37. ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
38. ГОСТ Р 51275–2006 «Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения».
39. ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

40. ГОСТ Р 56093–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования».
41. ГОСТ Р 56103–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения».
42. ГОСТ Р 56115–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования».
43. ГОСТ Р 51188–98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».
44. ГОСТ Р 52069.0–2013 «Защита информации. Система стандартов. Основные положения».
45. ГОСТ Р 56045–2014 «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью».
46. ГОСТ Р ИСО/МЭК 13335-1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
47. ГОСТ Р ИСО/МЭК ТО 13335-5–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».
48. ГОСТ Р ИСО/МЭК 18045–2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
49. ГОСТ Р ИСО/МЭК ТО 19791–2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
50. ГОСТ ИСО/МЭК 17000–2012 «Оценка соответствия. Словарь и общие принципы».
51. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 г. № 638.
52. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 г. № 28.
53. Требования к средствам контроля съемных машинных носителей. Утверждены приказом ФСТЭК России от 28.07.2014 г. № 87.

54. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 г. № 119.
55. Профиль защиты средств антивирусной защиты. Пакет методических документов. Утвержден ФСТЭК России 14.06.2012 г.
56. Профиль защиты систем обнаружения вторжений. Пакет методических документов. Утвержден ФСТЭК России 03.02.2012 г. и 06.03.2012 г.
57. Профиль защиты средств контроля подключения съемных машинных носителей информации. Пакет методических документов. Утвержден ФСТЭК России 01.12.2014 г.
58. Профиль защиты средства доверенной загрузки. Пакет методических документов. Утвержден ФСТЭК России 30.12.2013 г.
59. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
60. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18.02.2013 г. № 21.
61. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11.02.2014 г.
62. Приказ ФСБ и ФСТЭК от 31.08.2010 г. № 416/489 «О защите информации, содержащейся в информационных системах общего пользования».
63. ГОСТ Р ИСО/МЭК ТО 15446–2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».
64. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
65. ГОСТ Р ИСО/МЭК 27034-1–2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия».
66. ГОСТ Р 52447–2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества».
67. ГОСТ Р 52448–2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения».
68. ГОСТ Р 53110–2008 «Система обеспечения информационной безопасности. Сети связи общего пользования. Общие положения».

69. ГОСТ Р 52633.0–2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
70. ГОСТ Р 52633.1–2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».
71. ГОСТ Р 52633.2–2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».
72. ГОСТ Р 52633.3–2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
73. ГОСТ Р 52633.4–2011 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия – код доступа».
74. ГОСТ Р 52633.5–2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия – код доступа».
75. ГОСТ Р 52633.6–2012 «Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу “Свой”».
76. ГОСТ Р 53113.1–2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».
77. ГОСТ Р 53113.2–2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».
78. ГОСТ Р 53115–2008 «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства».
79. ГОСТ Р 53131–2008. «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов

безопасности информационных и телекоммуникационных технологий. Общие положения».

80. ГОСТ Р 56545–2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».
81. ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».
82. ГОСТ Р–2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет».
83. Комплекс стандартов по информационной безопасности Банка России (серия БР ИББС).

2.2. Защита от несанкционированного доступа к информации. Термины и определения

Руководящий документ Гостехкомиссии России от 30.03.1992 г. «Защита от несанкционированного доступа к информации. Термины и определения» устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Далее приведены некоторые из терминов.

Конфиденциальная информация – информация, требующая защиты.

ПРИМЕЧАНИЕ

Данный термин был законодательно закреплен Федеральным законом от 20.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» как «документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации». Однако из нового закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» этот термин исключен. Вместо него введен термин, отражающий свойство информации: «Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Доступ к информации – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС.

Защита от НСД – предотвращение или существенное затруднение НСД.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа – единица информационного ресурса АС, доступ к которой регламентируется правилами разграничения доступа.

Матрица доступа – таблица, отображающая правила разграничения доступа.

Уровень полномочий субъекта – совокупность прав доступа субъекта доступа.

Комплекс средств защиты – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты СВТ или АС от НСД к информации.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Пароль – идентификатор субъекта доступа, который является его секретом.

Безопасность информации – состояние защищенности информации, обрабатываемой СВТ или АС, от внутренних или внешних угроз.

Дискреционное управление доступом – разграничение доступа между поименованными субъектами и поименованными объектами.

Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении субъектов обращаться к информации такого уровня конфиденциальности.

Класс защищенности СВТ (АС) – определенная совокупность требований по защите СВТ (АС) от НСД к информации.

Средство криптографической защиты информации — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Сертификация — процесс установления соответствия СВТ или АС набору определенных требований по защите.

2.3. Концепция защиты СВТ и АС от НСД к информации

Руководящий документ Гостехкомиссии России от 30.03.1992 г. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» излагает систему взглядов и основных принципов, которые закладываются в основу проблемы защиты информации от НСД. Концепция предусматривает существование двух относительно самостоятельных направлений в проблеме защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Документ является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

- ◆ выработку требований по защите СВТ и АС от НСД к информации;
- ◆ создание защищенных от НСД к информации СВТ и АС;
- ◆ сертификацию защищенных СВТ и АС.

Защита СВТ обеспечивается комплексом программно-технических средств. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС.

Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

В соответствии с моделью в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ. Нарушители классифицируются по четырем иерархическим уровням возможностей (каждый следующий уровень включает в себя функциональные возможности предыдущего).

- ◆ Уровень 1 (самый низкий) — возможность запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

- ◆ Уровень 2 – возможность создания и запуска собственных программ с новыми функциями обработки информации.
- ◆ Уровень 3 – возможность управления функционированием АС, то есть воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.
- ◆ Уровень 4 – определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями обработки информации.

К основным способам НСД относятся:

- ◆ непосредственное обращение к объектам доступа;
- ◆ создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- ◆ модификация средств защиты, позволяющая осуществить НСД;
- ◆ внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Защита СВТ и АС обеспечивается:

- ◆ системой разграничения доступа субъектов к объектам доступа;
- ◆ обеспечивающими средствами для СРД.

Основными функциями СРД являются:

- ◆ реализация правил разграничения доступа субъектов и их процессов к данным;
- ◆ реализация ПРД субъектов к устройствам создания твердых копий;
- ◆ изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- ◆ управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;
- ◆ реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Обеспечивающие средства для СРД выполняют следующие функции:

- ◆ идентификацию и аутентификацию субъектов и поддержание привязки субъекта к процессу;
- ◆ регистрацию действий субъекта и его процесса;

- ◆ предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- ◆ реагирование на попытки НСД, восстановление после НСД;
- ◆ тестирование;
- ◆ очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- ◆ учет выходных печатных и графических форм и твердых копий в АС;
- ◆ контроль целостности программной и информационной части.

Полнота и качество СРД оцениваются по наличию четких непротиворечивых правил доступа к объектам доступа.

При оценке состава и качества обеспечивающих средств для СРД учитываются средства идентификации и опознания субъектов и порядок их использования, полнота учета действий субъектов и способы поддержания привязки субъекта к его процессу.

Оцениваемые АС или СВТ должны быть тщательно документированы. В состав документации включаются «Руководство пользователя» по использованию защитных механизмов и «Руководство по управлению средствами защиты». Оценка АС и СВТ, претендующих на высокий уровень защищенности, осуществляется при наличии проектной документации (эскизный, технический и рабочий проекты), а также описаний процедур тестирования и их результатов.

Для детальной, дифференцированной разработки требований по защите от НСД производится классификация АС.

В основу системы классификации АС положены характеристики:

- ◆ информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС из-за потери информации;
- ◆ организационные, определяющие полномочия пользователей;
- ◆ технологические, определяющие условия обработки информации, – способ обработки (автономный, мультипрограммный и т. д.), время циркуляции (транзит, хранение и т. д.), вид АС (автономная, сеть, стационарная, подвижная и т. д.).

Организация работ по защите СВТ и АС от НСД к информации должна быть частью общей организации работ по безопасности информации. Разработка мероприятий по защите должна проводиться одновременно с разработкой СВТ и АС.

На базе Концепции Гостехкомиссией 30.03.1992 г. утвержден руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Положение определяет следующие основные вопросы:

- ◆ организационную структуру и порядок проведения работ по защите информации от НСД;
- ◆ систему государственных нормативных актов, стандартов, руководящих документов и требований по этой проблеме;
- ◆ порядок разработки и изготовления защищенных СВТ, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД;
- ◆ порядок приемки и сертификации указанных средств и систем перед сдачей в эксплуатацию в составе АС, порядок их эксплуатации и контроля работоспособности этих средств и систем в процессе эксплуатации;
- ◆ порядок обучения, переподготовки и повышения квалификации специалистов в области защиты информации от НСД.

2.4. Показатели защищенности СВТ от НСД к информации

Руководящий документ Гостехкомиссии России от 30.03.1992 г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под СВТ в документе понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Устанавливаются семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Класс 7 присваивают СВТ, к которым предъявлялись требования по защите от НСД, но при оценке защищенность оказалась ниже уровня требований класса 6.

Выбор класса защищенности СВТ для АС, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы. Перечень показателей по классам защищенности СВТ приведен в табл. 2.1.

Таблица 2.1. Показатели защищенности СВТ

Показатель	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения в таблице:

«-» — нет требований к данному классу;

«+» — новые или дополнительные требования;

«=» — требования совпадают с требованиями к СВТ предыдущего класса.

Требования к СВТ варьируются по уровню и глубине в зависимости от соответствующего класса защищенности. С точки зрения принципиальных моментов безопасности информации можно выделить три группы СВТ (рис. 2.1):

1. СВТ с гарантированной (верифицированной) защитой информации – класс 1.
2. СВТ с полномочным (мандатным) управлением доступом – классы 2–4.
3. СВТ с избирательным (дискреционным) управлением доступом – классы 5 и 6.

Классы 5 и 6 могут быть использованы для защиты информации конфиденциального характера (например, персональных данных), классы с 4-го по 2-й – для защиты сведений, составляющих государственную тайну.

После утверждения рассматриваемого руководящего документа Гостехкомиссии в 1995 г. был принят ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования». Описание этого стандарта приведено далее.

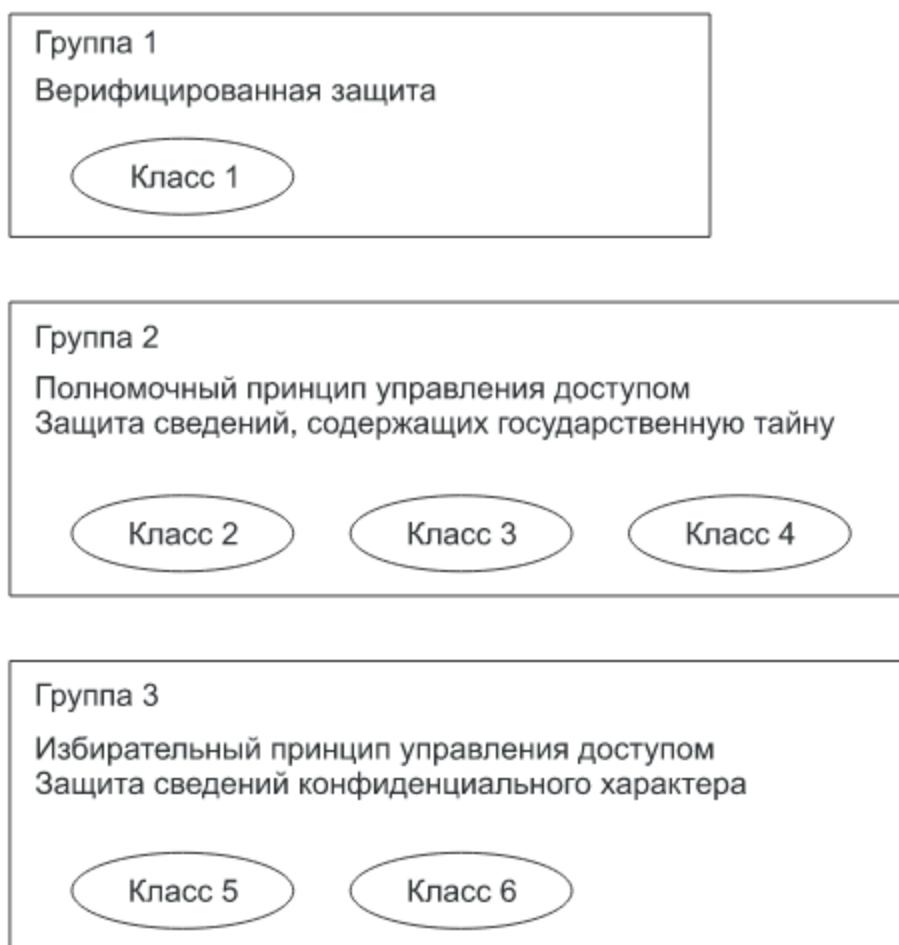


Рис. 2.1. Классы защищенности СВТ

2.5. Классификация автоматизированных систем и требования по защите информации

Руководящий документ Гостехкомиссии России от 30.03.1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливает классификацию АС, подлежащих защите от НСД к информации, и требования по защите информации в АС различных классов.

В целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации проводится классификация АС. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- ◆ наличие в АС информации различного уровня конфиденциальности;
- ◆ уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- ◆ режим обработки данных в АС – коллективный или индивидуальный.

Устанавливаются девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, различающиеся особенностями обработки информации в АС (рис. 2.2).

Группа 3 включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Группа 2 включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Группа 1 включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Комплекс программно-технических средств и организационных решений по защите информации от НСД реализуется в рамках системы, состоящей из следующих четырех подсистем:

- ◆ управления доступом;
- ◆ регистрации и учета;
- ◆ криптографической;
- ◆ обеспечения целостности.

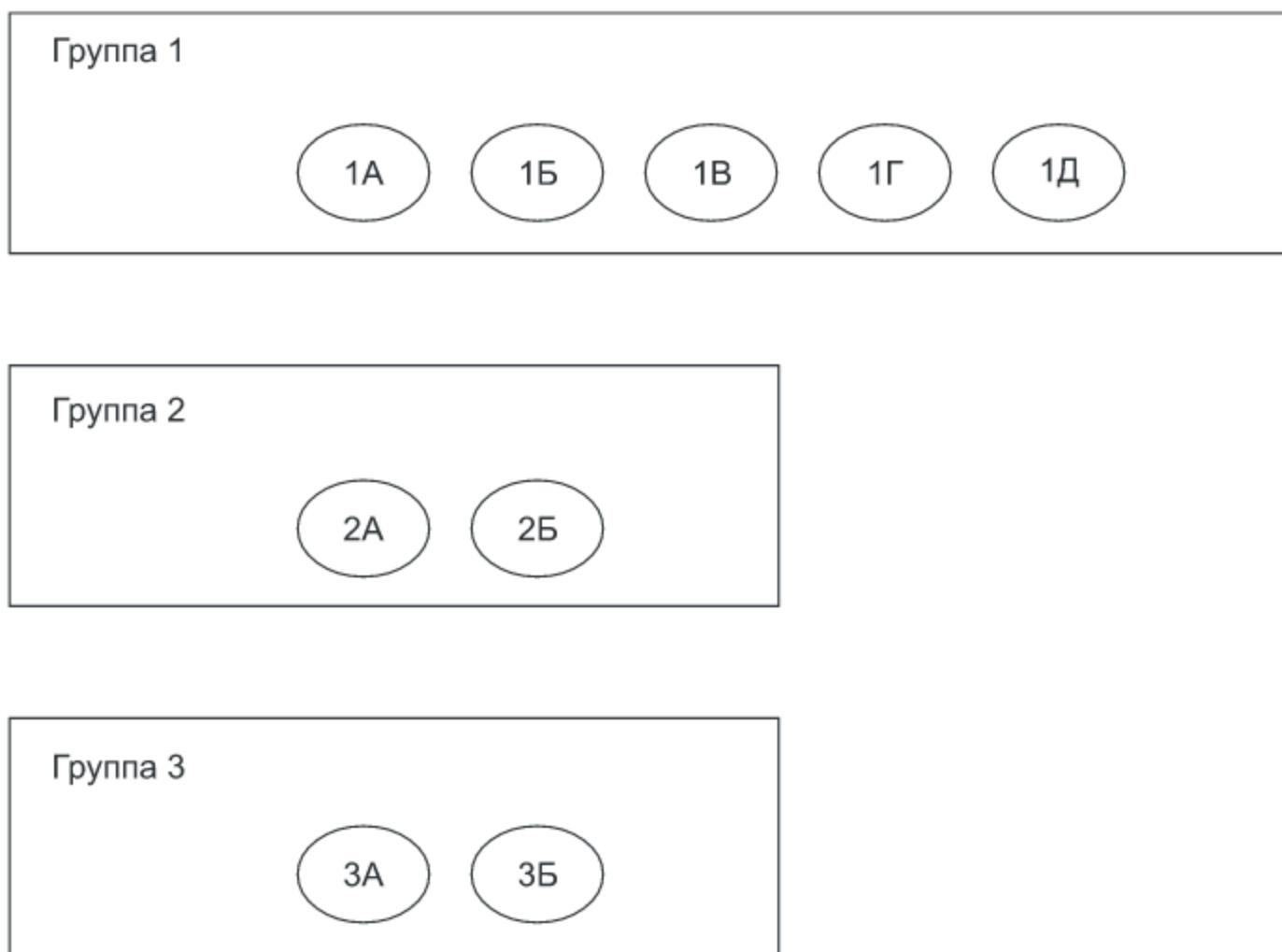


Рис. 2.2. Классы защищенности АС

Перечень конкретных требований для классов представлен в табл. 2.2.

При разработке АС, предназначенной для обработки или хранения информации, содержащей сведения, составляющие государственную тайну, необходимо ориентироваться на классы защищенности АС не ниже 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

- ◆ не ниже класса 4 – для АС класса 1В;
- ◆ не ниже класса 3 – для АС класса 1Б;
- ◆ не ниже класса 2 – для АС класса 1А.

С 01.10.2009 г. введен в действие стандарт ГОСТ Р ИСО/МЭК ТО 19791–2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

С 01.09.2014 г. введен в действие национальный стандарт ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Описания указанных стандартов приведены далее.

Таблица 2.2. Требования по защите информации для АС

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
<i>1. Подсистема управления доступом</i>									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
— в систему;	+	+	+	+	+	+	+	+	+
— к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+		+	+	+	+
— к программам;	-	-	-	+		+	+	+	+
— к томам, каталогам, файлам, записям, полям записей	-	-	-	+		+	+	+	+
1.2. Управление потоками информации	-	-	-	+			+	+	+
<i>2. Подсистема регистрации и учета</i>									
2.1. Регистрация и учет:									
— входа субъектов доступа в систему (выхода из системы) (узел сети);	+	+	+	+	+		+	+	+
— выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
— запуска (завершения) программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
— доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;	-	-	-	+	-	+	+	+	+
— доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
— изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
— создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4. Сигнализация о попытках нарушения защиты	-	-	-	-	-	-	+	+	+

Подсистемы и требования	Классы									
	ЗБ	ЗА	2Б	2А	1Д	1Г	1В	1Б	1А	
<i>3. Криптографическая подсистема</i>										
3.1. Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+	
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	-	-	-	-	+	
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+	
<i>4. Подсистема обеспечения целостности</i>										
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+	
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+	
4.3. Наличие администратора (службы) защиты информации в АС	-	-	-	+	-	-	+	+	+	
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+	
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+	
4.5. Наличие средств восстановления СЗИ НСД	-	+	-	+	-	-	+	+	+	

Кроме того, с 01.07.2015 г. введены в действие три национальных стандарта: ГОСТ Р 56115–2014, ГОСТ Р 56103–2014 и ГОСТ Р 56093–2014, которые посвящены средствам защиты автоматизированных систем в защищенном исполнении от преднамеренных силовых электромагнитных воздействий. Они устанавливают дополнительные требования и положения комплекса стандартов на автоматизированные системы в части создания и применения средств защиты автоматизированных систем в защищенном исполнении от преднамеренных силовых электромагнитных воздействий, которые могут привести к деструктивным последствиям.

2.6. Межсетевые экраны. Показатели защищенности от НСД

Руководящий документ Гостехкомиссии России от 25.07.1997 г. «Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию межсетевых экранов по уровню защищенности от НСД на базе перечня показателей защищенности и совокупности описывающих их требований.

В документе МЭ представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Устанавливаются пять классов защищенности МЭ (рис. 2.3). Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

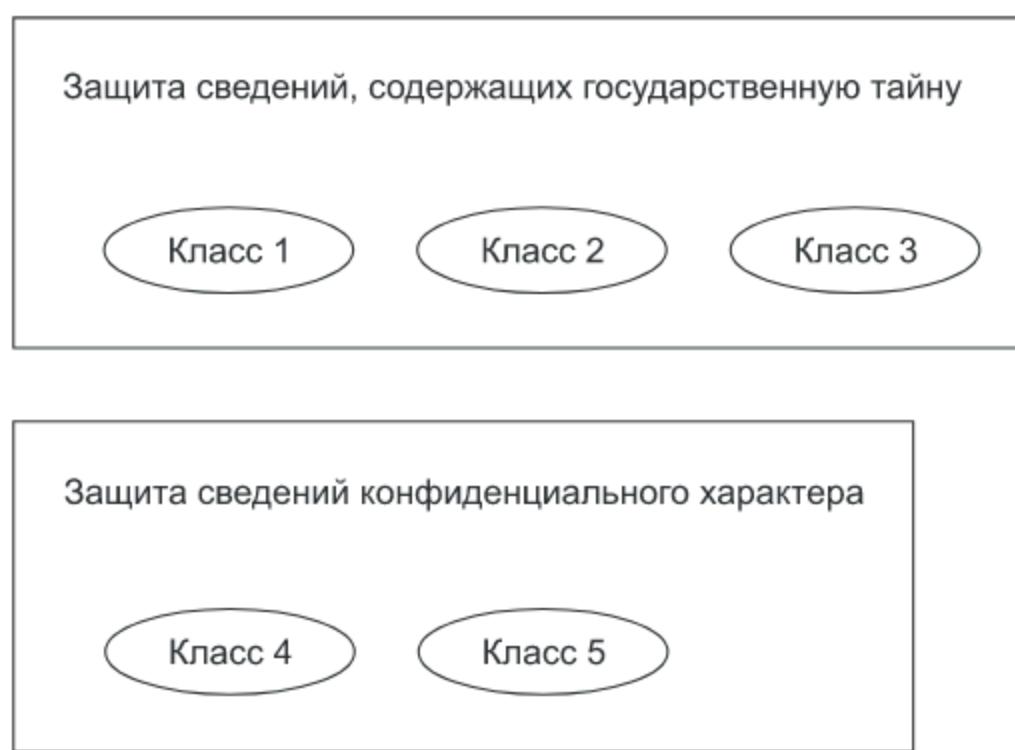


Рис. 2.3. Классы защищенности МЭ

Самый низкий класс защищенности – пятый, самый высокий – первый. Конкретные требования к показателям защищенности в зависимости от класса межсетевого экрана приведены в табл. 2.3.

Таблица 2.3. Показатели защищенности МЭ

Показатель защищенности	Класс защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование:					
— идентификация и аутентификация;	+	=	+	+	+
— регистрация;	+	+	+	=	=
— простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Для защиты информации, содержащей сведения, отнесенные к государственной тайне, должны использоваться МЭ 1–3-го классов защищенности.

Стандарт устанавливает следующее соответствие между классами АС и классами защищенности МЭ для безопасного взаимодействия с внешней средой (табл. 2.4).

Таблица 2.4. Соответствие классов АС и МЭ

Класс МЭ	Класс АС
1	1А, 2А, 3А с грифом «Особой важности»
2	1Б, 2А, 3А с грифом «Совершенно секретно»
3	1В, 2А, 3А с грифом «Секретно»
4	1Г
5	1Д, 2Б, 3Б

При включении межсетевого экрана в АС определенного класса защищенности класс защищенности совокупной АС, полученной из исходной путем добавления в нее данного межсетевого экрана, не должен понижаться.

2.7. Контроль отсутствия НДВ в программном обеспечении

Руководящий документ Гостехкомиссии России от 04.06.1999 г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» устанавливает классификацию отечественного и импортного программного обеспечения, предназначенного для защиты информации ограниченного доступа, в том числе встроенного в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Действие документа не распространяется на ПО средств криптографической защиты информации.

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия НДВ.

В документе дается определение ряду терминов.

Недекларированные возможности – функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Программные закладки – преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

Фактический маршрут выполнения функциональных объектов – последовательность фактически выполняемых функциональных объектов при определенных условиях (входных данных).

Критический маршрут выполнения функциональных объектов – маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов.

Статический анализ исходных текстов программ – совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ.

Динамический анализ исходных текстов программ – совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа.

Устанавливаются четыре уровня контроля отсутствия недекларированных возможностей (рис. 2.4). Перечень требований к уровням контроля представлен в табл. 2.5.



Рис. 2.4. Уровни контроля отсутствия НДВ

Для программного обеспечения, используемого при защите информации, отнесенной к государственной тайне, должен быть обеспечен уровень контроля не ниже третьего.

Самый высокий уровень контроля – первый – достаточен для программного обеспечения, используемого при защите информации с грифом «Особой важности».

Второй уровень контроля достаточен для программного обеспечения, используемого при защите информации с грифом «Совершенно секретно».

Третий уровень контроля достаточен для программного обеспечения, используемого при защите информации с грифом «Секретно».

Самый низкий уровень контроля – четвертый – достаточен для программного обеспечения, используемого при защите конфиденциальной информации.

Таблица 2.5. Требования к уровням контроля отсутствия НДВ

Наименование требования	Уровень контроля			
	4	3	2	1
<i>Требования к документации</i>				
1. Контроль состава и содержания документации				
1.1. Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2. Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3. Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4. Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
1.5. Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
<i>Требования к содержанию испытаний</i>				
2. Контроль исходного состояния ПО	+	=	=	=
3. Статический анализ исходных текстов программ				
3.1. Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3. Контроль связей функциональных объектов по управлению	-	+	=	=
3.4. Контроль связей функциональных объектов по информации	-	+	=	=
3.5. Контроль информационных объектов	-	+	=	=
3.6. Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
3.7. Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
3.8. Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
3.9. Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	-	-	+	=
4. Динамический анализ исходных текстов программ				
4.1. Контроль выполнения функциональных объектов	-	+	+	=
4.2. Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=
5. Отчетность	+	+	+	+

С 01.07.1999 г. введен в действие государственный стандарт ГОСТ Р 51188–98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство». Стандарт предназначен для применения в испытательных лабораториях, проводящих сертификационные испытания программных средств на выполнение требований защиты информации. Он распространяется на испытания ПС и их компонентов с целью обнаружить и устраниТЬ из них компьютерные вирусы и устанавливает общие требования к организации и проведению таких испытаний.

В стандарте дано описание термина «компьютерный вирус».

Компьютерный вирус — программа, способная создавать свои копии (не обязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Стандарт устанавливает типовые требования, предъявляемые к испытаниям ПС на наличие вирусов, в том числе:

- ◆ к составу мероприятий по подготовке и проведению испытаний;
- ◆ составу, структуре и назначению основных частей программино-аппаратного стенда, обеспечивающего проведение испытаний;
- ◆ выбору и использованию методов проведения испытаний;
- ◆ тестовым (антивирусным) программам, обнаруживающим и уничтожающим вирус;
- ◆ составу и содержанию документации, фиксирующей порядок проведения испытаний и их результаты.

К способам решения проблем защиты информации от недекларированных возможностей аппаратно-программных средств можно отнести еще два национальных стандарта Российской Федерации, посвященных защите от угроз ИБ с использованием скрытых каналов.

1. ГОСТ Р 53113.1–2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».
2. ГОСТ Р 53113.2–2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».

Более подробно эти стандарты будут рассмотрены далее.

2.8. Требования к защите персональных данных

В соответствии с законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» персональные данные отнесены к информации ограниченного доступа и в соответствии со степенью конфиденциальности подлежат соответствующей защите. Следует отметить, что с момента выхода этого закона до сегодняшнего дня нормативная база по защите персональных данных почти полностью изменилась. Многие нормативные документы регуляторов (ФСТЭК, ФСБ, Роскомнадзора и Правительства РФ) отменены, а взамен появились новые.

Постановлением Правительства РФ от 17.11.2007 г. № 781 было утверждено «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Во исполнение этого постановления в феврале 2008 г. ФСТЭК разработал следующие документы с грифом «ДСП».

1. Базовая модель угроз безопасности ПД при их обработке в информационных системах персональных данных.
2. Методика определения актуальных угроз безопасности ПД при их обработке в информационных системах персональных данных.
3. Основные мероприятия по организации и техническому обеспечению безопасности ПД при их обработке в информационных системах персональных данных.
4. Рекомендации по обеспечению безопасности ПД при их обработке в информационных системах персональных данных.

Гриф «ДСП» был снят в ноябре 2009 г., и документы были опубликованы на сайте ФСТЭК. Позже последние два документа были отменены.

Совместным приказом ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 г. № 55/86/20 утвержден «Порядок проведения классификации информационных систем ПД», согласно которому все ИСПДн в зависимости от степени конфиденциальности ПД и других параметров делились на четыре класса: К1, К2, К3, К4. Данный приказ также был отменен совместным приказом от 31.12.2013 г. № 151/786/461.

Приказом ФСТЭК от 05.02.2010 г. № 58 было утверждено «Положение о методах и способах защиты информации в информационных системах персональных данных», которое через три года было отменено приказом ФСТЭК от 18.02.2013 г. № 21.

Постановлением Правительства РФ от 01.11.2012 г. № 1119 были утверждены новые требования к защите ПД и отменено положение, принятое

постановлением № 781. Согласно новым требованиям введено понятие уровней защищенности ПД в ИСПДн (4 уровня).

К настоящему времени в сфере защиты персональных данных можно отметить следующие основные действующие нормативные документы.

1. Постановление Правительства РФ от 15.09.2008 г. № 687 «Положение об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации».
2. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. Постановление Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
4. Постановление Правительства РФ от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
5. Приказ ФСТЭК от 18.02.2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
7. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11.02.2014 г.
8. Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК 15.02.2008 г.

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК 14.02.2008 г.
11. Информационное сообщение ФСТЭК от 15.07.2013 г. № 240/22/2637 по вопросам защиты информации и обеспечения безопасности ПД при их обработке в информационных системах в связи с изданием приказов № 17 и № 21.

Кроме того, ФСТЭК разработал Банк данных угроз безопасности информации, который доступен на сайте службы. Целью создания и ведения Банка является повышение информированности заинтересованных лиц о существующих угрозах в информационных (автоматизированных) системах. Он содержит сведения об основных угрозах безопасности информации и уязвимостях, характерных в первую очередь для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов. Банк предназначен для заказчиков, операторов, разработчиков ИС (АС) и их систем защиты, разработчиков и производителей средств ЗИ, испытательных лабораторий и органов по сертификации средств защиты информации, а также иных заинтересованных организаций и лиц.

В мае 2015 г. ФСТЭК разработал проект документа «Методика определения угроз безопасности информации в информационных системах». Документ устанавливает единый методический подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в государственных информационных системах, защита информации в которых обеспечивается в соответствии с Требованиями, утвержденными приказом ФСТЭК России от 11.02.2013 г. № 17. По решению оператора персональных данных Методика может применяться для определения угроз безопасности ПД при их обработке в ИСПДн, защита которых обеспечивается в соответствии с приказом ФСТЭК России от 18.02.2013 г. № 21. На момент подготовки данного пособия Методика еще не была утверждена ФСТЭК.

Постановление Правительства РФ № 1119 устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных. Система защиты ПД включает в себя организационные и/или технические меры, определенные с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в ИС (на основании документов ФСТЭК).

Под актуальными угрозами безопасности ПД понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПД при их обработке в ИСПДн, результатом которого могут стать уничтожение, изменение, блокирование,

копирование, предоставление, распространение ПД, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для ИС, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИС.

Угрозы 2-го типа актуальны для ИС, если для нее в том числе актуальны угрозы, связанные с наличием НДВ в прикладном программном обеспечении, используемом в ИС.

Угрозы 3-го типа актуальны для ИС, если для нее актуальны угрозы, не связанные с наличием НДВ в системном и прикладном программном обеспечении, используемом в ИС.

При обработке ПД в информационных системах устанавливаются 4 уровня защищенности персональных данных (самый высокий – 1, самый низкий – 4).

Приказ ФСТЭК № 21 устанавливает состав и содержание организационных и технических мер по обеспечению безопасности ПД при их обработке в ИСПДн для каждого из уровней защищенности ПД (кроме ПД, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением криптографических средств защиты информации).

На основании информационного сообщения ФСТЭК № 240/22/2637 для выбора мер по обеспечению безопасности ПД при их обработке в государственных информационных системах достаточно руководствоваться требованиями, установленными приказом ФСТЭК № 17 с учетом методического документа ФСТЭК от 11.02.2014 г. «Меры защиты информации в государственных информационных системах», а также требованиями (в том числе в части определения уровня защищенности ПД), установленными постановлением № 1119. При этом должно быть обеспечено соотношение класса защищенности ГИС с уровнем защищенности ПД, приведенное в табл. 2.6.

Таблица 2.6. Соотношение класса защищенности ГИС и уровня защищенности ПД

Класс защищенности ГИС	Уровень защищенности ПД
1	1–4
2	2–4
3	3–4
4	4

В состав мер по обеспечению безопасности ПД с учетом актуальных угроз безопасности входят:

- ◆ идентификация и аутентификация субъектов доступа и объектов доступа;

- ◆ управление доступом субъектов доступа к объектам доступа;
- ◆ ограничение программной среды;
- ◆ защита машинных носителей информации, на которых хранятся и/или обрабатываются ПД;
- ◆ регистрация событий безопасности;
- ◆ антивирусная защита;
- ◆ обнаружение (предотвращение) вторжений;
- ◆ контроль (анализ) защищенности персональных данных;
- ◆ обеспечение целостности ИС и ПД;
- ◆ обеспечение доступности ПД;
- ◆ защита среды виртуализации;
- ◆ защита технических средств;
- ◆ защита ИС, ее средств, систем связи и передачи данных;
- ◆ выявление инцидентов, которые могут привести к сбоям или нарушению функционирования ИС и/или возникновению угроз безопасности ПД, и реагирование на них;
- ◆ управление конфигурацией ИС и системы защиты ПД.

Конкретный состав и содержание мер по обеспечению безопасности ПД определяется в зависимости от уровней защищенности ПД.

Для обеспечения 1-го и 2-го уровней защищенности ПД применяются:

- ◆ средства вычислительной техники не ниже 5-го класса;
- ◆ системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го класса;
- ◆ межсетевые экраны не ниже 3-го и 4-го классов.

Для обеспечения 3-го уровня защищенности ПД применяются:

- ◆ средства вычислительной техники не ниже 5-го класса;
- ◆ системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го и 5-го классов;
- ◆ межсетевые экраны не ниже 3-го и 4-го классов.

Для обеспечения 4-го уровня защищенности ПД применяются:

- ◆ средства вычислительной техники не ниже 6-го класса;
- ◆ системы обнаружения вторжений и средства антивирусной защиты не ниже 5-го класса;
- ◆ межсетевые экраны 5-го класса.

Для обеспечения 1–3-го уровней защищенности ПД применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4-му уровню контроля отсутствия НДВ.

2.9. Требования о защите информации в государственных информационных системах

Требования к обеспечению защиты информации ограниченного доступа (кроме государственной тайны), обрабатываемой в государственных информационных системах, утверждены приказом ФСТЭК России от 11.02.2013 г. № 17. Методический документ ФСТЭК России от 11.02.2014 г. «Меры защиты информации в государственных информационных системах» детализирует меры защиты информации, установленные приказом № 17.

Выбор мер защиты информации осуществляется, исходя из класса защищенности информационной системы. Устанавливаются четыре класса защищенности информационной системы: первый (К1), второй (К2), третий (К3), четвертый (К4), определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы. УЗ информации определяется степенью возможного ущерба от нарушения конфиденциальности, целостности или доступности информации. Степень возможного ущерба определяется обладателем информации или оператором самостоятельно и может быть высокой, средней, низкой и минимальной. В соответствии со степенью ущерба устанавливаются уровни значимости УЗ1, УЗ2, УЗ3, УЗ4.

Масштаб информационной системы определяется назначением и распределенностью сегментов информационной системы и может быть федеральным, региональным и объектовым.

Класс защищенности информационной системы определяется в соответствии с табл. 2.7.

Требования к системе защиты информации ИС определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации. Для определения угроз безопасности информации и разработки модели угроз безопасности применяются соответствующие методические документы ФСТЭК.

Таблица 2.7. Классы защищенности ИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	K1	K1	K1
УЗ 2	K1	K2	K2
УЗ 3	K2	K3	K3
УЗ 4	K3	K3	K4

Организационные и технические меры защиты информации, реализуемые в информационной системе, должны обеспечивать:

- ◆ идентификацию и аутентификацию субъектов и объектов доступа;
- ◆ управление доступом субъектов доступа к объектам доступа;
- ◆ ограничение программной среды;
- ◆ защиту машинных носителей информации;
- ◆ регистрацию событий безопасности;
- ◆ антивирусную защиту;
- ◆ обнаружение (предотвращение) вторжений;
- ◆ контроль (анализ) защищенности информации;
- ◆ целостность информационной системы и информации;
- ◆ доступность информации;
- ◆ защиту среды виртуализации;
- ◆ защиту технических средств;
- ◆ защиту ИС, ее средств, систем связи и передачи данных.

Внедрение системы защиты информации ИС включает:

- ◆ установку и настройку средств защиты информации в ИС;
- ◆ разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИС;
- ◆ внедрение организационных мер защиты информации;
- ◆ предварительные испытания системы защиты информации ИС;
- ◆ опытную эксплуатацию системы защиты информации;
- ◆ анализ уязвимостей ИС и принятие мер защиты информации по их устраниению;
- ◆ приемочные испытания системы защиты информации.

Аттестация ИС организуется обладателем информации или оператором и включает комплекс организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации информационной системы Требованиям.

Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и, в частности, включает:

- ◆ управление системой защиты информации ИС;
- ◆ выявление инцидентов и реагирование на них;
- ◆ управление конфигурацией аттестованной ИС;
- ◆ мониторинг обеспечения уровня защищенности информации.

Выбор мер защиты информации для их реализации в ИС включает:

- ◆ определение базового набора мер защиты для установленного класса защищенности ИС;
- ◆ адаптацию базового набора мер защиты применительно к структурно-функциональным характеристикам ИС, информационным технологиям, особенностям функционирования ИС;
- ◆ уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты;
- ◆ дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности.

Общий порядок действий по выбору мер защиты информации изображен на рис. 2.5 таким, каким он представлен в документах ФСТЭК.

В информационных системах К1 и К2 применяются:

- ◆ СВТ не ниже 5-го класса;
- ◆ системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го класса;
- ◆ межсетевые экраны не ниже 3-го класса (в случае взаимодействия ИС с сетями международного информационного обмена) либо 4-го класса.

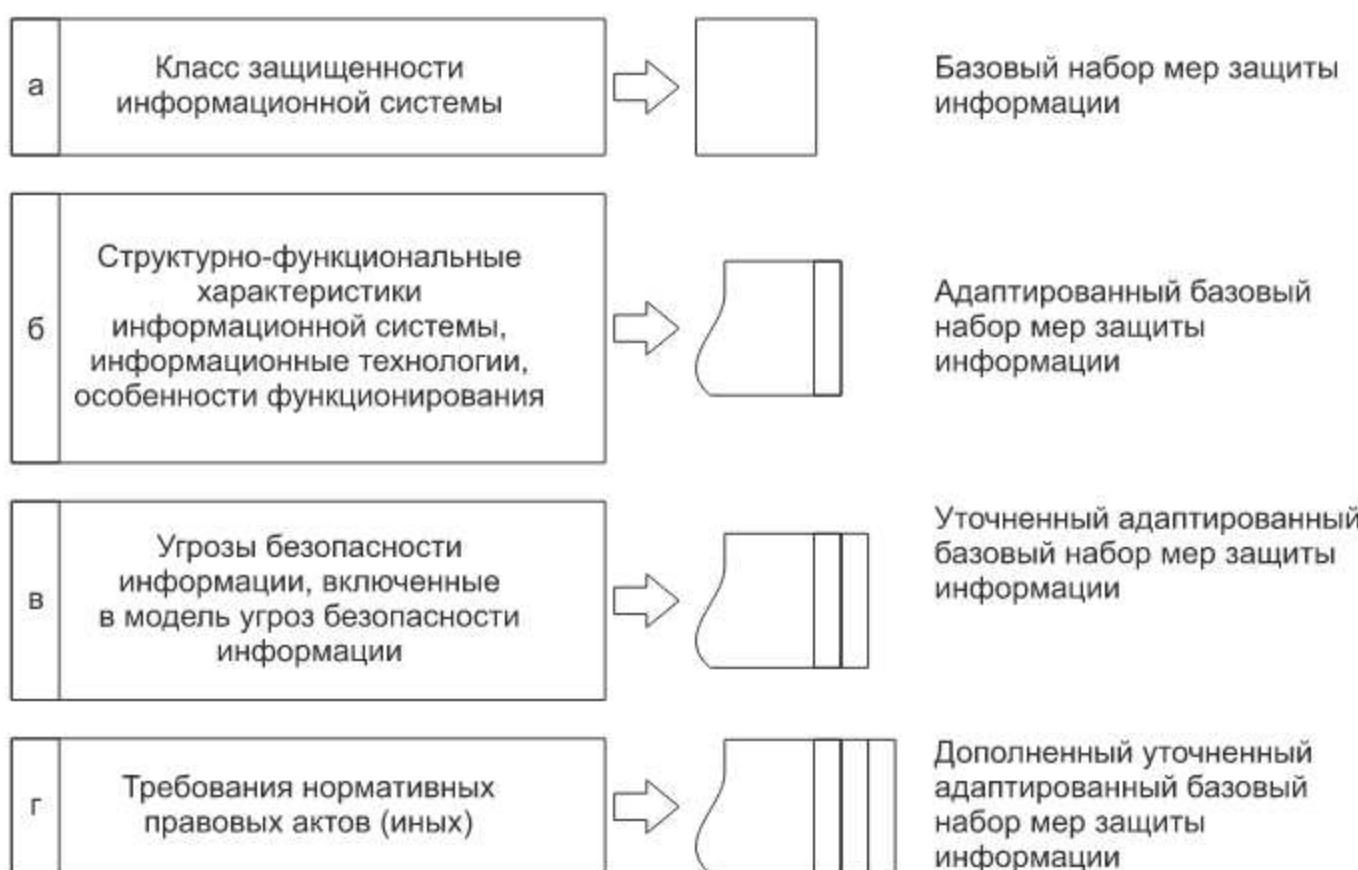


Рис. 2.5. Порядок действий по выбору мер защиты в ГИС

В информационных системах К3 применяются:

- ◆ СВТ не ниже 5-го класса;
- ◆ СОВ и САВЗ 4-го класса (в случае взаимодействия ИС с сетями международного информационного обмена) либо не ниже 5-го класса;
- ◆ межсетевые экраны не ниже 3-го класса (в случае взаимодействия ИС с сетями международного информационного обмена) либо 4-го класса.

В информационных системах 4-го класса защищенности применяются:

- ◆ СВТ не ниже 5-го класса;
- ◆ СОВ и САВЗ не ниже 5-го класса;
- ◆ межсетевые экраны не ниже 4-го класса.

В информационных системах 1-го и 2-го классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4-му уровню контроля отсутствия недекларированных возможностей.

В случае обработки в информационной системе информации, содержащей персональные данные:

- ◆ для ИС К1 обеспечивают 1–4-й уровни защищенности ПД;
- ◆ для ИС К2 обеспечивают 2–4-й уровни защищенности ПД;

- ◆ для ИС К3 обеспечивают 3-й и 4-й уровни защищенности ПД;
- ◆ для ИС К4 обеспечивают 4-й уровень защищенности ПД.

2.10. Требования о защите информации в ИС общего пользования

Совместным приказом ФСБ России и ФСТЭК России от 31.08.2010 г. № 416/489 «О защите информации, содержащейся в информационных системах общего пользования» утверждены требования, которые распространяются на федеральные ГИС, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в сети Интернет.

Требования являются обязательными для операторов ИС общего пользования при разработке и эксплуатации таких систем.

ИС ОП должны обеспечивать:

- ◆ сохранность и неизменность обрабатываемой информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения (целостность информации);
- ◆ беспрепятственный доступ пользователей к содержащейся в ИС ОП информации (доступность информации);
- ◆ защиту от действий пользователей в отношении информации, не предусмотренных правилами пользования ИС ОП, приводящих в том числе к уничтожению, модификации и блокированию информации (неправомерные действия).

Информация, содержащаяся в ИС ОП, является общедоступной.

ИС ОП в зависимости от значимости содержащейся в них информации и требований к ее защите разделяются на два класса.

К I классу относятся ИС ОП Правительства Российской Федерации и иные ИС ОП в случае, если нарушение целостности и доступности информации, содержащейся в них, может привести к возникновению угроз безопасности Российской Федерации. Отнесение ИС ОП к I классу выполняется по решению руководителя соответствующего федерального органа исполнительной власти.

Ко II классу относятся ИС ОП, не относящиеся к классу I.

Размещение ИС ОП и охрана помещений, в которых находятся технические средства, организация режима обеспечения безопасности в этих помещениях

должны обеспечивать сохранность носителей информации и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Защиту информации в ИС ОП обеспечивает оператор ИС, который назначает структурное подразделение или должностное лицо, ответственное за обеспечение защиты информации.

В ИС ОП должны быть обеспечены:

- ◆ поддержание целостности и доступности информации;
- ◆ предупреждение возможных неблагоприятных последствий нарушения порядка доступа к информации;
- ◆ проведение мероприятий, направленных на предотвращение неправомерных действий в отношении информации;
- ◆ своевременное обнаружение фактов неправомерных действий в отношении информации;
- ◆ недопущение воздействия на технические средства ИС ОП, в результате которого может быть нарушено их функционирование;
- ◆ возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий;
- ◆ проведение мероприятий по постоянному контролю за обеспечением их защищенности;
- ◆ возможность записи и хранения сетевого трафика.

Мероприятия по обеспечению защиты информации в ИС ОП включают в себя:

- ◆ определение угроз безопасности информации, формирование на их основе модели угроз;
- ◆ разработку на основе модели угроз системы ЗИ, обеспечивающейнейтрализацию предполагаемых угроз с использованием методов и способов ЗИ, предусмотренных для соответствующего класса ИС ОП;
- ◆ проверку готовности средств ЗИ к использованию с составлением заключений о возможности их эксплуатации;
- ◆ установку и ввод в эксплуатацию средств ЗИ в соответствии с эксплуатационной и технической документацией;
- ◆ обучение лиц, использующих средства ЗИ, применяемые в ИС ОП, правилам работы с ними;
- ◆ учет применяемых средств ЗИ, эксплуатационной и технической документации к ним;

- ◆ контроль за соблюдением условий использования средств ЗИ, предусмотренных эксплуатационной и технической документацией;
- ◆ проведение разбирательств и составление заключений по фактам несоблюдения условий использования средств ЗИ, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности ИС ОП, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- ◆ описание системы их защиты.

Запросы пользователей на получение информации, содержащейся в ИС ОП, а также факты предоставления информации по этим запросам регистрируются автоматизированными средствами ИС ОП в электронном журнале обращений.

Требования по защите информации в ИС ОП I класса:

- ◆ Использование средств ЗИ от неправомерных действий, в том числе средств криптографической ЗИ, сертифицированных ФСБ России.
- ◆ Использование средств обнаружения вредоносного программного обеспечения, в том числе антивирусных средств, сертифицированных ФСБ России.
- ◆ Использование средств контроля доступа к информации, в том числе средств обнаружения компьютерных атак, сертифицированных ФСБ России.
- ◆ Использование средств фильтрации и блокирования сетевого трафика, в том числе средств межсетевого экранирования, сертифицированных ФСБ России.
- ◆ Локализация и ликвидация неблагоприятных последствий нарушения порядка доступа к информации.
- ◆ Запись и хранение сетевого трафика при обращении к государственным информационным ресурсам за 10 и более последних дней и предоставление доступа к записям по запросам уполномоченных государственных органов, осуществляющих оперативно-розыскную деятельность.
- ◆ Обеспечение защиты от воздействий на технические и программные средства ИС ОП, в результате которых нарушается их функционирование, и несанкционированного доступа в помещения, в которых находятся данные средства, с использованием технических средств охраны, в том числе систем видеонаблюдения, предотвращающих проникновение в помещения посторонних лиц.
- ◆ Регистрация действий обслуживающего персонала и пользователей.

- ◆ Обеспечение резервирования технических и программных средств, дублирования носителей и массивов информации.
- ◆ Использование сертифицированных в установленном порядке систем обеспечения гарантированного электропитания (источников бесперебойного питания).
- ◆ Мониторинг защищенности уполномоченным подразделением ФСБ России.
- ◆ Введение в эксплуатацию только после направления оператором ИС ОП в ФСБ России уведомления о готовности ввода ИС ОП в эксплуатацию и ее соответствии Требованиям.

Требования по защите информации в ИС ОП II класса:

- ◆ Использование средств ЗИ от неправомерных действий, сертифицированных ФСБ России и/или ФСТЭК России с учетом их компетенции, в том числе средств криптографической ЗИ.
- ◆ Использование средств обнаружения вредоносного ПО, в том числе антивирусных средств, сертифицированных ФСБ России и/или ФСТЭК России с учетом их компетенции.
- ◆ Использование средств контроля доступа к информации, в том числе средств обнаружения компьютерных атак, сертифицированных ФСБ России и/или ФСТЭК России с учетом их компетенции.
- ◆ Использование средств фильтрации и блокирования сетевого трафика, в том числе средств межсетевого экранирования, сертифицированных ФСБ России и/или ФСТЭК России с учетом их компетенции.
- ◆ Локализация и ликвидация неблагоприятных последствий нарушения порядка доступа к информации.
- ◆ Запись и хранение сетевого трафика при обращении к государственным информационным ресурсам за последние сутки и более и предоставление доступа к записям по запросам уполномоченных государственных органов, осуществляющих оперативно-розыскную деятельность.
- ◆ Обеспечение защиты от воздействий на технические и программные средства ИС ОП, в результате которых нарушается их функционирование, и несанкционированного доступа в помещения, в которых находятся данные средства.
- ◆ Регистрация действий обслуживающего персонала.
- ◆ Обеспечение частичного резервирования технических средств и дублирования массивов информации.

- ◆ Использование систем обеспечения гарантированного электропитания (источников бесперебойного питания).
- ◆ Мониторинг защищенности уполномоченным подразделением ФСБ России.
- ◆ Введение в эксплуатацию только после направления оператором ИС ОП в ФСТЭК России уведомления о готовности ввода ИС ОП в эксплуатацию и ее соответствии Требованиям.

Одно из принципиальных различий в требованиях по защите информации в ИС ОП I и II класса заключается в том, что сертификация СЗИ для систем I класса осуществляется только органами ФСБ, а для класса II может осуществляться органами ФСТЭК или ФСБ (кроме криптографических СЗИ, которые сертифицируются только ФСБ).

2.11. Требования к обеспечению защиты информации в АСУ ТП

Одним из путей предотвращения угроз информационной безопасности Российской Федерации в соответствии со Стратегией национальной безопасности Российской Федерации до 2020 г. (утверждена Указом Президента Российской Федерации от 12.05.2009 г. № 537) является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации.

Указом Президента Российской Федерации от 03.02.2012 г. № 803 утверждены «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», в которых предусматривалась разработка соответствующих нормативных правовых актов. В плане исполнения этого Указа приказом ФСТЭК России от 14.03.2014 г. № 31 утверждены «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

В документе устанавливаются требования к обеспечению ЗИ, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей

природной среды, от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.

В автоматизированной системе управления объектами защиты являются:

- ◆ информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);
- ◆ программно-технический комплекс, включающий технические средства, программное обеспечение, а также средства защиты информации.

Принимаемые организационные и технические меры ЗИ:

- ◆ должны обеспечивать доступность обрабатываемой в АСУ ТП информации, ее целостность, а также, при необходимости, конфиденциальность;
- ◆ должны соотноситься с мерами по обеспечению промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы управления и управляемого объекта и/или процесса;
- ◆ не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

В АСУ ТП применяются средства защиты информации, прошедшие оценку соответствия согласно законодательству Российской Федерации о техническом регулировании.

Формирование требований к ЗИ в АСУ ТП осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» и, в частности, включает:

- ◆ принятие решения о необходимости защиты информации;
- ◆ классификацию АСУ ТП;
- ◆ определение угроз безопасности информации и разработку на их основе модели угроз безопасности информации;
- ◆ определение требований к системе защиты АСУ ТП.

Устанавливаются три класса защищенности автоматизированной системы управления (К1, К2, К3), которые определяются в зависимости от уровня

значимости (критичности) обрабатываемой в ней информации. Самый низкий класс – третий, самый высокий – первый.

Уровень значимости (критичности) информации определяется степенью возможного ущерба от нарушения ее целостности, доступности или конфиденциальности, определяется заказчиком или оператором экспертным или иным методом и может быть высоким (УЗ1), средним (УЗ2) и низким (УЗ3). Класс К1 соответствует УЗ1, К2 – УЗ2, К3 – УЗ3.

Организационные и технические меры ЗИ в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик АСУ ТП и особенностей ее функционирования должны обеспечивать:

- ◆ идентификацию и аутентификацию субъектов и объектов доступа;
- ◆ управление доступом субъектов доступа к объектам доступа;
- ◆ ограничение программной среды;
- ◆ защиту машинных носителей информации;
- ◆ регистрацию событий безопасности;
- ◆ антивирусную защиту;
- ◆ обнаружение (предотвращение) вторжений;
- ◆ контроль (анализ) защищенности информации;
- ◆ целостность АСУ ТП и информации;
- ◆ доступность технических средств и информации;
- ◆ защиту среды виртуализации;
- ◆ защиту технических средств и оборудования;
- ◆ защиту автоматизированной системы и ее компонентов;
- ◆ безопасную разработку прикладного и специального ПО;
- ◆ управление обновлениями ПО;
- ◆ планирование мероприятий по обеспечению защиты информации;
- ◆ обеспечение действий в нештатных (непредвиденных) ситуациях;
- ◆ информирование и обучение персонала;
- ◆ анализ угроз безопасности информации и рисков от их реализации;
- ◆ выявление инцидентов и реагирование на них (управление инцидентами);
- ◆ управление конфигурацией АСУ ТП и ее системы защиты.

Внедрение системы защиты АСУ ТП осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации и, в частности, включает:

- ◆ настройку программного обеспечения АСУ ТП;
- ◆ разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в АСУ ТП в ходе ее эксплуатации;
- ◆ внедрение организационных мер защиты информации;
- ◆ установку и настройку средств защиты информации;
- ◆ предварительные испытания системы защиты;
- ◆ опытную эксплуатацию системы защиты;
- ◆ анализ уязвимостей и принятие мер по их устраниению;
- ◆ приемочные испытания системы защиты.

Обеспечение защиты информации в ходе эксплуатации АСУ ТП включает следующие процедуры:

- ◆ планирование мероприятий по обеспечению защиты информации;
- ◆ обеспечение действий в нештатных ситуациях в ходе эксплуатации АСУ ТП;
- ◆ информирование и обучение персонала;
- ◆ периодический анализ угроз безопасности информации и рисков от их реализации;
- ◆ управление (администрирование) системой защиты;
- ◆ выявление инцидентов в ходе эксплуатации АСУ ТП и реагирование на них;
- ◆ управление конфигурацией АСУ ТП и ее системы защиты;
- ◆ мониторинг обеспечения уровня защищенности АСУ ТП.

Выбор мер защиты информации для их реализации в АСУ ТП в рамках ее системы защиты включает:

- ◆ определение базового набора мер ЗИ для установленного класса защищенности;
- ◆ адаптацию базового набора мер ЗИ применительно к каждому уровню АСУ ТП, иным структурно-функциональным характеристикам и особенностям функционирования;
- ◆ уточнение адаптированного базового набора мер ЗИ с учетом не выбранных ранее мер защиты информации;

- ◆ дополнение уточненного адаптированного базового набора мер ЗИ мерами, обеспечивающими выполнение требований к ЗИ, установленными иными нормативными правовыми актами, локальными правовыми актами, национальными стандартами и стандартами организации в области ЗИ.

В случае использования в АСУ ТП сертифицированных по требованиям безопасности информации средств ЗИ применяются:

- ◆ в АСУ ТП 1-го класса защищенности (К1):
 - СВТ не ниже 5-го класса;
 - СОВ, САВЗ, средства доверенной загрузки и средства контроля съемных носителей информации не ниже 3-го класса;
 - межсетевые экраны не ниже 3-го класса в случае взаимодействия автоматизированной системы управления с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4-го класса в случае отсутствия такого взаимодействия;
- ◆ в АСУ ТП 2-го класса защищенности (К2):
 - СВТ не ниже 5-го класса;
 - СОВ, САВЗ, средства доверенной загрузки и средства контроля съемных носителей информации не ниже 4-го класса;
 - межсетевые экраны не ниже 3-го класса в случае взаимодействия автоматизированной системы управления с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4-го класса в случае отсутствия такого взаимодействия;
- ◆ в АСУ ТП 3-го класса защищенности (К3):
 - СВТ не ниже 5-го класса;
 - СОВ, САВЗ, средства доверенной загрузки и средства контроля съемных носителей информации не ниже 5-го класса;
 - межсетевые экраны не ниже 4-го класса.

В случае использования сертифицированных средств защиты информации в АСУ ТП 1-го и 2-го классов защищенности применяются средства защиты информации, ПО которых прошло проверку не ниже чем по 4-му уровню контроля отсутствия НДВ.

2.12. Новое поколение нормативных документов ФСТЭК

2.12.1. Общие замечания

До 2002 г. единственными нормативными документами по критериям оценки защищенности средств вычислительной техники и автоматизированных систем являлись рассмотренные ранее в данной главе руководящие и нормативно-технические документы Гостехкомиссии (ФСТЭК) России.

В 2002 г. в России был принят новый национальный стандарт, состоящий из трех частей, под общим наименованием ГОСТ Р ИСО/МЭК 15408–2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Стандарт содержал полный аутентичный текст международного стандарта ISO/IEC 15408:1999, известного как «Общие критерии».

Стандарт стал качественно новой основой при оценке безопасности продуктов и систем информационных технологий и положил начало этапу в разработке нового поколения нормативных документов в системе сертификации ФСТЭК России на основе методологии, описанной в национальном стандарте ГОСТ Р ИСО/МЭК 15408.

В июне 2002 г. Гостехкомиссией разработаны руководящие документы (три части под общим названием «Критерии оценки безопасности информационных технологий») в развитие серии документов по защите информации от несанкционированного доступа. Данные РД направлены на обеспечение практического использования нового стандарта в деятельности заказчиков, разработчиков, пользователей продуктов и систем ИТ, а также органов сертификации и испытательных лабораторий, для использования при проведении оценки и сертификации безопасности ИТ. Эти документы практически полностью идентичны стандарту ИСО/МЭК 15408 в его редакции от 2002 г.

В 2003 г. на основе «Общих критериев» Гостехкомиссия утвердила ряд методических документов:

- ◆ Руководство по разработке профилей защиты и заданий по безопасности;
- ◆ Положение по разработке профилей защиты и заданий по безопасности;
- ◆ Руководство по формированию семейств профилей защиты;
- ◆ Руководство по регистрации профилей защиты.

На основе «Общих критериев» в последние годы в России уже разработан ряд методических и нормативных документов ФСТЭК, а также национальных стандартов в области защиты информации.

В настоящее время ФСТЭК России разработал нормативные документы, касающиеся требований к системам обнаружения вторжений, средствам антивирусной защиты, средствам контроля съемных машинных носителей, средствам доверенной загрузки, а также методические документы по соответствующим им профилям защиты. Ожидается, что в ближайшее время на базе «Общих критериев» будут разработаны и другие документы ФСТЭК.

Для каждого из основных классов средств ЗИ будет разработан документ, классифицирующий данный вид средств защиты и определяющий требования к соответствующему семейству профилей защиты. В свою очередь, профили защиты должны служить основанием для разработки заданий по безопасности, на соответствие которым и будет сертифицироваться конечный продукт.

2.12.2. Пакет документов по профилям защиты

Пакет общих руководящих и методических документов Гостехкомиссии России, определяющих порядок разработки, оценки и регистрации профилей защиты и заданий по безопасности, включает в себя следующие документы.

1. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г.
2. Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г.
3. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003 г.
4. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 г.

Кроме указанных документов в России был принят национальный стандарт ГОСТ Р ИСО/МЭК ТО 15446–2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».

Документы предназначены для использования заказчиками и разработчиками профилей защиты, разработчиками и пользователями продуктов и систем информационных технологий, а также органами по сертификации и испытательными лабораториями при выполнении ими работ по обязательной сертификации средств защиты информации.

В документах используются следующие термины:

Активы – информация или ресурсы, подлежащие защите контрмерами изделия ИТ.

Доверие – основание для уверенности в том, что изделие ИТ отвечает своим целям безопасности.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия ИТ.

Профиль защиты – независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.

Оценка безопасности – исследования (испытания), проводимые для проверки соответствия ПЗ, ЗБ или изделия ИТ установленным требованиям безопасности.

Политика безопасности организации – совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Среда безопасности – область среды, в пределах которой предусматривается обеспечение необходимых условий для поддержания требуемого режима безопасности изделия ИТ.

По сути профиль защиты является нормативным документом, предназначенный для изложения проблемы безопасности определенной совокупности продуктов и систем ИТ и формулирования требований безопасности для решения данной проблемы. Разработчиком ПЗ может быть любое юридическое или физическое лицо.

Профиль защиты не регламентирует, каким образом данные требования будут выполнены. Он разрабатывается для определения типового набора требований безопасности, которым должны удовлетворять один или более продуктов или которым должны удовлетворять системы ИТ, предназначенные для использования в определенных целях.

Задание по безопасности является документом, содержащим требования безопасности для конкретного изделия ИТ, которые реализованы в нем для достижения установленных целей безопасности.

Требования безопасности, включаемые в ЗБ, могут быть определены ссылками на профили защиты, на отдельные стандартизованные требования, а также могут содержать требования в явном виде. Помимо требований безопасности в ЗБ включаются краткая спецификация изделия ИТ и необходимые обоснования и пояснения.

Одной из целей разработки ЗБ является демонстрация того, как изделие ИТ удовлетворяет потребностям безопасности, сформулированным в ПЗ.

Тем не менее соответствие задания по безопасности профилю защиты не является обязательным. В ЗБ могут быть определены функции безопасности, заявляемые разработчиком продукта ИТ вне зависимости от того, имеется ли на данный момент ПЗ на соответствующий тип изделий ИТ. ЗБ является основой для проведения оценки безопасности изделия ИТ.

Структура и общие требования к содержанию ПЗ и ЗБ, а также порядок оценки, сертификации и регистрации ПЗ определены названным Положением.

Профиль защиты должен содержать:

- ◆ описание потребностей пользователей изделия ИТ в обеспечении безопасности;
- ◆ описание среды безопасности изделия ИТ;
- ◆ цели безопасности изделия ИТ. Посредством целей безопасности следует показать, что должно быть сделано для решения проблемы безопасности, определенной для изделия ИТ;
- ◆ функциональные требования безопасности и требования доверия к безопасности, которые направлены на решение проблемы безопасности в соответствии с описанием среды безопасности и целями безопасности для изделия ИТ. Функциональные требования безопасности выражают то, что должно выполняться изделием ИТ и его средой для удовлетворения целей безопасности. Требования доверия к безопасности определяют степень уверенности в правильности реализации функций безопасности изделия ИТ. Функциональные требования безопасности и требования доверия к безопасности должны обеспечивать достижение целей безопасности;
- ◆ обоснование, показывающее, что функциональные требования и требования доверия к безопасности являются достаточными для удовлетворения сформулированных потребностей пользователей изделия ИТ в его безопасности.

Требования безопасности профилей защиты определяются классом защищенности изделия ИТ.

Оценка ПЗ осуществляется испытательными лабораториями согласно критериям оценки ПЗ, содержащимся в третьей части РД Гостехкомиссии России «Критерии оценки безопасности информационных технологий». При соответствии результатов испытаний требованиям нормативных документов орган сертификации оформляет отчет о сертификации и выдает сертификат соответствия.

После завершения разработки проекта ПЗ подается заявка на его регистрацию в орган регистрации профилей защиты в соответствии с РД

Гостехкомиссии России «Руководство по регистрации профилей защиты». При положительном результате проверки ПЗ включается в реестр профилей защиты. Орган регистрации обеспечивает ведение реестра профилей защиты и его публикацию.

2.12.3. Требования к средствам антивирусной защиты

Приказом ФСТЭК России от 20.03.2012 г. № 28 утверждены «Требования к средствам антивирусной защиты», которые вступили в действие 01.08.2012 г.

Под средствами антивирусной защиты понимаются программные средства, используемые в целях обеспечения защиты информации и реализующие функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ЗИ (вредоносные компьютерные программы, компьютерные вирусы), а также реагирования на обнаружение этих программ и информации.

Требования к САВЗ применяются к программным средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, а также иной информации с ограниченным доступом.

Требования предназначены для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств ЗИ, заявителей на осуществление сертификации продукции, а также испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств ЗИ на соответствие обязательным требованиям безопасности информации.

Таким образом, с 01.08.2012 г. сертификация средств защиты информации, реализующих функции антивирусной защиты, в системе сертификации ФСТЭК России проводится на соответствие Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК № 28.

Выполнение Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, применяемых для формирования государственных информационных ресурсов.

Установлены шесть классов защиты средств антивирусной защиты. Самый низкий класс – шестой, самый высокий – первый.

САВЗ, соответствующие 3, 2 и 1-му классам защиты, применяются в ИС, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Требования определяют также соответствие между классами САВЗ и классами ИС персональных данных. САВЗ 6-го класса применяются в ИСПДн 3-го и 4-го классов, САВЗ 5-го класса – в ИСПДн 2-го класса, САВЗ 4-го класса – в ИСПДн 1-го класса. Причем класс ИСПДн в Требованиях соответствует классу, определенному по совместному приказу ФСБ, ФСТЭК, Мининформсвязи от 13.02.2008 г. № 55/86/20. В приказе ФСТЭК № 21 от 18.02.2013 г. устанавливается несколько другое соответствие между классом САВЗ и уровнем защищенности персональных данных в ИСПДн, который определяется в соответствии с Постановлением Правительства РФ от 01.11.2012 г. № 1119. В связи с тем, что приказ ФСТЭК № 21 вышел позже Требований (20.03.2012 г.), видимо, следует руководствоваться приказом № 21.

В Требованиях также выделяются следующие типы средств антивирусной защиты:

- ◆ «А» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для централизованного администрирования, установленные на компонентах информационных систем (серверах, автоматизированных рабочих местах);
- ◆ «Б» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на серверах информационных систем;
- ◆ «В» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автоматизированных рабочих местах информационных систем;
- ◆ «Г» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автономных автоматизированных рабочих местах.

Средства антивирусной защиты типа «А» не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и/или «В».

Требования к средствам антивирусной защиты включают общие требования к средствам антивирусной защиты и требования к функциям безопасности САВЗ.

Детализация требований к функциям безопасности, а также взаимосвязи этих требований для каждого класса и типа САВЗ приведены в профилях

защиты, утвержденных ФСТЭК России 14.06.2012 г. в качестве методических документов.

Методические документы ФСТЭК России, содержащие профили защиты САВЗ 4–6-го классов защиты, размещены на официальном сайте ФСТЭК России www.fstec.ru.

Классификация САВЗ представлена на рис. 2.6.

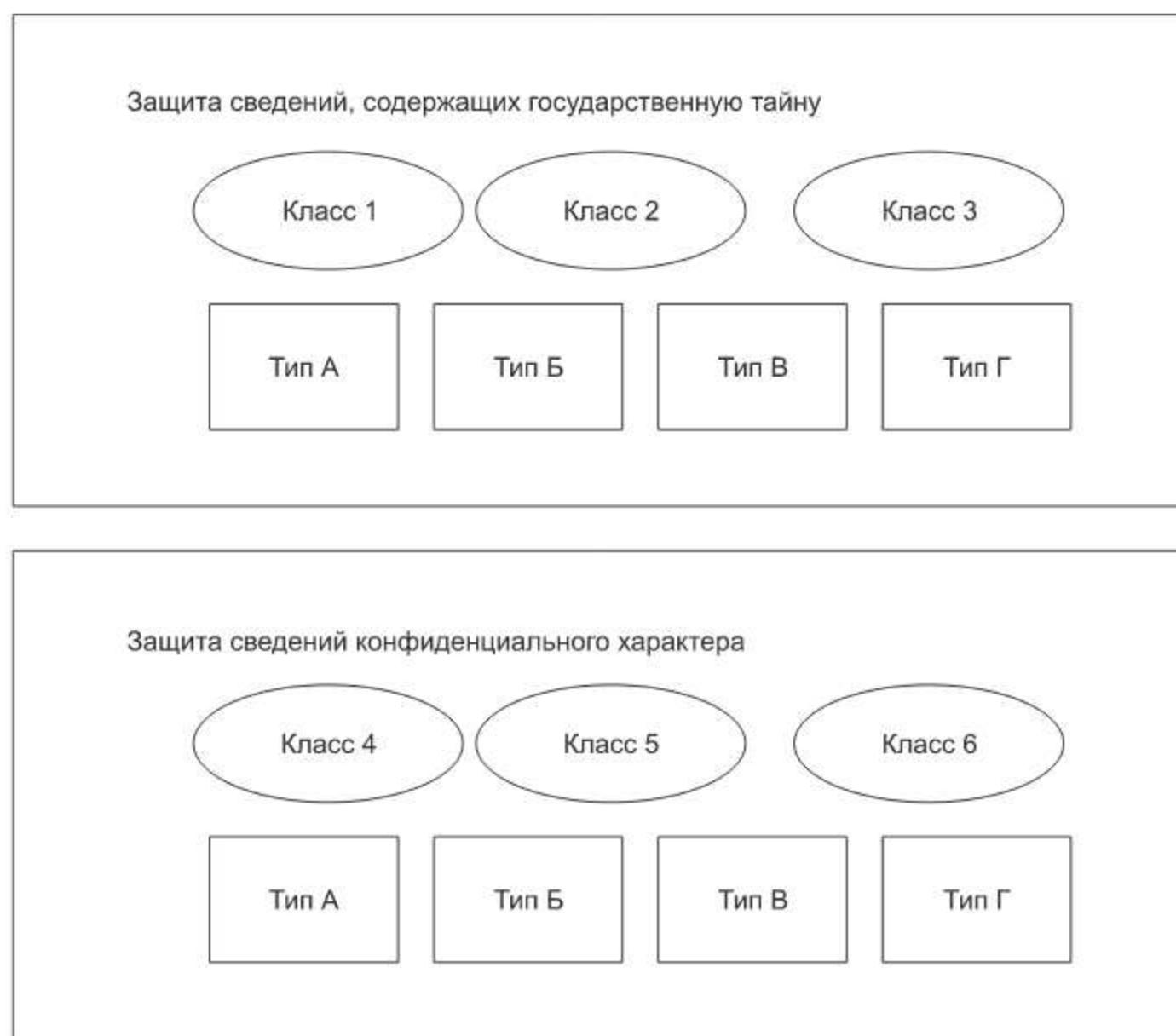


Рис. 2.6. Классификация САВЗ

Требования к САВЗ, а также методические документы ФСТЭК России, содержащие профили защиты средств антивирусной защиты 1–3-го классов защиты, имеют гриф «Ограниченный доступ», получить их можно в соответствии с Временным порядком обеспечения органов государственной власти Российской Федерации, органов местного самоуправления и организаций документами ФСТЭК России.

Например, ФСТЭК России 14.06.2012 г. утвердил методический документ «Профиль защиты средств антивирусной защиты типа «В» четвертого класса защиты».

Название ПЗ: Профиль защиты средств антивирусной защиты типа «В» четвертого класса защиты.

Тип САВЗ: САВЗ типа «В».

Класс защиты САВЗ: четвертый.

Версия ПЗ: версия 1.0.

Обозначение ПЗ: ИТ.САВЗ.В4.ПЗ.

Идентификация объекта оценки: САВЗ типа «В» четвертого класса защиты.

Основными угрозами, для противостояния которым используются САВЗ типа «В», являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и/или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов).

Согласно документу антивирусная защита определяется как защита информации и компонентов информационной системы от вредоносных компьютерных программ (обнаружение вирусов, блокирование, изолирование зараженных объектов, удаление вирусов из зараженных объектов).

Сигнатура определена как характерные признаки компьютерной вредоносной программы (вируса), используемые для ее обнаружения.

На рис. 2.7 в формате документа ФСТЭК изображена типовая схема ИС, в которой применяется САВЗ 4-го класса защиты типа «В».

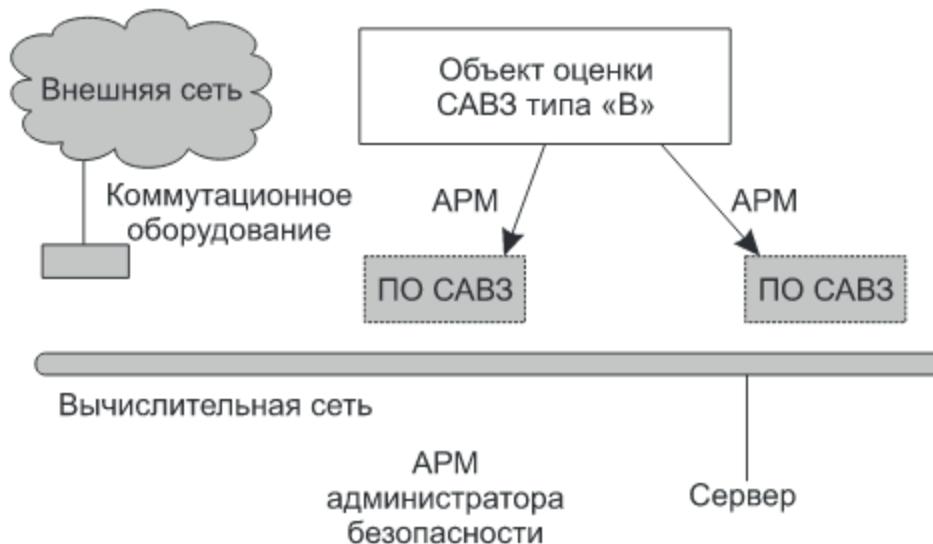


Рис. 2.7. Типовая схема применения САВЗ типа «В»

2.12.4. Требования к средствам обнаружения вторжений

Приказом ФСТЭК от 06.12.2011 г. № 638 утверждены «Требования к системам обнаружения вторжений», которые вступили в действие 15.03.2012 г.

Система обнаружения вторжений — программное или программно-техническое средство, реализующее функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Требования к СОВ применяются к программным и программно-техническим средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом.

Требования предназначены для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств ЗИ, заявителей на осуществление сертификации продукции, а также испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств ЗИ на соответствие обязательным требованиям по безопасности информации.

Выполнение Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической ЗИ и средств обеспечения безопасности ИТ, применяемых для формирования государственных информационных ресурсов, организуемых ФСТЭК России в пределах своих полномочий.

Требования к СОВ включают общие требования и требования к функциям безопасности систем обнаружения вторжений.

Для дифференциации требований к функциям безопасности установлены шесть классов защиты СОВ (рис. 2.8). Самый низкий класс — шестой, самый высокий — первый.

СОВ, соответствующие 4-му классу защиты, применяются в государственных ИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, а также в информационных системах общего пользования II класса.

СОВ, соответствующие 3–1-му классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.



Рис. 2.8. Классификация СОВ

Методические документы ФСТЭК России, содержащие профили защиты систем обнаружения вторжений 6, 5 и 4-го классов защиты, размещены на официальном сайте ФСТЭК, а документы для 1–3-го классов распространяются в соответствии с Временным порядком обеспечения организаций документами ФСТЭК России.

СОВ рассматривается как один из базовых элементов системы защиты ИС. Выделяются два типа систем: системы обнаружения вторжений уровня сети и системы обнаружения вторжений уровня узла.

Основной задачей СОВ уровня сети является сбор информации о сетевом трафике, передаваемом в пределах информационной системы, и ее дальнейший анализ с целью выявления вторжений.

СОВ уровня узла должна обнаруживать вторжения на основе анализа данных с узлов контролируемой ИС, включающих сетевой трафик, проходящий через контролируемые узлы, события, регистрируемые в журналах аудита ОС и прикладного ПО, вызовы функций, обращения к ресурсам.

ФСТЭК России 06.03.2012 г. утвердил «Профиль защиты СОВ уровня сети пятого класса».

Название ПЗ: Профиль защиты СОВ уровня сети пятого класса.

Тип СОВ: СОВ уровня сети.

Класс защиты: пятый.

Версия ПЗ: версия 1.0.

Обозначение ПЗ: ИТ.СОВ.С5.ПЗ.

Идентификация объекта оценки: системы обнаружения вторжений уровня сети.

Настоящий профиль защиты определяет требования безопасности для систем обнаружения вторжений уровня сети (объекта оценки), предназначенных для использования в информационных системах, функционирующих на базе вычислительных сетей. Объект оценки представляет собой элемент системы защиты информации информационных систем, функционирующих на базе вычислительных сетей, и применяется совместно с другими средствами ЗИ от НСД к информации в информационных системах.

Объект оценки должен обеспечивать обнаружение и/или блокирование следующих основных угроз безопасности информации:

- ◆ преднамеренного несанкционированного доступа или специальных воздействий на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- ◆ преднамеренного несанкционированного доступа или специальных воздействий на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Основными компонентами СОВ являются датчики (сенсоры) и анализаторы. Сенсоры собирают информацию о пакетах данных, передаваемых в пределах информационной системы (сегмента ИС), в которой (котором) установлены эти датчики. Датчики СОВ уровня сети могут быть реализованы в виде программного обеспечения, устанавливаемого на стандартные программно-технические платформы, а также в виде программно-технических устройств, подключаемых к ИС (сегменту ИС). Анализаторы выполняют анализ собранной датчиками информации, генерируют отчеты по результатам анализа и управляют процессами реагирования на выявленные вторжения.

На рис. 2.9 изображена типовая схема применения СОВ уровня сети, какой она представлена в документе ФСТЭК.

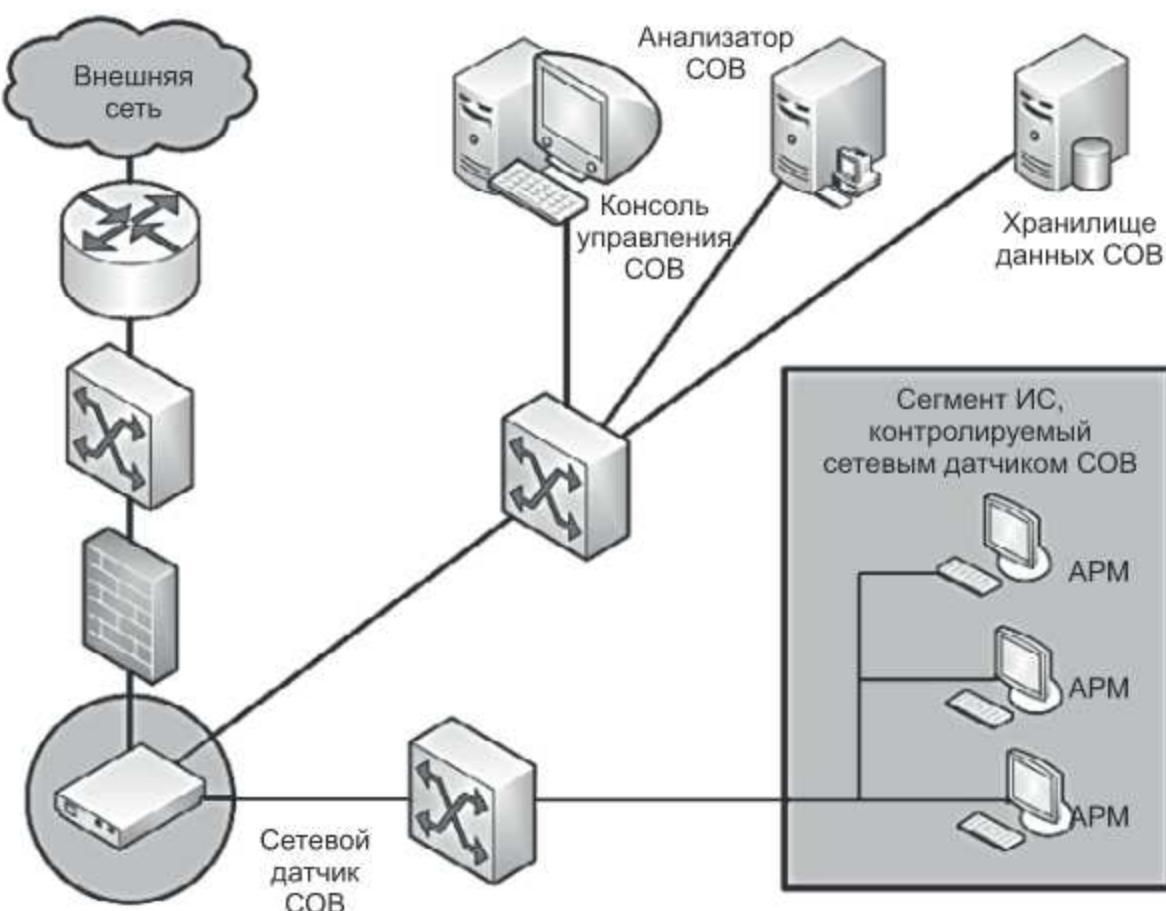


Рис. 2.9. Типовая схема применения СОВ уровня сети

2.12.5. Требования к средствам контроля съемных машинных носителей

Приказом ФСТЭК России от 28.07.2014 г. № 87 утверждены «Требования к средствам контроля съемных машинных носителей информации», которые вступили в силу 01.12.2014 г.

Требования применяются к программным и программно-техническим средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом и реализующим функции предотвращения НСД к информации с использованием съемных машинных носителей информации, подключаемых к ИС, и/или предотвращения несанкционированного переноса информации ограниченного доступа с зарегистрированных (учтенных) съемных машинных носителей информации. Требования предназначены для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств ЗИ, заявителей на осуществление обязательной сертификации продукции, а также испытательных лабораторий и органов

по сертификации, выполняющих работы по сертификации средств ЗИ на соответствие обязательным требованиям безопасности информации.

В Требованиях выделены следующие типы средств контроля съемных машинных носителей информации:

- ◆ средства контроля подключения съемных машинных носителей информации;
- ◆ средства контроля переноса информации со съемных машинных носителей информации.

Для дифференциации требований к функциям безопасности выделяются шесть классов защиты СКН (рис. 2.10). Самый низкий класс – шестой, самый высокий – первый.

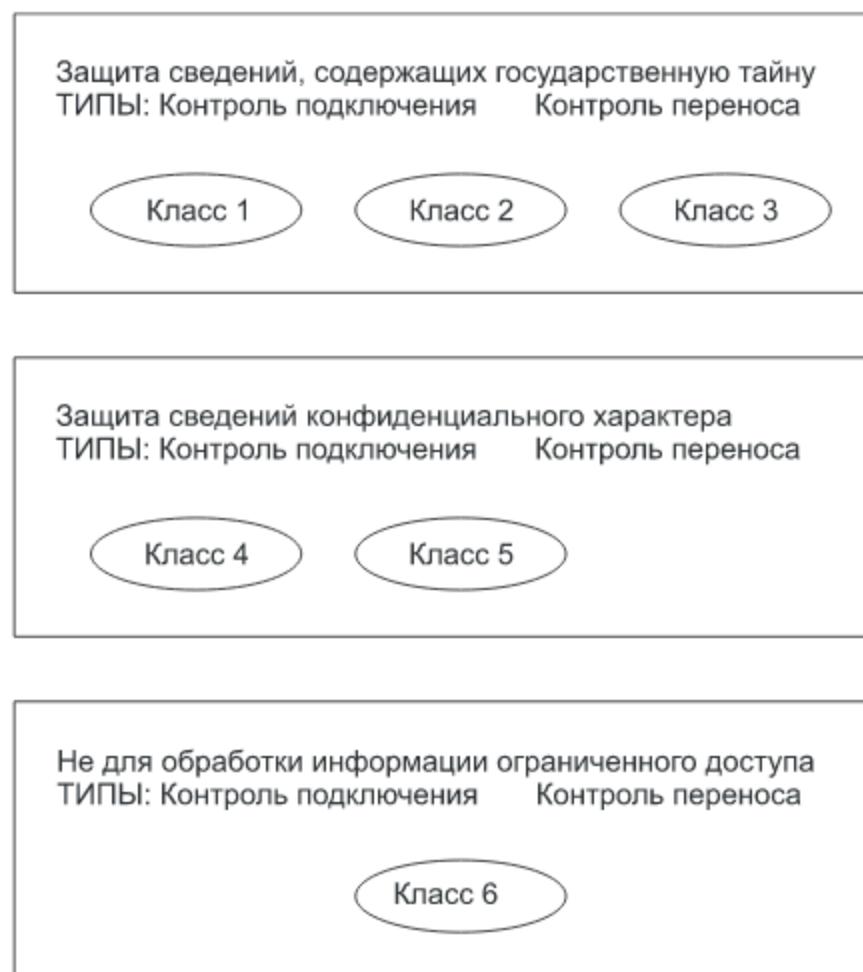


Рис. 2.10. Классификация СКН

СКН, соответствующие 6-му классу защиты, применяются в информационных системах, не являющихся государственными информационными системами, информационными системами персональных данных, информационными системами общего пользования и не предназначенных для обработки информации ограниченного доступа, содержащей сведения, составляющие государственную тайну.

СКН, соответствующие 5-му классу защиты, применяются в ГИС 3-го класса защищенности в случае отсутствия взаимодействия этих систем с информационно-телекоммуникационными сетями международного информационного обмена, а также в ГИС 4-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го уровня защищенности персональных данных в случае актуальности угроз 3-го типа и отсутствия взаимодействия этих систем с информационно-телекоммуникационными сетями международного информационного обмена, а также при необходимости обеспечения 4-го уровня защищенности персональных данных.

СКН, соответствующие 4-му классу защиты, применяются в государственных информационных системах 3-го класса защищенности в случае их взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена, а также в государственных информационных системах 1-го и 2-го классов защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го уровня защищенности персональных данных в случае актуальности угроз 2-го типа или взаимодействия этих систем с информационно-телекоммуникационными сетями международного информационного обмена, а также при необходимости обеспечения 1-го и 2-го уровня защищенности персональных данных, в информационных системах общего пользования 2-го класса.

Средства контроля съемных машинных носителей информации, соответствующие 3, 2 и 1-му классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

ПРИМЕЧАНИЕ

Тип актуальности угроз определен Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Детализация требований к функциям безопасности средств контроля съемных машинных носителей информации, установленных Требованиями, а также взаимосвязи этих Требований приведены для каждого класса и типа СКН в профилях защиты, утвержденных ФСТЭК России 01.12.2014 г. в качестве методических документов.

Идентификаторы профилей защиты приводятся в формате «И. СКН.“тип”“класс”.ПЗ», где обозначение «тип» может принимать значение «П», которое определяет, что СКН относится к средствам контроля подключения съемных машинных носителей информации, или значение «Н», которое определяет, что СКН относится к средствам контроля переноса

информации со съемных машинных носителей информации, а обозначение «класс» может принимать значения от 1 до 6 в соответствии с классом защиты СКН.

Методические документы ФСТЭК России, содержащие профили защиты СКН 6, 5 и 4-го классов защиты, размещены на официальном сайте ФСТЭК России, а документы для 1–3-го классов распространяются в соответствии с Временным порядком обеспечения организаций документами ФСТЭК России.

Идентификация профиля защиты:

Наименование ПЗ: Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты.

Тип СКН: средство контроля подключения съемных машинных носителей информации.

Класс защиты: четвертый.

Версия ПЗ: версия 1.0.

Обозначение ПЗ: ИТ.СКН.П4.ПЗ.

Идентификация объекта оценки: средство контроля подключения съемных машинных носителей информации.

В качестве типов съемных машинных носителей информации в данном профиле рассматриваются флэш-накопители, внешние накопители на жестких дисках и иные устройства.

Объект оценки представляет собой программное или программно-техническое средство, которое предназначено для обеспечения контроля использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации.

Объект оценки должен обеспечивать нейтрализацию угроз безопасности информации, связанных с подключением к ИС внутренними и внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из ИС или загрузкой в ИС с этих съемных машинных носителей информации вредоносного ПО.

В состав средства контроля подключения съемных машинных носителей информации входят следующие компоненты:

- ◆ программное обеспечение, устанавливаемое на средствах вычислительной техники и обеспечивающее взаимодействие с подключаемыми съемными машинными носителями информации;

- ◆ программное обеспечение управления (локального и/или централизованного) средствами контроля подключения съемных машинных носителей информации.

Данный профиль защиты разработан в соответствии с национальными стандартами Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» и ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

2.12.6. Требования к средствам доверенной загрузки

Приказом ФСТЭК России от 27.09.2013 г. № 119 утверждены «Требования к средствам доверенной загрузки», которые вступили в действие 01.01.2014 г.

Требования применяются к программным и программно-техническим средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом и реализующим функции по предотвращению НСД к программным и/или техническим ресурсам средствами вычислительной техники на этапе его загрузки.

Выполнение Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической ЗИ и средств обеспечения безопасности информационных технологий в системе сертификации ФСТЭК России.

В Требованиях выделены следующие типы СДЗ:

- ◆ средства доверенной загрузки уровня базовой системы ввода-вывода (УБ);
- ◆ средства доверенной загрузки уровня платы расширения (ПР);
- ◆ средства доверенной загрузки уровня загрузочной записи (ЗЗ).

Для дифференциации требований к функциям безопасности СДЗ выделяются шесть классов защиты (рис. 2.11). Самый низкий класс – шестой, самый высокий – первый.

Средства доверенной загрузки, соответствующие 6-му классу защиты, применяются в ИС, не являющихся государственными информационными системами, информационными системами персональных данных, информационными системами общего пользования и не предназначенных для обработки информации ограниченного доступа, содержащей сведения, составляющие государственную тайну.

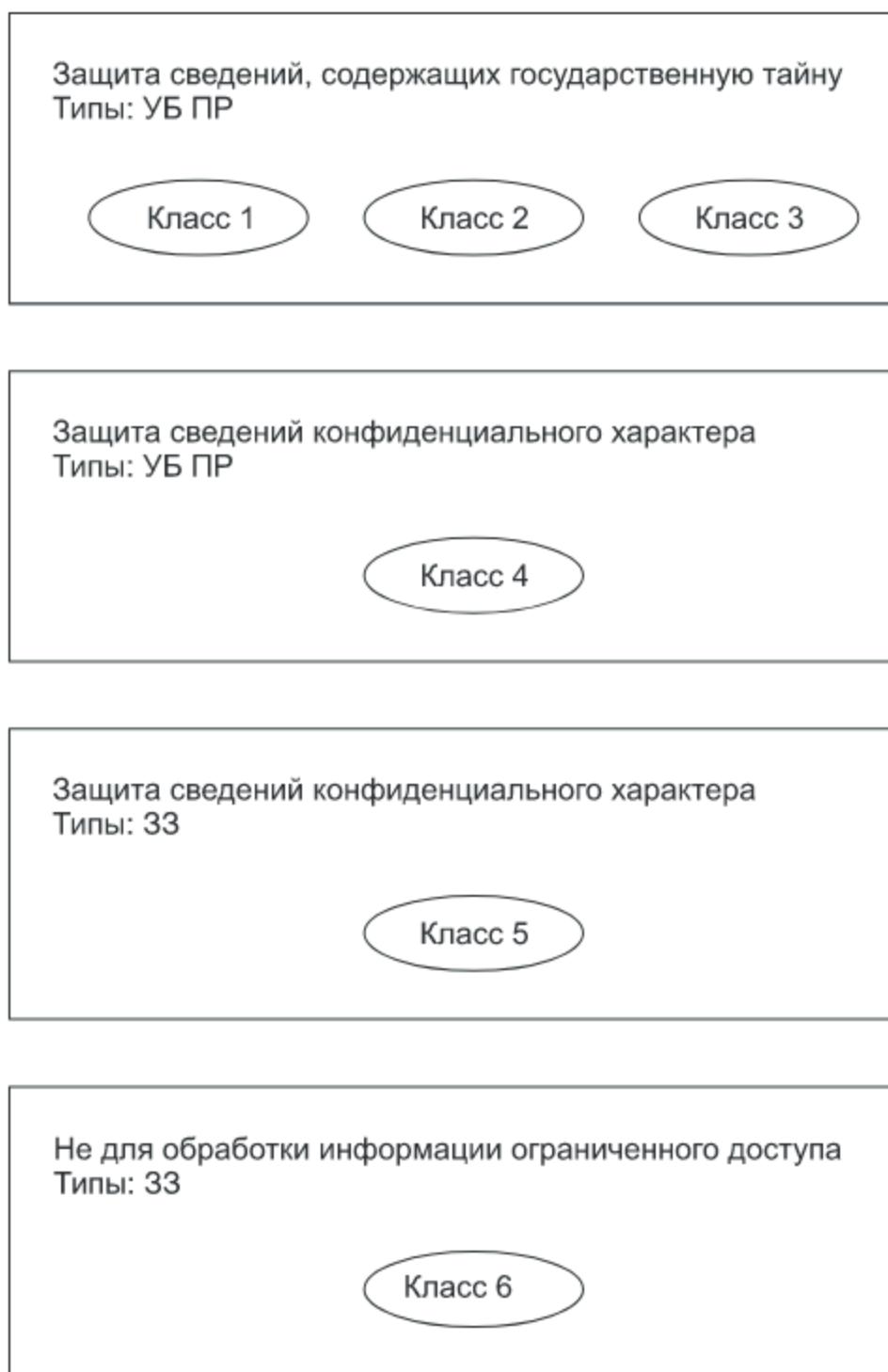


Рис. 2.11. Классификация СДЗ

Детализация требований к функциям безопасности СДЗ приведена для классов и типов средств доверенной загрузки в профилях защиты, утвержденных ФСТЭК России 30.12.2013 г. в качестве методических документов. Для СДЗ уровня базовой системы ввода-вывода и СДЗ уровня платы расширения разработаны ПЗ для классов 1–4, а для СДЗ уровня загрузочной записи – ПЗ для классов 5 и 6.

В Требованиях определено также соответствие классов СДЗ и уровней защищенности информации в ГИС, ИСПДн, а также информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

2.13. Заключительные замечания

В данной главе были рассмотрены основные традиционные руководящие документы Гостехкомиссии России и ее преемницы, ФСТЭК России. Несмотря на то что многие документы были разработаны еще в прошлом веке, они остаются актуальными и в настоящее время и используются в системах сертификации ФСТЭК. Однако с 2002 г. в России в различных системах сертификации стали постепенно разрабатываться и внедряться нормативные документы на основе международного стандарта, известного как «Общие критерии». Часть таких документов ФСТЭК была рассмотрена в этой главе.

Следует отметить, что в некоторых случаях требования, содержащиеся в традиционных документах ФСТЭК, мягко говоря, не совпадают с теми, которые содержатся в документах нового поколения. В частности, это касается соответствия между классами (уровнями) защищенности средств защиты информации (САЗ, МЭ, НДВ и т. д.) и различными информационными системами обработки информации. В первую очередь это касается информационных систем персональных данных. Это связано, вероятно, с тем, что закон № 152-ФЗ «О персональных данных» (принят 08.07.2006 г.) к настоящему времени претерпел существенные изменения, даже в части терминологии. Соответственно, несколько раз менялись нормативные документы регуляторов (ФСТЭК, ФСБ, Роскомнадзора) в части требований к защите персональных данных, а также принципов классификации информационных систем персональных данных в зависимости от типов обрабатываемых персональных данных и способов их обработки. Об этом, в частности, свидетельствует упомянутое ранее информационное сообщение ФСТЭК от 15.07.2013 г. № 240/22/2637.

Также не совсем понятным является соотношение понятий «автоматизированная система» и «информационная система», хотя, по сути, эти определения являются родственными. В ранних документах Гостехкомиссии используется вариант АС, а в современных документах ФСТЭК – термин ИС, который был введен в новом базовом законе от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В связи с принятием федерального закона № 149-ФЗ утратили силу два федеральных закона: от 20.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» и от 04.07.1996 г. № 85-ФЗ «Об участии в международном информационном обмене», а в ряд ранее принятых законов введены соответствующие изменения, в том числе в области терминологии.

На основе рассмотренных в данной главе нормативных документов в табл. 2.8 представлена сводная информация о соответствии между

классами защищенности и уровнями конфиденциальности информации, обрабатываемой в различных информационных системах. Для ИСПДн данные приведены в соответствии с нормативной базой на начало 2016 г.

Таблица 2.8. Соответствие между классом защищенности и уровнем конфиденциальности информации

Тип информации в ИС	Класс (уровень) защищенности информации	Класс (уровень) защищенности						
		СВТ (1–7)	САЗ (1–6)	МЭ (1–5)	СОВ (1–6)	СКН (1–6)	НДВ (1–4)	СДЗ (1–6)
Государственная тайна	Секретная (АС: 1В, 2А, 3А)	4	3	3	3	3	3	3
	Совершенно секретная (АС: 1Б, 2А, 3А)	3	2	2	2	2	2	2
	Особой важности (АС: 1А, 2А, 3А)	2	1	1	1	1	1	1
ИСПДн	1	5	4	3,4	4	4	4	4
	2	5	4	3,4	4	4	4	4
	3	5	4,5	3,4	4,5	4,5	4	4,5
	4	6	5	5	5	5	–	5
ГИС	K1	5	4	3,4	4	4	4	4
	K2	5	4	3,4	4	4	4	4
	K3	5	4,5	3,4	4,5	4,5	–	4,5
	K4	5	5	4	5	5	–	5
АСУ ТП	K1	5	3	3,4	3	3	4	–
	K2	5	4	3,4	4	4	4	–
	K3	5	5	4	5	5	–	–
АС	1А	2	1	1	1	1	1	1
	1Б	3	2	2	2	2	2	2
	1В	4	3	3	3	3	3	3
	1Г	–	–	4	–	–	–	–
	1Д	–	–	5	–	–	–	–
	2А, 3А	2–4	1–3	1–3	1–3	1–3	1–3	1–3
	2Б, 3Б	–	–	–	–	–	–	–
ИС ОП	I	–	–	–	–	–	–	–
	II	–	4	–	4	4	–	4

В таблице приняты следующие сокращения:

- ◆ СКН – классы защиты средств контроля съемных машинных носителей информации;
- ◆ СОВ – классы защиты систем обнаружения вторжений;
- ◆ САВЗ – классы защиты средств антивирусной защиты;
- ◆ НДВ – уровни контроля отсутствия недекларированных возможностей в программном обеспечении;
- ◆ МЭ – классы защищенности межсетевых экранов;
- ◆ СВТ – классы защищенности средств вычислительной техники;
- ◆ АСУ ТП – классы защищенности автоматизированных систем управления производственными и технологическими процессами;
- ◆ ИС ОП – классы защищенности информационных систем общего пользования;
- ◆ ГИС – классы защищенности государственных информационных систем, содержащих информацию ограниченного доступа (кроме гостайны);
- ◆ ИСПДн – уровни защищенности информационных систем персональных данных;
- ◆ АС – классы защищенности автоматизированных систем обработки информации.
- ◆ СДЗ – классы защищенности средств доверенной загрузки.

В заголовке таблицы цифры в скобках означают диапазон возможных классов средств защиты.

Контрольные вопросы и задания к главе 2

1. Каковы основные способы реализации НСД к информации?
2. Назовите основные руководящие документы Гостехкомиссии в области защиты информации.
3. Назовите основные нормативные документы ФСТЭК нового поколения в области защиты информации.
4. В чем отличие стандарта РФ от технического регламента?
5. Какой орган государственной власти осуществляет деятельность по стандартизации и техническому регулированию (ФСБ, ФСТЭК, Роскомнадзор, Росстандарт, Роспатент, МВД Минобороны)?
6. Сколько классов защищенности от НСД установлено в РД Гостехкомиссии для СВТ (3, 4, 5, 7, 9, 15)?

7. Сколько классов защищенности от НСД установлено в РД Гостехкомиссии для АС (3, 4, 5, 7, 9, 15)?
8. СВТ каких классов защищенности должны быть использованы при обработке сведений, содержащих гостайну?
9. Каковы определяющие признаки группировки АС в различные классы? Назовите основные классы защищенности АС.
10. АС каких классов защищенности должны быть использованы при обработке сведений, содержащих гостайну?
11. Сколько классов защищенности установлено в РД Гостехкомиссии для межсетевых экранов (3, 4, 5, 7, 9, 15)?
12. Межсетевые экраны какого класса должны применяться при обработке информации с грифом: «Секретно», «Совершенно секретно», «Особой важности»?
13. Сколько уровней контроля отсутствия НДВ в программном обеспечении установлено в РД Гостехкомиссии?
14. Какие уровни контроля отсутствия НДВ должны быть использованы при обработке сведений, содержащих гостайну?
15. Что такое профиль защиты?
16. Что такое задание по безопасности?
17. Какую информацию должен содержать профиль защиты?
18. Сколько классов защищенности установлено для САВЗ?
19. Каковы типы САВЗ?
20. САВЗ каких классов защищенности должны быть использованы при обработке сведений, содержащих гостайну?
21. Сколько классов защищенности установлено для СОВ?
22. СОВ каких классов защищенности должны быть использованы при обработке сведений, содержащих гостайну?
23. Что такое СКН?
24. Сколько классов защищенности установлено для СКН?
25. СКН каких классов защищенности должны быть использованы при обработке сведений, содержащих гостайну?

Глава 3. Национальные и международные стандарты в области информационной безопасности

3.1. Государственный стандарт по защите информации от НСД ГОСТ Р 50739–95

Государственный стандарт ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» введен в действие 01.01.1996 г. Он устанавливает единые функциональные требования к защите СВТ от несанкционированного доступа к информации, к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ.

Стандарт закрепляет на государственном уровне требования соответствующих нормативных документов Гостехкомиссии России 1992 г., рассмотренных ранее.

Защищенность от НСД к информации при ее обработке СВТ обеспечивается тремя группами требований к средствам защиты, реализуемым в СВТ:

- ◆ требования к разграничению доступа;
- ◆ требования к учету (СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации);
- ◆ требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

Требования к разграничению доступа определяют следующие показатели защищенности, которые должны поддерживаться СВТ:

- ◆ дискретизационный принцип контроля доступа;
- ◆ мандатный принцип контроля доступа;
- ◆ идентификация и аутентификация;
- ◆ очистка памяти;
- ◆ изоляция модулей;
- ◆ защита ввода и вывода на отчуждаемый физический носитель информации;
- ◆ сопоставление пользователя с устройством.

Комплекс средств защиты должен регистрировать следующие события:

- ◆ использование идентификационного и аутентификационного механизма;
- ◆ запрос на доступ к защищаемому ресурсу (например, открытие файла, запуск программы);
- ◆ создание и уничтожение объекта;
- ◆ действия, связанные с изменением правил разграничения доступа.

Для каждого из этих событий должна быть зарегистрирована следующая информация: дата и время, субъект, осуществляющий регистрируемое действие, тип события, успешность события.

КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.

В СВТ должны тестироваться:

- ◆ реализация правил разграничения доступа;
- ◆ очистка оперативной и внешней памяти;
- ◆ работа механизма изоляции процессов в оперативной памяти;
- ◆ маркировка документов;
- ◆ защита ввода информации и ее вывода на отчуждаемый физический носитель и сопоставление пользователя с устройством;
- ◆ идентификация и аутентификация, а также средства их защиты;
- ◆ регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- ◆ работа механизма надежного восстановления;
- ◆ работа механизма, осуществляющего контроль за целостностью комплекса средств защиты;
- ◆ работа механизма, осуществляющего контроль дистрибуции.

При приемке СВТ, их сертификации и испытаниях необходима документация, включающая в себя:

- ◆ руководство пользователя;
- ◆ руководство по КСЗ;
- ◆ тестовую документацию;
- ◆ конструкторскую (проектную) документацию.

3.2. Национальный стандарт по менеджменту инцидентов ИБ ГОСТ Р ИСО/МЭК ТО 18044–2007

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» введен в действие 01.07.2008 г. Он идентичен международному стандарту ISO/IEC TR 18044:2004 «Информационные технологии. Финансовые услуги. Рекомендации по информационной безопасности» («Information technology – Security techniques – Information security incident management»).

В стандарте содержатся рекомендации по менеджменту инцидентов информационной безопасности в организациях для руководителей подразделений по обеспечению ИБ при применении информационных технологий, информационных систем, сервисов и сетей. Его положения могут использоваться совместно с другими стандартами, в том числе стандартами, содержащими требования к системе менеджмента ИБ организации, которые будут рассмотрены далее.

Предпринимаемые защитные меры ИБ не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей. После внедрения защитных мер останутся (или возникнут со временем) слабые места, которые могут сделать неэффективным обеспечение информационной безопасности и, следовательно, возможными инциденты ИБ.

Под инцидентом информационной безопасности в стандарте понимается появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ. Инциденты ИБ могут быть преднамеренными или случайными и вызываться как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение информации, ее

уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение.

В качестве примера в стандарте приведены следующие инциденты:

1. Отказ в обслуживании.
2. Сбор информации (предполагает проведение разведки с целью определения потенциальных уязвимостей, потенциальных целей атаки и получения представления о сервисах).
3. Несанкционированный доступ (к информации, сервисам, сети).

В качестве основы общей стратегии ИБ организации необходимо использовать структурный подход к менеджменту инцидентов ИБ, целями которого должно стать обеспечение следующих условий:

- ◆ события ИБ должны быть обнаружены и эффективно обработаны;
- ◆ идентифицированные инциденты ИБ должны быть оценены, и реагирование на них должно быть осуществлено наиболее целесообразным и результативным способом;
- ◆ воздействия инцидентов ИБ на организацию и ее бизнес-операции необходимо минимизировать соответствующими защитными мерами;
- ◆ из инцидентов ИБ и их менеджмента необходимо быстро извлечь уроки с целью повышения шансов предотвращения инцидентов ИБ в будущем, улучшения защитных мер ИБ и системы менеджмента инцидентов ИБ.

Менеджмент инцидентов ИБ подразделяют на четыре этапа:

- ◆ планирование и подготовка;
- ◆ использование;
- ◆ анализ;
- ◆ улучшение.

Первый этап предполагает, в частности, создание в организации структурного подразделения менеджмента инцидентов ИБ – группы реагирования на инциденты ИБ (ГРИИБ). Целью создания ГРИИБ является обеспечение организации персоналом, который способен оценить инциденты ИБ, отреагировать на них и извлечь из них уроки. Состав и количество персонала, а также структура ГРИИБ должны соответствовать масштабу и структуре организации. Уровень полномочий руководителя и членов ГРИИБ должен позволять предпринимать действия, адекватные инциденту ИБ. Руководитель ГРИИБ должен иметь делегированные полномочия немедленно принимать решение о том, какие меры предпринять относительно инцидента.

Необходимо установить отношения между ГРИИБ и сторонними лицами и организациями, которые могут быть привлечены для анализа инцидентов и ликвидации их последствий.

Блок-схема последовательности операций обработки событий и инцидентов ИБ представлена на рис. 3.1.

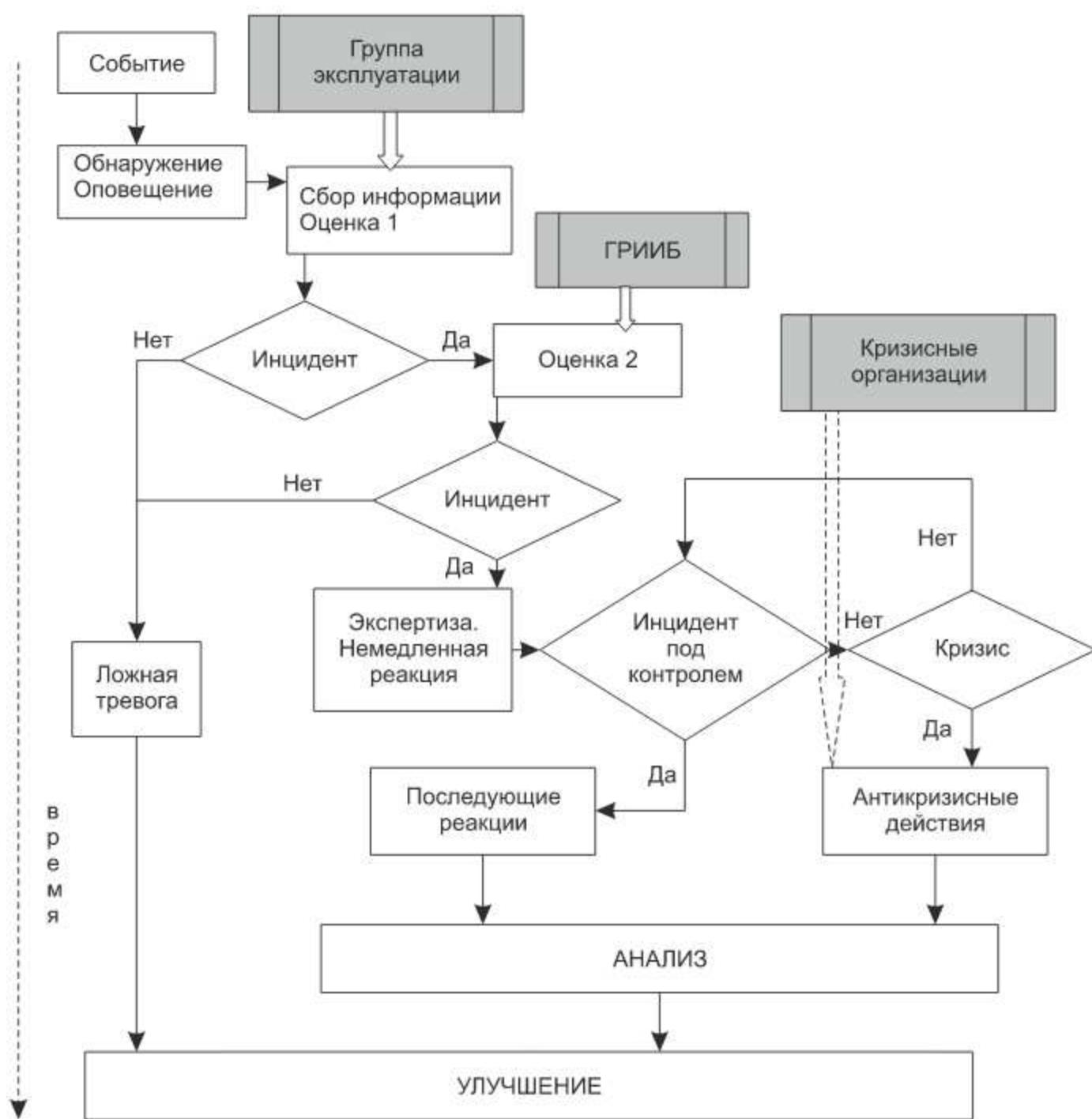


Рис. 3.1. Блок-схема обработки инцидентов

Для принятия структурного подхода к менеджменту инцидентов ИБ жизненно необходима постоянная поддержка со стороны руководства. Персонал организации должен распознавать инциденты ИБ и знать свои действия при их возникновении.

В системе менеджмента инцидентов ИБ может содержаться конфиденциальная информация, и лицам, занимающимся инцидентами, может потребоваться доступ к ней. Поэтому во время обработки необходимо обеспечивать анонимность этой информации, или персонал должен подписать соглашение о конфиденциальности (неразглашении) при получении доступа к ней.

3.3. Национальный стандарт по менеджменту безопасности ИТТ ГОСТ Р ИСО/МЭК 13335-1–2006

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 13335-1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» введен в действие 01.06.2007 г. Он идентичен международному стандарту ISO/IEC 13335-1:2004 («Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management»).

Стандарт представляет собой руководство по управлению безопасностью информационных и телекоммуникационных технологий, устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ.

Стандарт вводит несколько терминов в области ИБ.

Конфиденциальность – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

В утратившем силу федеральном законе № 24-ФЗ был введен термин «конфиденциальная информация» – «документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации». Закон № 149-ФЗ исключил термин «конфиденциальная информация», а ввел термин «конфиденциальность информации» как «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Конфиденциальность в переводе с латинского означает «доверие» (то есть, передавая такую информацию, мы надеемся на ее сохранность и нераспространение). Таким образом, в законе № 149-ФЗ конфиденциальность определяется как требование к лицу, а в стандарте – как свойство информации.

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами ИБ согласно стандарту являются:

- ◆ утрата услуг, оборудования или устройств;
- ◆ системные сбои или перегрузки;
- ◆ ошибки пользователей;
- ◆ несоблюдение политик или рекомендаций;
- ◆ нарушение физических мер защиты;
- ◆ неконтролируемые изменения систем;
- ◆ сбои программного обеспечения и отказы технических средств;
- ◆ нарушение правил доступа.

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Риск – потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов. Риск определяется как сочетание вероятности события и его последствий.

Оценка риска – процесс, объединяющий идентификацию риска, анализ риска и оценивание риска.

Менеджмент риска – полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказывать влияние на ресурсы информационно-телекоммуникационных технологий.

Угроза – потенциальная причина инцидента, который может нанести ущерб системе или организации.

Уязвимость – слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

Для создания эффективной программы безопасности ИТТ фундаментальными являются следующие принципы безопасности:

- ◆ менеджмент риска – активы должны быть защищены путем принятия соответствующих мер;
- ◆ обязательства – важны обязательства организации в области безопасности ИТТ и в управлении рисками;
- ◆ служебные обязанности и ответственность – руководство организации несет ответственность за обеспечение безопасности активов;

- ◆ цели, стратегии и политика — управление рисками, связанными с безопасностью ИТТ, должно осуществляться с учетом целей, стратегий и политики организации;
- ◆ управление жизненным циклом — управление безопасностью ИТТ должно быть непрерывным в течение всего их жизненного цикла.

Основными компонентами безопасности являются активы, угрозы, уязвимости, воздействие, риск, защитные меры и ограничения.

Активы включают в себя:

- ◆ материальные активы;
- ◆ информацию (например, документы, базы данных);
- ◆ программное обеспечение;
- ◆ способность производить продукт или предоставлять услугу;
- ◆ людей;
- ◆ нематериальные ресурсы (престиж фирмы, репутацию и т. п.).

Все активы должны быть идентифицированы и оценены.

Активы могут быть подвержены многим видам угроз. Все угрозы должны быть идентифицированы, а их уровень и вероятность возникновения — оценены.

Угрозы могут быть естественного происхождения или связанными с человеческим фактором, которые, в свою очередь, могут быть случайными или целенаправленными.

Характеристики угроз:

- ◆ источник (внутренний или внешний);
- ◆ мотивация, например финансовая выгода;
- ◆ частота возникновения;
- ◆ правдоподобие;
- ◆ вредоносное воздействие.

При оценке уровень угрозы в зависимости от результата ее воздействия может быть определен как высокий, средний или низкий.

Уязвимость сама по себе не причиняет ущерб, но является условием или набором условий, позволяющим угрозе воздействовать на активы. Уязвимость необходимо оценивать индивидуально и в совокупности, чтобы рассмотреть сложившуюся ситуацию в целом. Оценка уязвимостей — это проверка слабостей, которые могут быть использованы существующими угрозами. Эта оценка должна учитывать окружающую среду и существующие защитные

меры. При оценке уровень уязвимости может быть определен как высокий, средний или низкий.

Воздействие – это результат инцидента ИБ, вызванного угрозой и нанесшего ущерб ее активу. Контроль за воздействием позволяет достичь равновесия между предполагаемыми последствиями инцидента и стоимостью защитных мер. Количественное и качественное измерение воздействия могут быть проведены:

- ◆ определением финансовых потерь;
- ◆ использованием эмпирической шкалы серьезности воздействия, например от 1 до 10;
- ◆ использованием заранее оговоренных уровней (высокий, средний и низкий).

Риск – это способность конкретной угрозы использовать уязвимости одного или нескольких видов активов для нанесения ущерба организации. Риск характеризуется комбинацией двух факторов: вероятностью возникновения инцидента и его разрушительным воздействием. Риск никогда не устраняется полностью. Принятие остаточного риска является частью заключения о соответствии уровня безопасности потребностям организации.

Защитные меры – это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов. Защитные меры могут выполнять одну или несколько из следующих функций: предотвращение, сдерживание, обнаружение, ограничение, исправление, восстановление, мониторинг, уведомление. Области использования защитных мер включают в себя физическую среду, техническую среду (аппаратно-программное обеспечение и средства связи), персонал, администрирование.

Ограничения устанавливает или признает руководство организации, а также определяет среда, в которой действует организация. Ограничения могут быть организационные, коммерческие, финансовые, по окружающей среде, по персоналу, временные, правовые, технические, социальные. Ограничения могут со временем изменяться, поэтому необходимо периодически пересматривать существующие и учитывать новые.

На рис. 3.2 представлена модель, которая отображает взаимосвязь компонентов безопасности:

- ◆ окружающую среду, содержащую ограничения и угрозы;
- ◆ активы организации;
- ◆ уязвимости, присущие данным активам;

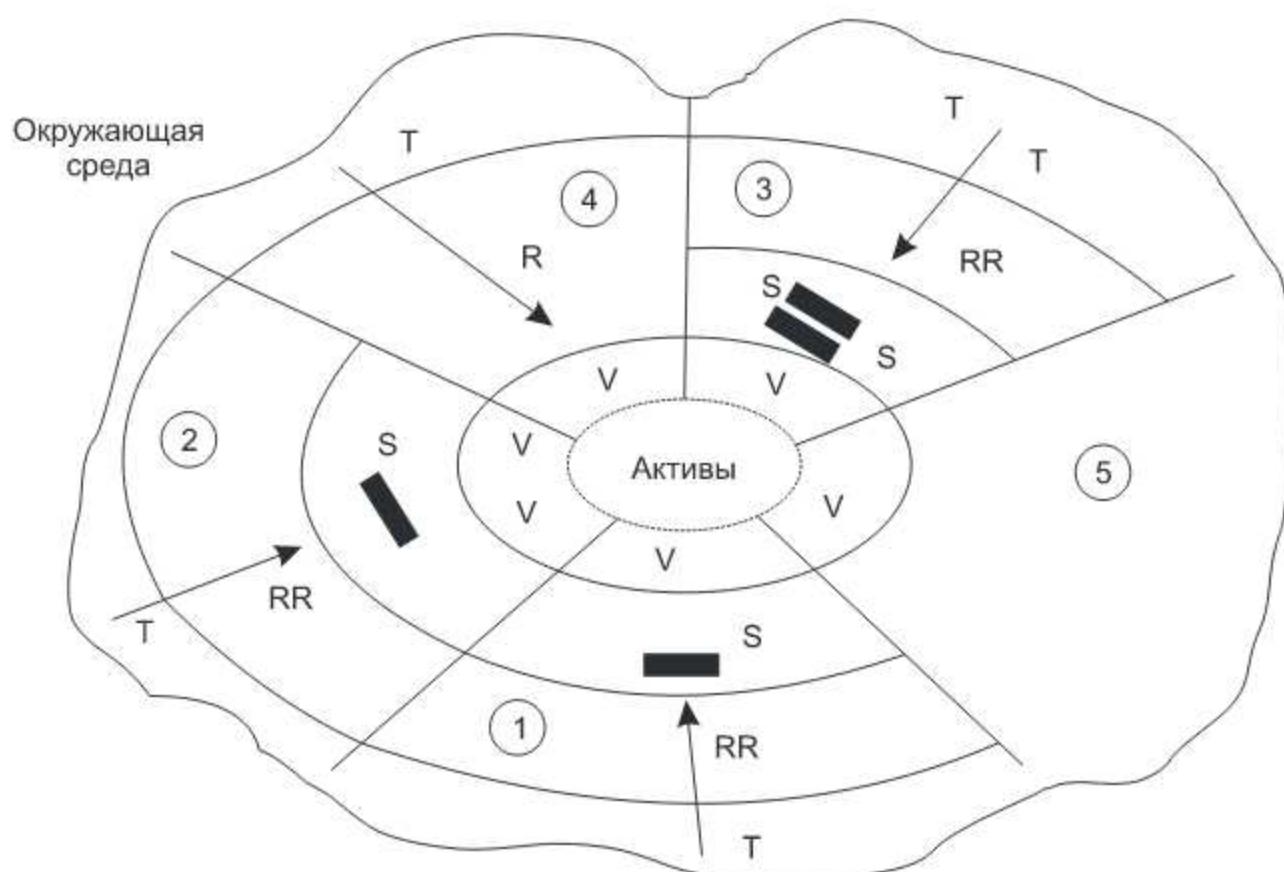
- ◆ меры для защиты активов;
- ◆ приемлемые для организации остаточные риски.

В модели используются следующие обозначения: R – риск; RR – остаточный риск; S – защитная мера; T – угроза; V – уязвимость актива.

ГОСТ Р ИСО/МЭК 13335-1-2006

Взаимосвязь компонентов безопасности

5 возможных сценариев



R – риск; RR – остаточный риск; S – защитная мера; Т – угроза; V – уязвимость актива

Рис. 3.2. Взаимосвязь компонентов безопасности

Модель отражает пять возможных сценариев.

Сценарий 1 – защитная мера может быть эффективна для снижения рисков, связанных с угрозой, способной использовать уязвимость актива.

Сценарий 2 – защитная мера может быть эффективной для снижения риска, связанного с угрозой, использующей группу уязвимостей актива.

Сценарий 3 – группа защитных мер может быть эффективной для снижения рисков, связанных с группой угроз, использующих уязвимость актива.

Сценарий 4 – риск считают приемлемым, и никакие меры не реализуются даже в присутствии угроз и при наличии уязвимостей актива.

Сценарий 5 – существует уязвимость актива, но неизвестны угрозы, которые могли бы ее использовать. В качестве защитной меры может быть

использован мониторинг угроз для того, чтобы убедиться, что угрозы, способные использовать уязвимость актива, не появились.

В качестве основы безопасности ИТТ организации в виде руководящих документов различного уровня должны быть сформулированы цели (чего необходимо достичь), стратегии (способы достижения цели), политика (правила, которые следует соблюдать при реализации стратегий) и процедуры (методы осуществления политики). Они определяют уровень безопасности для организации и порог приемлемого риска. Иерархия документации должна поддерживаться и актуализироваться по результатам периодического анализа безопасности (например, по результатам оценки рисков, внешнего и внутреннего аудита безопасности) и в связи с изменениями целей деятельности организации.

Тщательное определение приемлемых рисков и, следовательно, соответствующего уровня безопасности – это ключ к успешному управлению безопасностью. Чтобы оценить, в какой мере бизнес организации зависит от ИТТ, и установить задачи безопасности ИТТ, необходимо рассмотреть вопросы о том:

- ◆ какие составляющие бизнеса не могут осуществляться без ИТТ;
- ◆ какие задачи могут быть решены только при помощи ИТТ;
- ◆ какие важные решения зависят от конфиденциальности, целостности, доступности, неотказемости, подотчетности и аутентичности информации, хранимой или обрабатываемой ИТТ;
- ◆ какая хранимая или обрабатываемая информация должна защищаться;
- ◆ какими для организации могут быть последствия инцидента безопасности.

Политику безопасности ИТТ следует формировать, исходя из согласованных целей и стратегий безопасности ИТТ организации, она должна соответствовать законодательству и требованиям регулирующих органов.

Политика безопасности ИТТ должна распространяться на:

- ◆ предмет и задачи безопасности;
- ◆ цели безопасности;
- ◆ требования безопасности ИТТ к обеспечению конфиденциальности, целостности, доступности информации и средств ее обработки;
- ◆ ссылки на стандарты;
- ◆ администрирование ИБ, охватывающее организационные и индивидуальные ответственности и полномочия;

- ◆ уровень безопасности и остаточный риск, определяемый руководством организации;
- ◆ общие правила контроля доступа;
- ◆ процедуры проверки и поддержания безопасности.

Стандарт определяет организационные меры обеспечения безопасности ИТТ. Руководство должно отвечать за все аспекты управления безопасностью, включая принятие решений по управлению рисками. В организации должны иметься следующие структурные единицы: совет по безопасности ИТТ, администратор безопасности ИТТ. Они должны иметь строго определенные и четко сформулированные обязанности и достаточные полномочия для обеспечения выполнения политики безопасности ИТТ.

В совет по безопасности ИТТ должны входить люди, обладающие достаточной квалификацией, чтобы давать консультации и рекомендации в отношении стратегий, определять требования, формулировать политику, разрабатывать программу безопасности, проверять их выполнение и руководить администратором безопасности ИТТ.

Администратор безопасности ИТТ должен играть роль центра для всех направлений безопасности ИТТ в рамках организации. В обязанности администратора безопасности ИТТ входит:

- ◆ наблюдение за реализацией программы безопасности ИТТ;
- ◆ координация расследования инцидентов;
- ◆ установление целей и критериев безопасности ИТТ;
- ◆ анализ, аудит и мониторинг эффективности контроля безопасности.

В крупных организациях может существовать сеть администраторов для подразделений, департаментов и т. д.

Обязательства руководства организации в отношении задач безопасности включают в себя:

- ◆ понимание общих потребностей организации;
- ◆ понимание потребности в безопасности ИТТ в рамках организации;
- ◆ демонстрацию обязательств в отношении безопасности ИТТ;
- ◆ необходимость выделения ресурсов для безопасности ИТТ;
- ◆ осведомленность о том, что является средствами безопасности ИТТ и в чем она заключается.

Безопасность должна быть обеспечена на протяжении всего жизненного цикла информации и ИТТ, от планирования до приобретения, тестирования и эксплуатации.

При управлении функциональной деятельностью в области безопасности необходимо учитывать внешнюю среду, в которой действует организация, поскольку она может оказывать значительное влияние на общий подход к организации информационной безопасности.

3.4. Национальный стандарт по менеджменту безопасности сетей ГОСТ Р ИСО/МЭК 13335-5–2006

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 13335-5–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети» введен в действие 01.06.2007 г. Он полностью идентичен международному ISO/IEC TR 13335-5:2001 («Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security»). Стандарт представляет собой руководство по управлению безопасностью сетей и содержит основные положения по выявлению и анализу факторов, имеющих отношение к компонентам безопасности связи. Эти факторы следует учитывать при установлении требований по безопасности сети.

В стандарте приведено описание трех основных критериев идентификации потенциальных контролируемых зон. Эти критерии распознают:

- ◆ разные типы сетевых соединений;
- ◆ характеристики разной организации сети;
- ◆ потенциальные виды рисков обеспечения безопасности, связанного с сетевыми соединениями.

Для того чтобы идентифицировать заданные требования безопасности сети и контролируемые зоны, необходимо решить следующие задачи:

- ◆ проанализировать общие требования к обеспечению безопасности сетевых соединений, изложенных в политике безопасности ИТ организации;
- ◆ проанализировать сетевую структуру;
- ◆ идентифицировать типы соединения сети;
- ◆ проанализировать характеристики объединения в сеть;
- ◆ определить виды рисков безопасности;
- ◆ идентифицировать потенциально контролируемые зоны;
- ◆ разработать документацию и выполнить анализ вариантов структуры обеспечения безопасности;
- ◆ распределить задачи по детальному выбору защитных мер.

Анализ требований политики безопасности ИТ организации позволяет выявить типы угроз и требования безопасности, имеющие непосредственное отношение к сетевым соединениям.

Виды рисков безопасности, с которыми может встретиться организация, касаются:

- ◆ конфиденциальности информации;
- ◆ целостности информации;
- ◆ доступности информации и услуг;
- ◆ отказа от подтверждения обязательств;
- ◆ подотчетности транзакций;
- ◆ достоверности информации;
- ◆ надежности информации.

Более подробно аспекты безопасности сетей изложены в национальных стандартах серии ГОСТ Р ИСО/МЭК 27033, которые рассматриваются далее.

3.5. Стандарты серии 27000 по менеджменту ИБ

3.5.1. История создания стандартов серии 27000

Все организации собирают, обрабатывают, хранят и передают большое количество информации, которая является важнейшим ресурсом. Однако эта информация является объектом различных угроз, а следовательно, будучи важнейшим активом, имеющим ценность, она требует соответствующей защиты, например, от потери доступности, конфиденциальности и целостности. Защита информационных активов посредством определения, достижения, поддержания и улучшения информационной безопасности является важным аспектом деятельности организации, позволяющим достигать целей бизнеса и поддерживать репутацию.

Так как угрозы активам, а следовательно, и риски информационной безопасности постоянно меняются в зависимости от обстоятельств, организациям необходимо:

- ◆ контролировать и оценивать эффективность имеющихся средств управления;

- ◆ идентифицировать появляющиеся угрозы и риски;
- ◆ выбирать, реализовывать и улучшать должным образом соответствующие меры и средства контроля и управления.

Эти скоординированные действия являются элементами системы менеджмента информационной безопасности. Такая система представляет модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов.

В первой половине 90-х гг. прошлого века в Великобритании был разработан стандарт BS 7799, который в 1995 г. в качестве свода норм и правил по отношению к обеспечению ИБ получил статус государственного. Первая часть стандарта BS 7799, которая называлась «Практические правила управления информационной безопасностью», была разработана в 1995 г. по заказу правительства Великобритании. Она стала практическим руководством по управлению информационной безопасностью в организации.

В 1998 г. была принята вторая часть стандарта BS 7799 «Системы менеджмента информационной безопасности. Спецификация и руководство по применению», которая определила общую модель построения СМИБ и набор обязательных требований, на соответствие которым должна производиться ее сертификация.

В 2000 г. после пересмотра первой части стандарта технический комитет ISO принял его в качестве международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000). Вторая часть BS 7799 в 2005 г. была принята ИСО в качестве международного стандарта ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». В том же году была обновлена первая часть стандарта, которая стала версией ISO/IEC 17799:2005, а затем переименована в ISO/IEC 27002–2005.

На сегодняшний момент опыт построения эффективных систем менеджмента информационной безопасности зафиксирован в целой серии международных стандартов серии 27000. На основе международных стандартов этой серии приняты соответствующие идентичные национальные стандарты Российской Федерации:

- ◆ **ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»** (аналог ISO/IEC 27000:2009 «Information technology – Security techniques – Information security management systems – Overview and vocabulary»). Введен в действие 01.12.2013 г.

- ◆ **ГОСТ Р ИСО/МЭК 27001–2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»** (аналог ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements»). Введен в действие 01.02.2008 г.
- ◆ **ГОСТ Р ИСО/МЭК 27002–2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»** (аналог ISO/IEC 27002:2005 «Information technology – Security techniques – Code of practice for information security management»). Введен в действие 01.01.2014 г.
- ◆ **ГОСТ Р ИСО/МЭК 27003–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности»** (аналог ISO/IEC 27003:2010 «Information technology – Security techniques – Information security management systems implementation guidance»). Введен в действие 01.12.2013 г.
- ◆ **ГОСТ Р ИСО/МЭК 27004–2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения»** (аналог ISO/IEC 27004:2009 «Information technology – Security techniques – Information security management – Measurement»). Введен в действие 01.01.2012 г.
- ◆ **ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»** (аналог ISO/IEC 27005:2008 «Information technology – Security techniques – Information security risk management»). Введен в действие 01.12.2011 г.
- ◆ **ГОСТ Р ИСО/МЭК 27006–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»** (аналог ISO/IEC 27006:2007 «Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems»). Введен в действие 01.10.2009 г.
- ◆ **ГОСТ Р ИСО/МЭК 27007–2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»** (аналог ISO/IEC 27007:2011 «Information technology – Security techniques – Guidelines for information security management systems auditing»). Введен в действие 01.06.2015 г.
- ◆ **ГОСТ Р ИСО/МЭК 27011–2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту**

информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002» (аналог ISO/IEC 27011:2008 «Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002»). Введен в действие 01.01.2014 г.

Семейство национальных стандартов России СМИБ поддерживает взаимосвязь со многими другими стандартами и классифицируется по следующим признакам:

- ◆ стандарты, содержащие общий обзор и терминологию;
- ◆ стандарты, задающие требования;
- ◆ стандарты, содержащие общие рекомендации.

Семейство стандартов СМИБ состоит из взаимосвязанных стандартов и содержит несколько существенных структурных компонентов:

- ◆ стандарты, содержащие общий обзор и терминологию;
- ◆ стандарты, описывающие требования СМИБ и требования для организаций, сертифицирующих соответствие стандарту;
- ◆ стандарты, обеспечивающие руководство при различных аспектах реализации СМИБ.

Взаимосвязь стандартов семейства ИСО/МЭК 27000 представлена на рис. 3.3.

Терминологию и основы системы менеджмента информационной безопасности определяет стандарт ИСО/МЭК 27000.

Стандарт ИСО/МЭК 27001 содержит нормативные требования для создания, внедрения и эксплуатации СМИБ.

Стандарт ИСО/МЭК 27002 является руководством по внедрению средств управления защитой информации.

Стандарт ИСО/МЭК 27003 содержит описание процессного подхода к внедрению СМИБ.

Стандарт ИСО/МЭК 27004 содержит систему измерений, позволяющую оценивать эффективность СМИБ.

Стандарт ИСО/МЭК 27005 содержит руководство по внедрению процессного подхода к управлению рисками.

Стандарт ИСО/МЭК 27006 задает требования и является руководством для органов, проводящих аудит и сертификацию СМИБ.

Стандарт ИСО/МЭК 27007 содержит руководство для организаций, которым необходимо проводить внутренний или внешний аудит СМИБ или управлять программой проведения аудита СМИБ.

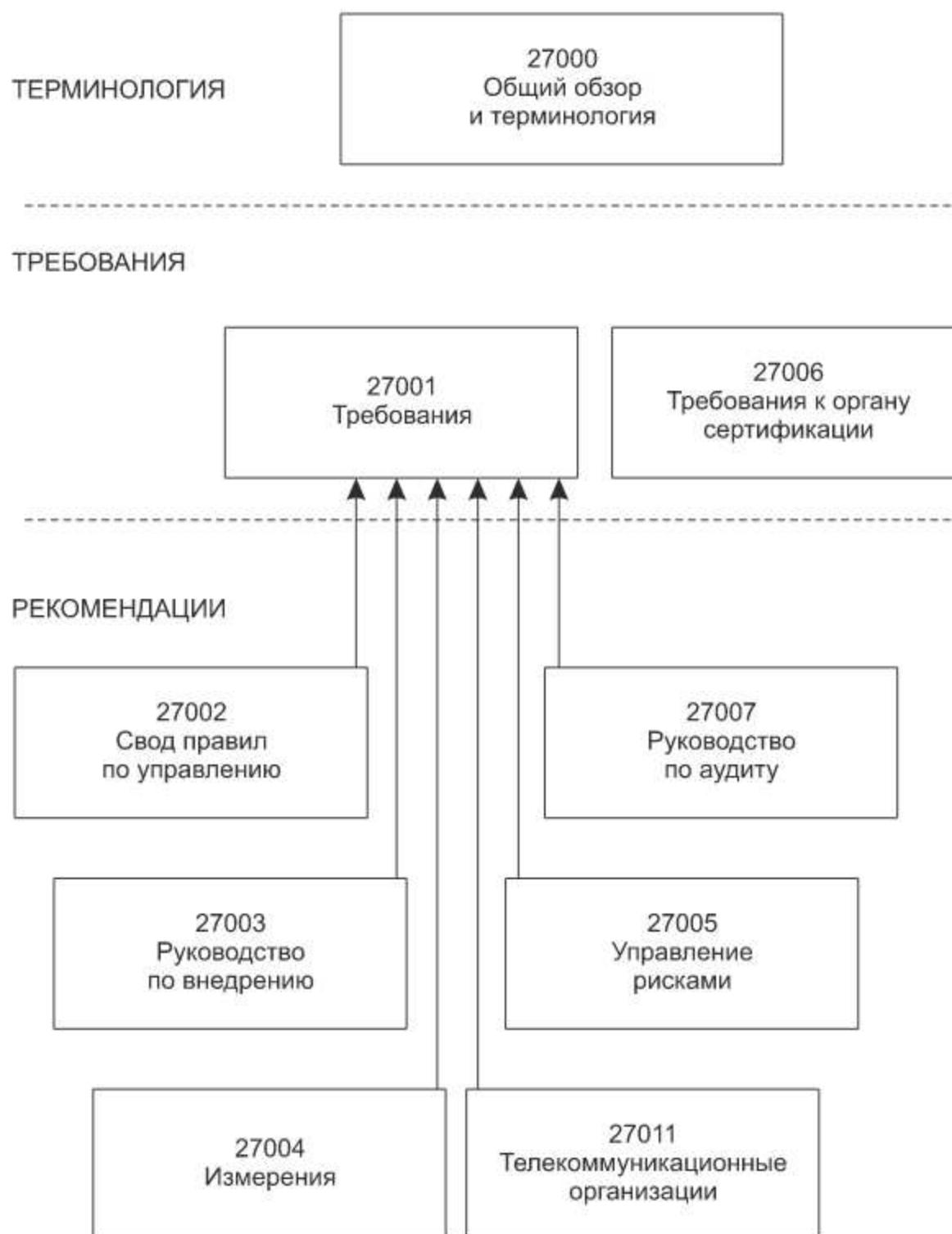


Рис. 3.3. Взаимосвязь стандартов семейства СМИБ

Стандарт ИСО/МЭК 27011 содержит дополнительные рекомендации по реализации и менеджменту информационной безопасности в организациях, предоставляющих телекоммуникационные услуги, на основе стандарта ISO/IEC 27002.

В состав международных стандартов серии 27000 входит еще ряд стандартов, которые в настоящее время не имеют аналогов в России. Среди них можно отметить стандарты, представляющие рекомендации в специфических областях. Примером такого типа стандартов является ISO 27799:2008 «Health informatics – Information security management in health using ISO/

IEC 27002» («Информатика в здравоохранении. Менеджмент информационной безопасности по стандарту ISO/IEC 27002»).

3.5.2. Национальный стандарт ГОСТ Р ИСО/МЭК 27000–2012 – термины по СМИБ

Национальный стандарт ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология», введенный в действие 01.12.2013 г., идентичен международному стандарту ISO/IEC 27000:2009. Он содержит:

- ◆ обзор семейства стандартов СМИБ;
- ◆ введение в систему менеджмента информационной безопасности;
- ◆ термины и определения для использования в семействе стандартов СМИБ.

В стандарте введен ряд терминов, в частности, следующие.

Атака — попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения НСД к активу или его несанкционированного использования.

Конфиденциальность — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов.

Информационная безопасность — сохранение конфиденциальности, целостности и доступности информации.

ПРИМЕЧАНИЕ

Также сюда могут быть включены другие свойства, такие как подлинность, подотчетность, неотказуемость и достоверность.

Подлинность — свойство, гарантирующее, что субъект или ресурс идентичен заявленному.

Подотчетность — ответственность субъекта за его действия и решения.

Неотказуемость — способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение.

Достоверность — свойство соответствия предусмотренному поведению и результатам.

Система менеджмента информационной безопасности (СМИБ) — часть общей системы менеджмента, основанная на подходе бизнес-рисков

по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению информационной безопасности.

Риск – сочетание вероятности события и его последствий.

Угроза – возможная причина нежелательного инцидента, который может нанести ущерб системе или организации.

Уязвимость – слабое место актива или меры и средства контроля и управления, которое может быть использовано угрозой.

Основными принципами успешной реализации СМИБ согласно стандарту являются:

- ◆ понимание необходимости системы ИБ;
- ◆ назначение ответственных за информационную безопасность;
- ◆ соединение административных обязанностей и интересов заинтересованных лиц;
- ◆ оценка риска, определяющая соответствующие меры и средства контроля и управления для достижения допустимых уровней риска;
- ◆ безопасность как неотъемлемый существенный элемент информационных сетей и систем;
- ◆ активное предупреждение и выявление инцидентов ИБ;
- ◆ обеспечение комплексного подхода к менеджменту ИБ;
- ◆ непрерывная переоценка и соответствующая модификация системы ИБ.

В стандарте приведена краткая характеристика процессного подхода для СМИБ «План – Осуществление – Проверка – Действие». Элементы такого подхода означают:

- ◆ план – постановка целей и разработка планов (проанализировать ситуацию в организации, наметить общие цели, поставить задачи и разработать планы для их достижения);
- ◆ осуществление – реализация планов;
- ◆ проверка – проверка результатов (измерение/контроль степени соответствия достигнутых результатов плану);
- ◆ действие – коррекция и улучшение работы.

Организация должна предпринимать следующие меры по внедрению, контролю, поддержке и улучшению ее СМИБ:

- ◆ определение информационных активов и связанных с ними требований безопасности;
- ◆ оценка рисков информационной безопасности;

- ◆ выбор и реализация соответствующих средств управления для управления неприемлемыми рисками;
- ◆ контроль, поддержка и повышение эффективности средств управления безопасностью, связанных с информационными активами организации.

3.5.3. Национальный стандарт ГОСТ Р ИСО/МЭК 27001–2006 – требования к СМИБ

Национальный стандарт ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» введен в действие 01.02.2008 г. Он идентичен международному стандарту ISO/IEC 27001:2005.

Стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности.

Стандарт использует процессный подход для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации. Схема такого подхода изображена в стандарте и представлена на рис. 3.4.

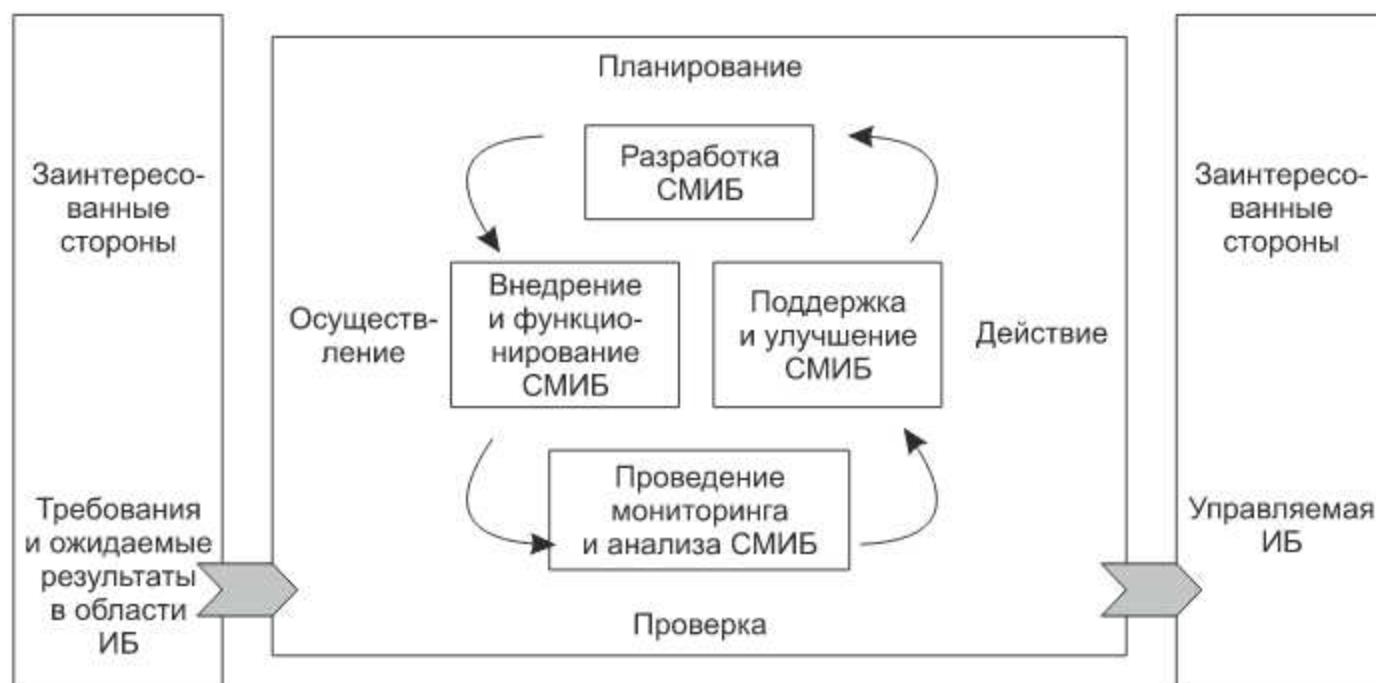


Рис. 3.4. Модель процессного подхода

Для разработки СМИБ организация должна:

- ◆ определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий;
- ◆ определить политику СМИБ;
- ◆ определить подход к оценке риска в организации;
- ◆ идентифицировать риски;
- ◆ проанализировать и оценить риски;
- ◆ определить и оценить различные варианты обработки рисков;
- ◆ выбрать цели и меры управления для обработки рисков.

Стандарт дает рекомендации в отношении конкретных мер:

- ◆ по внедрению и функционированию СМИБ;
- ◆ мониторингу и анализу СМИБ;
- ◆ поддержке и улучшению СМИБ.

Руководство организации должно:

- ◆ разработать политику СМИБ;
- ◆ обеспечить разработку целей и планов СМИБ;
- ◆ определить функции и ответственность в области ИБ;
- ◆ довести до всех сотрудников организации информацию о важности достижения целей ИБ, об их ответственности перед законом, а также о необходимости непрерывного совершенствования в реализации мер ИБ;
- ◆ выделить необходимые и достаточные ресурсы для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ;
- ◆ установить критерии принятия рисков и уровни их приемлемости;
- ◆ обеспечить проведение внутренних аудитов СМИБ;
- ◆ проводить анализ СМИБ.

В приложении к стандарту приведен перечень примерных мер управления и контроля, который должен быть осуществлен для реализации и управления СМИБ:

- ◆ разработка политики ИБ, ее пересмотр и реализация;
- ◆ организация информационной безопасности (организационные меры управления);
- ◆ управление активами;

- ◆ правила безопасности, связанные с персоналом;
- ◆ физическая защита и защита от воздействия окружающей среды (включая безопасность оборудования);
- ◆ управление средствами коммуникаций и их функционированием;
- ◆ контроль доступа (к информации, сервисам, устройствам и т. п.);
- ◆ меры при разработке, внедрении и обслуживании информационных систем;
- ◆ управление инцидентами ИБ;
- ◆ управление непрерывностью бизнеса;
- ◆ соответствие требованиям (нормативно-правовым документам, политикам и стандартам).

3.5.4. Национальный стандарт ГОСТ Р ИСО/МЭК 27002–2012 – свод норм и правил СМИБ

Национальный стандарт ГОСТ Р ИСО/МЭК 27002–2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» введен в действие 01.01.2014 г. взамен ранее принятого стандарта ГОСТ Р ИСО/МЭК 17799–2005. Он идентичен международному стандарту ISO/IEC 27002:2005.

Стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации. Цели, изложенные в нем, обеспечивают полное руководство общепринятыми целями менеджмента информационной безопасности.

Стандарт состоит из следующих разделов, посвященных мерам и средствам контроля и управления безопасности:

- ◆ политика безопасности;
- ◆ организационные аспекты информационной безопасности;
- ◆ менеджмент активов;
- ◆ безопасность, связанная с персоналом;
- ◆ физическая защита и защита от воздействия окружающей среды;
- ◆ менеджмент коммуникаций и работ;
- ◆ управление доступом;
- ◆ приобретение, разработка и эксплуатация ИС;
- ◆ менеджмент инцидентов информационной безопасности;

- ◆ менеджмент непрерывности бизнеса;
- ◆ соответствие.

Кроме того, стандарт дает рекомендации по оценке и обработке рисков. Оценка рисков должна идентифицировать риски, определить количество и приоритеты рисков на основе критериев для принятия риска и целей, значимых для организации. Оценивать риски следует периодически, чтобы учитывать изменения в требованиях безопасности и в ситуации, связанной с риском.

В отношении каждого из выявленных рисков вслед за его оценкой необходимо принимать решение по обработке, которая включает в себя:

- ◆ применение соответствующих мер и средств контроля и управления для снижения рисков;
- ◆ сознательное и объективное принятие рисков в том случае, если они удовлетворяют политике и критериям организации в отношении принятия рисков;
- ◆ предотвращение рисков путем недопущения действий, которые могут стать причиной возникновения рисков.

Стандарт дает рекомендации по разработке и реализации политики информационной безопасности организации. Политика должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций. Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности и содержать положения относительно:

- ◆ определения ИБ, ее общих целей и сферы действия;
- ◆ изложения намерений руководства, поддерживающих цели и принципы ИБ в соответствии со стратегией и целями бизнеса;
- ◆ подхода к установлению мер и средств контроля и управления и целей их применения, включая структуру оценки риска и менеджмента риска;
- ◆ краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия;
- ◆ определения общих и конкретных обязанностей сотрудников в рамках менеджмента ИБ, включая информирование об инцидентах безопасности;
- ◆ ссылок на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо если произошли значительные изменения внутри организации или в ее окружении.

В организационном плане стандарт рекомендует необходимость создания структуры менеджмента для инициирования и контроля обеспечения ИБ в организации. Высшее руководство должно назначать ответственных лиц в области политики ИБ, а также координировать и анализировать внедрение информационной безопасности в организации. Следует четко определять обязанности по защите отдельных активов и выполнению конкретных процессов, связанных с информационной безопасностью.

В стандарте даны рекомендации по включению в соглашения о конфиденциальности полученной информации ряда сведений:

- ◆ определение информации, подлежащей защите;
- ◆ предполагаемый срок действия соглашения;
- ◆ необходимые действия при окончании срока действия соглашения;
- ◆ обязанности и действия лиц, подписавших соглашение;
- ◆ разрешенное использование конфиденциальной информации и права лиц, подписавших соглашение, в отношении использования информации;
- ◆ право подвергать аудиту и мониторингу деятельность, связанную с конфиденциальной информацией;
- ◆ процедуру предупреждения и сообщения о несанкционированном разглашении или нарушениях, связанных с конфиденциальной информацией;
- ◆ условия возврата или уничтожения информации в случае приостановления действия соглашения;
- ◆ предполагаемые действия, которые должны быть предприняты в случае нарушения данного соглашения.

В стандарте предусмотрено также применение соответствующих процедур, определяющих, когда и с какими инстанциями (правоохранительными, пожарными надзорными органами и т. п.) необходимо вступить в контакт и каким образом следует своевременно сообщать о выявленных инцидентах информационной безопасности, если есть подозрение о возможности нарушения закона.

В плане реализации организационных мероприятий стандарт дает рекомендации по аспектам взаимодействия со сторонними организациями (идентификация рисков от сторонних организаций, вопросы безопасности при работе с клиентами и при заключении договоров с третьей стороной).

Все активы организации должны быть определены и иметь назначенного владельца, отвечающего за его защиту.

В плане обеспечения безопасности, связанной с персоналом, стандарт рекомендует для всех сотрудников и подрядчиков четко определять роли и обязанности в области ИБ и оформлять их документально. В организации должен существовать формальный дисциплинарный процесс, применяемый в отношении сотрудников, нарушивших безопасность.

Для всех кандидатов на постоянную работу и подрядчиков должна проводиться проверка согласно соответствующим законам, инструкциям и правилам этики пропорционально требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и предполагаемым рискам.

Целями обеспечения физической безопасности и защиты от воздействий окружающей среды является предотвращение неавторизованного физического доступа, повреждения и воздействия в отношении помещений и информации организации. Уровень защищенности должен быть соразмерен выявленным рискам.

Целью менеджмента коммуникаций и работ является обеспечение уверенности в надлежащем и безопасном функционировании средств обработки информации. Должны быть установлены обязанности и процедуры в отношении управления и эксплуатации всех средств обработки информации, включая разработку соответствующих эксплуатационных процедур. Здесь же следует обратить внимание на защиту информации в сетях и защиту поддерживающей сетевой инфраструктуры, включая меры и средства контроля сетей и управления ими и обеспечение безопасности сетевых услуг.

Должны быть определены также соответствующие процедуры и средства контроля и управления в отношении обработки и хранения информации и обмена ею при использовании средств связи, защиты документов, компьютерных носителей информации и системной документации от неавторизованного раскрытия, модификации, выноса и уничтожения.

Доступ к информации, средствам обработки информации и процессам бизнеса должен быть управляемым с учетом требований бизнеса и безопасности. Правила управления доступом и права каждого пользователя или группы пользователей должны быть четко сформулированы в политике управления доступом.

Стандарт дает подробные рекомендации в области управления доступа:

- ◆ к сети и сетевым устройствам;
- ◆ эксплуатируемым информационным системам;
- ◆ информации и прикладным программам;
- ◆ средствам мобильной вычислительной техники и связи.

Один из разделов стандарта посвящен мерам и средствам контроля безопасности и управления ею при приобретении, разработке и эксплуатации информационных систем, включая использование криптографических средств, аутсорсинг разработки программного обеспечения, управление техническими уязвимостями.

В качестве одной из важнейших мер управления инцидентами ИБ стандарт рекомендует устанавливать обязанности должностных лиц по обеспечению быстрого, эффективного и应及时ного реагирования на инциденты информационной безопасности. Должны быть созданы механизмы, позволяющие установить типы, объемы и убытки, вызванные инцидентами ИБ, с целью извлечения соответствующих уроков и принятия дополнительных мер управления.

При внедрении СМИБ необходимо обеспечить соответствие требованиям законодательства, стандартам, утвержденным политиками безопасности.

3.5.5. Национальный стандарт ГОСТ Р ИСО/МЭК 27003–2012 – реализация СМИБ

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27003–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности» введен в действие 01.12.2013 г. Он идентичен международному стандарту ISO/IEC 27003:2010.

В стандарте рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения системы менеджмента информационной безопасности в соответствии со стандартом ИСО/МЭК 27001. Он предназначен для использования в сочетании со стандартами 27001 и 27002.

Внедрение СМИБ является важным видом деятельности и обычно осуществляется в организации как проект. Процесс внедрения СМИБ согласно стандарту включает пять фаз.

1. Получение одобрения руководства для запуска проекта СМИБ.
2. Определение области действия и политики СМИБ.
3. Анализ организации.
4. Анализ рисков и планирование обработки рисков.
5. Разработка СМИБ.

Область действия СМИБ определяется с помощью ответов на следующие вопросы:

- ◆ Что является важнейшими сферами деятельности предприятия и организации?
- ◆ Какие у организации существуют взаимоотношения и соглашения с третьими сторонами?
- ◆ Какая информация является наиболее важной для организации?
- ◆ Какими могли бы быть возможные последствия при разглашении определенной информации?
- ◆ Какие законы, контрактные соглашения и отраслевые требования, относящиеся к ИБ, применяются в организации?
- ◆ Какие нужны виды защиты и от каких угроз?
- ◆ Для каких отдельных категорий информации требуется защита?
- ◆ Каковы отдельные типы информационной деятельности, требующие защиты?

Окончательный документ, описывающий область действия и границы СМИБ, должен содержать следующую информацию:

- ◆ ключевые характеристики организации;
- ◆ процессы в организации, находящиеся в области действия СМИБ;
- ◆ конфигурация оборудования и сетей, находящихся в области действия СМИБ;
- ◆ перечень активов, находящихся в области действия СМИБ;
- ◆ схемы объектов, находящихся в области действия СМИБ, определяющие физические границы СМИБ;
- ◆ описание ролей и сфер ответственности в рамках СМИБ и их связи со структурой организации.

На этапе внедрения СМИБ необходимо проанализировать текущее состояние ИБ и определить подробные требования к ней. Стандарт рекомендует разработать политику информационной безопасности, которая документирует стратегическую позицию организации в отношении ИБ.

Организация может иметь несколько политик, по одной для каждой сферы деятельности. Политика безопасности организации является политикой высшего уровня. Она подкрепляется более конкретными политиками, включая политику ИБ и политику системы менеджмента ИБ. В свою очередь, политика ИБ может подкрепляться более детальными политиками по конкретным предметам, относящимся к аспектам ИБ (контроля доступа, использования сетевых служб, криптографических средств, резервного копирования, лицензирования программного обеспечения и т. п.).

Стандарт рекомендует следующую структуру политик.

1. Краткое изложение политики – общее описание из одного-двух предложений (иногда может объединяться с введением).
2. Введение – краткое объяснение предмета политики.
3. Область действия – описание частей или действий организации, находящихся под влиянием политики. При необходимости в этом пункте перечисляются другие политики, подкрепляемые данной политикой.
4. Цели – описание назначения политики.
5. Принципы – описание правил, касающихся действий и решений, принимаемых для достижения целей. В некоторых случаях может быть полезно определить ключевые процессы, связанные с предметом политики, и затем правила выполнения процессов.
6. Сфера ответственности – кто отвечает за действия по выполнению требований политики. В некоторых случаях этот пункт может содержать описание организационных соглашений, а также сферы ответственности лиц с определенными ролями.
7. Ключевые результаты – описание результатов, получаемых предприятием, если цели достигнуты.
8. Связанные политики – описание других политик, относящихся к достижению целей, обычно с представлением дополнительных подробностей, касающихся отдельных предметов.

Внедрение СМИБ должно периодически оцениваться путем внутреннего или независимого аудита.

Внутренний аудит должен осуществляться для оценки соответствия СМИБ требованиям ГОСТ 27001, законам, нормам и требованиям к ИБ, касающимся того, эффективно ли они внедряются и поддерживаются. Аудит не проводится сотрудниками, которые были заняты в планировании и разработке целей безопасности, поскольку сложно найти собственные ошибки. В качестве аудиторов руководство должно привлекать подразделения организации или сотрудников, находящихся вне области действия внутреннего аудита СМИБ.

Когда организация привлекает внешних аудиторов, следует принять во внимание следующее: внешние аудиторы хорошо знакомы с процедурой внутреннего аудита СМИБ, однако не обладают достаточными знаниями об организационной среде организации. Эта информация должна быть им предоставлена.

При проведении аудита следует руководствоваться документом ГОСТ Р ИСО/МЭК 27006–2008 «Требования к организациям, проводящим аудит и сертификацию СМИБ».

В стандарте приведен пример документа «Политика информационной безопасности».

Краткое изложение политики

Информация всегда должна быть защищена независимо от ее формы и способа распространения, передачи и хранения.

Введение

Информация может существовать во многих формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных устройств, показываться на пленках или передаваться устно в процессе общения.

Информационная безопасность – это защита информации от различных угроз, призванная обеспечить непрерывность бизнес-процессов, минимизировать риск для бизнеса, максимизировать возвращение вложений и обеспечить возможности деловой деятельности.

Область действия

Данная политика подкрепляет общую политику безопасности организации. Данная политика применяется ко всем сотрудникам организации.

Цели информационной безопасности

- ◆ Понимание и обработка стратегических и оперативных рисков для информационной безопасности так, чтобы они были приемлемы для организации.
- ◆ Защита конфиденциальности информации клиентов, разработок продукции и планов маркетинга.
- ◆ Сохранение целостности материалов бухгалтерского учета.
- ◆ Соответствие общих веб-сервисов и внутренних сетей стандартам доступности.

Принципы информационной безопасности

- ◆ Данная организация способствует принятию рисков и преодолевает риски, которые не могут преодолеть организации с консервативным управлением, при условии понимания, мониторинга и обработки рисков для информации при необходимости. Подробное описание подходов, применяемых для оценки и обработки рисков, можно найти в политике СМИБ.
- ◆ Весь персонал должен быть осведомлен об информационной безопасности в отношении своих должностных обязанностей и подотчетен.
- ◆ Необходимо принять меры для финансирования средств управления информационной безопасностью и процессов управления проектами.

- ◆ Возможности мошенничества и злоупотреблений в области информационных систем должны быть приняты в расчет при общем управлении информационными системами.
- ◆ Отчеты о состоянии информационной безопасности должны быть доступны.
- ◆ Необходимо отслеживать риски для информационной безопасности и предпринимать действия, когда изменения приводят к возникновению непредвиденных рисков.
- ◆ Критерии классификации рисков и приемлемости рисков можно найти в политике СМИБ.
- ◆ Ситуации, которые могут привести организацию к нарушению законов и установленных норм, допускаться не должны.

Сфера ответственности

- ◆ Группа руководителей высшего звена отвечает за обеспечение соответствующей проработки информации во всей организации.
- ◆ Каждый руководитель высшего звена отвечает за то, чтобы сотрудники, работающие под его руководством, осуществляли защиту информации в соответствии со стандартами организации.
- ◆ Начальник отдела безопасности консультирует группу руководителей высшего звена, оказывает экспертную помощь сотрудникам организации и обеспечивает доступность отчетов о состоянии информационной безопасности.
- ◆ Каждый сотрудник организации отвечает за информационную безопасность как часть выполнения своих должностных обязанностей.

Ключевые результаты

- ◆ Инциденты информационной безопасности не должны приводить к серьезным непредвиденным затратам или серьезным срывам работы служб и деятельности предприятия.
- ◆ Потери из-за мошенничества должны быть известны и находиться в рамках приемлемых ограничений.
- ◆ Вопросы информационной безопасности не должны неблагоприятно влиять на прием заказчиками продукции и услуг.

Связанные политики

Следующие детальные политики содержат принципы и рекомендации по отдельным аспектам информационной безопасности:

- ◆ политика системы менеджмента информационной безопасности;

- ◆ политика контроля доступа;
- ◆ политика чистого стола и чистого экрана;
- ◆ политика неразрешенного программного обеспечения;
- ◆ политика, касающаяся получения файлов программного обеспечения из внешних сетей или через них;
- ◆ политика, касающаяся мобильного кода;
- ◆ политика резервного копирования;
- ◆ политика, касающаяся обмена информацией между организациями;
- ◆ политика, касающаяся допустимого использования электронных средств связи;
- ◆ политика сохранения записей;
- ◆ политика использования сетевых служб;
- ◆ политика, касающаяся мобильных вычислений и связи;
- ◆ политика дистанционной работы;
- ◆ политика использования криптографического контроля;
- ◆ политика соответствия;
- ◆ политика лицензирования программного обеспечения;
- ◆ политика удаления программного обеспечения;
- ◆ политика защиты и секретности данных.

Все эти политики подкрепляют:

- ◆ идентификацию риска путем предоставления основных средств управления, которые могут использоваться для обнаружения недостатков в проектировании и внедрении систем;
- ◆ обработку риска путем оказания помощи в определении способов обработки для определенных уязвимостей и угроз.

3.5.6. Национальный стандарт ГОСТ Р ИСО/МЭК 27004–2011 – измерения в СМИБ

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27004–2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения» введен в действие 01.01.2012 г. Он идентичен международному стандарту ISO/IEC 27004:2009.

Стандарт содержит рекомендации по разработке и использованию измерений и мер измерения для оценки эффективности реализованной СМИБ, а также мер и средств контроля и управления по ИСО/МЭК 27001.

Процесс измерений затрагивает политику, менеджмент риска информационной безопасности, меры и средства контроля и управления и цели их применения, процессы и процедуры, а также поддерживает процесс проверки СМИБ. Он реализуется в виде программы измерений, предназначеннной для оказания помощи руководству организации в выявлении и оценивании не соответствующих требованием и неэффективных процессов, мер, средств контроля и управления СМИБ.

Отправной точкой для разработки мер измерения и измерений являются доскональное понимание рисков ИБ, с которыми сталкивается организация, и корректное выполнение организацией действий по оценке риска в соответствии с требованиями ИСО/МЭК 27001.

Стандарт предлагает рекомендации, касающиеся следующей деятельности:

- ◆ разработка мер измерений;
- ◆ разработка и выполнение программы измерений;
- ◆ сбор и анализ данных;
- ◆ обработка результатов измерений;
- ◆ сообщение обработанных результатов измерений заинтересованным сторонам;
- ◆ использование результатов измерений для принятия решений, относящихся к СМИБ;
- ◆ использование результатов измерений для выявления потребностей в совершенствовании реализованной СМИБ;
- ◆ содействие постоянному совершенствованию программы измерений.

В структуре стандарта выделены следующие разделы:

- ◆ общий обзор программы измерений и модели измерений, связанных с информационной безопасностью;
- ◆ обязанности руководства в отношении измерений, связанных с информационной безопасностью;
- ◆ конструктивные элементы и процессы измерений, подлежащие реализации в рамках программы измерений.

Организация через запланированные интервалы времени должна оценивать эффективность реализованной программы измерений и полезность результатов измерений.

3.5.7. Национальный стандарт ГОСТ Р ИСО/МЭК 27005–2010 – менеджмент риска ИБ

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» введен в действие 01.12.2011 г. взамен двух ранее принятых стандартов, ГОСТ Р ИСО/МЭК 13335-3–2007 и ГОСТ Р ИСО/МЭК 13335-4–2007. Он идентичен международному стандарту ISO/IEC 27005:2008.

Стандарт представляет собой руководство по менеджменту риска информационной безопасности и поддерживает общие концепции, определенные в ИСО/МЭК 27001. Он предназначен для руководителей и персонала, занимающегося в организации вопросами менеджмента риска информационной безопасности.

Стандарт содержит описание процесса менеджмента риска ИБ и связанных с ним видов деятельности:

- ◆ установление контекста;
- ◆ оценка риска;
- ◆ обработка риска;
- ◆ принятие риска;
- ◆ коммуникация риска;
- ◆ мониторинг и переоценка риска.

Процесс менеджмента риска информационной безопасности изображен на рис. 3.5 так, как он представлен в стандарте.

Установление контекста менеджмента риска ИБ включает определение основных критериев, необходимых для менеджмента риска ИБ, определение области применения и границ, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ.

Как видно из рисунка, в процессе менеджмента риска ИБ процедуры оценки риска и обработки риска могут выполняться итеративно. Сначала устанавливается контекст, а затем оценивается риск. Если при этом удается получить информацию, достаточную для эффективного определения действий, требуемых для снижения риска до приемлемого уровня, то задача выполнена, после чего следует обработка риска. Если же информации недостаточно, выполняется очередная итерация оценки риска в условиях пересмотренного контекста (например, критериев оценки рисков, принятия рисков) (первая точка принятия решения).

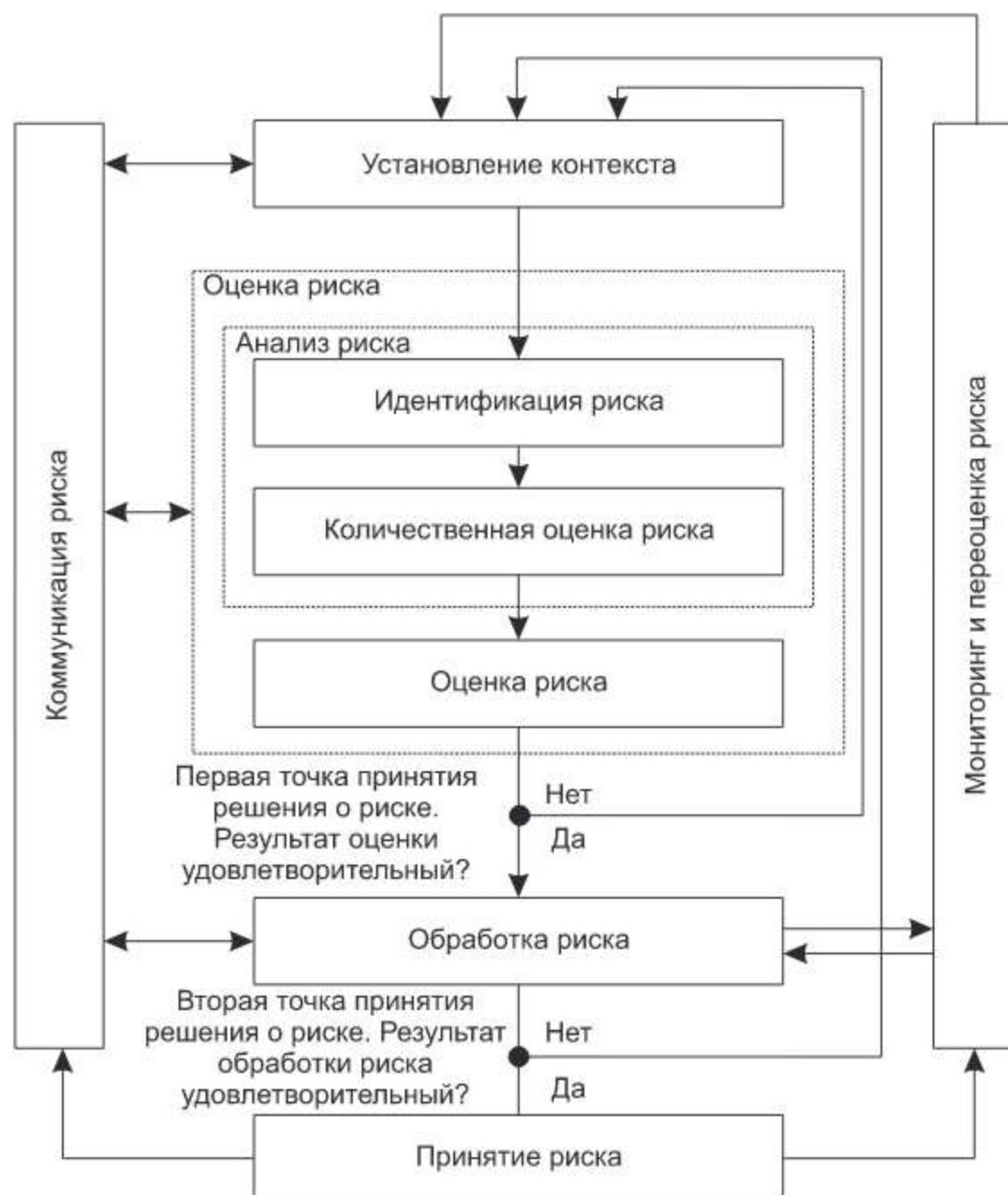


Рис. 3.5. Процесс менеджмента риска ИБ

Эффективность обработки риска зависит от результатов оценки риска. Обработка риска может не обеспечить сразу же приемлемый уровень остаточного риска. В этой ситуации потребуется, если необходимо, еще одна итерация оценки риска с измененными параметрами контекста, за которой последует очередная процедура обработки риска (вторая точка принятия решения).

На рис. 3.6 иллюстрируется деятельность по обработке риска в рамках процесса менеджмента риска ИБ так, как это представлено в стандарте.

Для процесса менеджмента риска ИБ необходимо устанавливать и поддерживать организационную структуру и распределение обязанностей. Далее перечисляются основные роли и области ответственности, присущие этой организационной структуре.

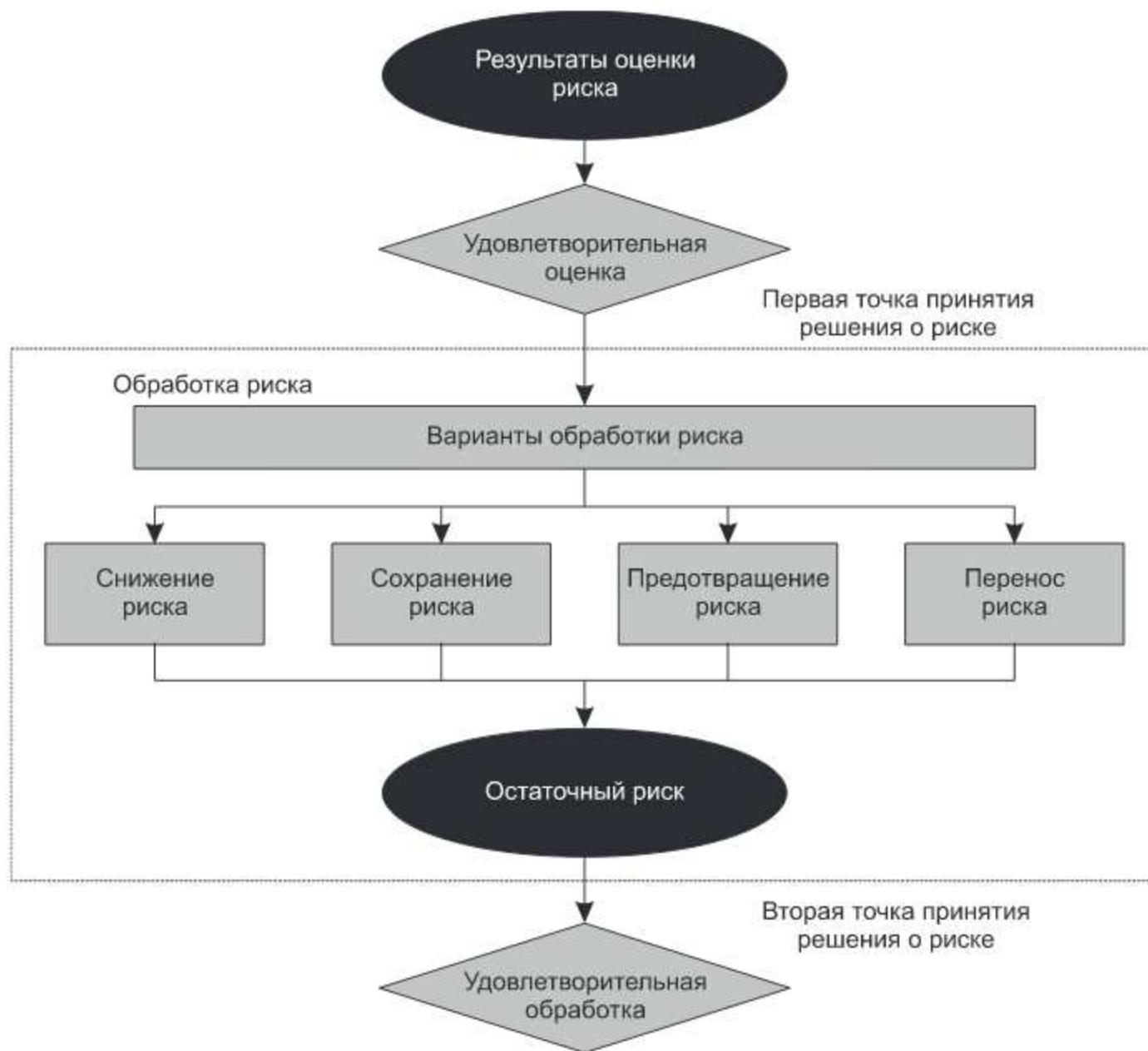


Рис. 3.6. Деятельность по обработке риска. Выявление и изучение причастных сторон

- ◆ Разработка процесса менеджмента риска ИБ, подходящего для данной организации.
- ◆ Определение ролей и обязанностей всех сторон, как внутренних, так и внешних по отношению к организации.
- ◆ Установление требуемых взаимосвязей между организацией и причастными сторонами, а также взаимодействия с другими значимыми проектами и видами деятельности.
- ◆ Определение путей передачи принятий решений на более высокий уровень и/или другим специалистам.
- ◆ Определение подлежащих ведению документов.

Вся информация о рисках, полученная в результате деятельности по менеджменту риска, должна подвергаться мониторингу и переоценке.

Организации должны обеспечивать проведение непрерывного мониторинга следующих факторов:

- ◆ новых активов, которые были включены в область действия менеджмента риска;
- ◆ необходимой модификации ценности активов, например, вследствие изменившихся бизнес-требований;
- ◆ новых угроз, которые могут действовать вне и внутри организации и которые еще не были оценены;
- ◆ вероятности того, что новые или возросшие уязвимости могут сделать возможным использование их угрозами;
- ◆ выявленных уязвимостей для определения тех из них, которые становятся подверженными новым или повторно возникающим угрозам;
- ◆ возросшего влияния или последствий оцененных угроз, уязвимостей и рисков, объединенное действие которых имеет результатом неприемлемый уровень риска;
- ◆ инцидентов ИБ.

Таким образом, процесс менеджмента риска ИБ подлежит постоянному мониторингу, анализу и улучшению.

3.5.8. Национальные стандарты в области аудита СМИБ (ГОСТ 27006–2008, ГОСТ 27007–2014)

В области аудита СМИБ в настоящее время действуют два стандарта.

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27006–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» введен в действие 01.10.2009 г. Он идентичен международному стандарту ISO/IEC 27006:2007.

Стандарт устанавливает требования к органам, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности, и способствует проведению аккредитации органов сертификации.

Под органом сертификации в стандарте понимается третья сторона, оценивающая и сертифицирующая СМИБ организации-клиента на соответствие действующим стандартам.

Стандарт содержит следующие разделы.

1. Принципы.
2. Общие требования (юридические и договорные вопросы, менеджмент беспристрастности, обязательства и финансирование).

3. Требования к структуре (структура организации и руководство, комитет по обеспечению защиты беспристрастности).
4. Требования к ресурсам (компетентность руководства и персонала, а также персонала, участвующего в сертификации, привлечение внешних аудиторов и экспертов, аутсорсинг).
5. Требования к информации (общедоступная информация, документы по сертификации, список сертифицированных клиентов, конфиденциальность, обмен информацией между органом сертификации и его клиентами).
6. Требования к процессу (общие требования к аудиту, время аудита, методология аудита, первоначальный аудит и сертификация, деятельность по надзору, повторная сертификация, специальный аудит, приостановка, отмена и сокращение сферы действия сертификата, апелляции, документы заявителей).
7. Требования системы менеджмента к органам сертификации.

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27007–2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности» введен в действие 01.06.2015 г. Он идентичен международному стандарту ISO/IEC 27007:2011.

Стандарт представляет руководство по менеджменту программы аудита системы менеджмента информационной безопасности и проведению внутреннего или внешнего аудита на соответствие ИСО/МЭК 27001, а также руководство по вопросу компетентности и оценки аудиторов СМИБ.

В стандарте рассматриваются:

- ◆ принципы аудита;
- ◆ менеджмент программы аудита;
- ◆ проведение аудита;
- ◆ компетентность и оценка аудиторов;

В приложении к стандарту дано практическое руководство по аудиту системы менеджмента ИБ.

Оба стандарта используют нормативные ссылки на следующие стандарты:

- ◆ ИСО/МЭК 17021–2012 «Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента»;
- ◆ ГОСТ Р ИСО 19011–2012 «Руководящие указания по аудиту систем менеджмента».

3.5.9. Национальный стандарт по СМИБ в телекоммуникационных организациях (ГОСТ 27011–2014)

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27011–2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002» введен в действие 01.01.2014 г. Он идентичен международному стандарту ISO/IEC 27011:2008.

Стандарт определяет рекомендации, поддерживающие реализацию менеджмента информационной безопасности в телекоммуникационных организациях на основе ИСО/МЭК 27002. Под телекоммуникационной организацией в стандарте понимается коммерческая организация, предоставляющая телекоммуникационные услуги с целью удовлетворения потребностей других лиц.

Помимо целей безопасности, мер и средств контроля и управления, описанных в ИСО/МЭК 27002, телекоммуникационные организации должны принимать во внимание следующие аспекты безопасности: конфиденциальность, целостность и доступность.

Конфиденциальность означает неразглашение сведений о наличии, содержании, источнике, адресе назначения, а также дате и времени переданной информации.

Целостность подразумевает обеспечение уверенности в подлинности, точности и полноте информации, переданной, отправленной или полученной с помощью проводной связи, радиосвязи или любыми другими способами.

Доступность подразумевает обеспечение только санкционированного доступа к телекоммуникационной информации, оборудованию и среде, которые используются для предоставления услуг связи.

Стандарт определяет следующие источники требований к безопасности в телекоммуникациях:

- ◆ клиенты/абоненты, нуждающиеся в доверии к сетям и предоставляемым услугам, включая доступность услуг в случае серьезных катастроф;
- ◆ органы государственной власти, требующие обеспечения безопасности в соответствии с нормами и законами;
- ◆ сетевые операторы и поставщики услуг, нуждающиеся в обеспечении безопасности для защиты своих практических интересов, а также выполнения своих обязательств перед клиентами и обществом.

Кроме того, телекоммуникационные организации должны учитывать следующие инциденты, связанные с окружающей средой и безопасностью эксплуатации.

- ◆ Телекоммуникационные услуги сильно зависят от различных взаимосвязанных средств связи (маршрутизаторов, коммутаторов, серверов и т. п.), следовательно, проблемы безопасности телекоммуникаций могут возникать в различном оборудовании и быстро распространяться через сеть на другое оборудование.
- ◆ В дополнение к телекоммуникационным средствам к серьезным нарушениям безопасности могут приводить также уязвимости сетевых протоколов и топологии сети.
- ◆ Основное беспокойство телекоммуникационных организаций вызывает вероятность компрометации безопасности, ведущая к простою сети, который может быть очень дорогостоящим с точки зрения отношений с клиентами, упущеной выгоды и расходов на восстановление. Умышленные атаки, нацеленные на доступность национальной телекоммуникационной инфраструктуры, могут рассматриваться как проблема национальной безопасности.
- ◆ Системы и сети управления телекоммуникациями уязвимы для проникновения хакеров.
- ◆ Организации, предоставляющие услуги связи, помимо внешних проникновений озабочены компрометацией безопасности из внутренних источников — со стороны неуполномоченного персонала.

Характерные для телекоммуникационного сектора рекомендации и информация рассматриваются в следующих разделах стандарта:

- ◆ организационные аспекты информационной безопасности;
- ◆ менеджмент активов;
- ◆ безопасность, связанная с персоналом;
- ◆ физическая безопасность и защита от воздействий окружающей среды;
- ◆ менеджмент коммуникаций и работ;
- ◆ управление доступом;
- ◆ приобретение, разработка и эксплуатация информационных систем;
- ◆ менеджмент инцидентов информационной безопасности;
- ◆ менеджмент непрерывности бизнеса.

3.6. Стандарты серии 27033 по безопасности сетей

3.6.1. Общие замечания

В современном мире информационные системы большинства организаций связаны сетями, при этом сетевые соединения могут относиться к одному или нескольким видам, представленным на рис. 3.7 (как они изображены в стандарте):

- ◆ в пределах организации;
- ◆ между различными организациями;
- ◆ между организацией и неограниченным кругом лиц.



Рис. 3.7. Виды сетевых соединений

Использование сетевых технологий, в том числе глобальной информационно-телекоммуникационной сети Интернет, обеспечивает новые широкие возможности для ведения бизнеса и получения значительных преимуществ. Однако наряду с преимуществами появляются новые риски безопасности, которые могут оказывать существенное неблагоприятное влияние на деятельность организаций, а следовательно, требуют управления. Поэтому одним из важнейших требований при использовании сетевых технологий является обеспечение адекватной защиты сетей, информационных систем, сетевых сервисов и обрабатываемой информации.

Назначение стандартов серии ИСО/МЭК 27033 состоит в том, чтобы представить подробные рекомендации по аспектам безопасности менеджмента, функционирования и использования сетей информационных систем и их соединений. Они представляют дополнительные детализированные рекомендации по реализации мер и средств контроля и управления сетевой безопасностью, определенных в базовом стандарте ИСО/МЭК 27002.

Структура стандартов серии ИСО/МЭК 27033 описана в его первой части и представлена на рис. 3.8. Как видно из рисунка, стандарт состоит из нескольких частей, целями которых являются:

- ◆ для ИСО/МЭК 27033-1 «Обзор и концепция» — определение и описание концепций, связанных с сетевой безопасностью, и представление рекомендаций по менеджменту сетевой безопасности. Стандарт содержит общий обзор сетевой безопасности и связанных с ней определений, рекомендации по идентификации и анализу рисков сетевой безопасности и, кроме того, определение требований сетевой безопасности;

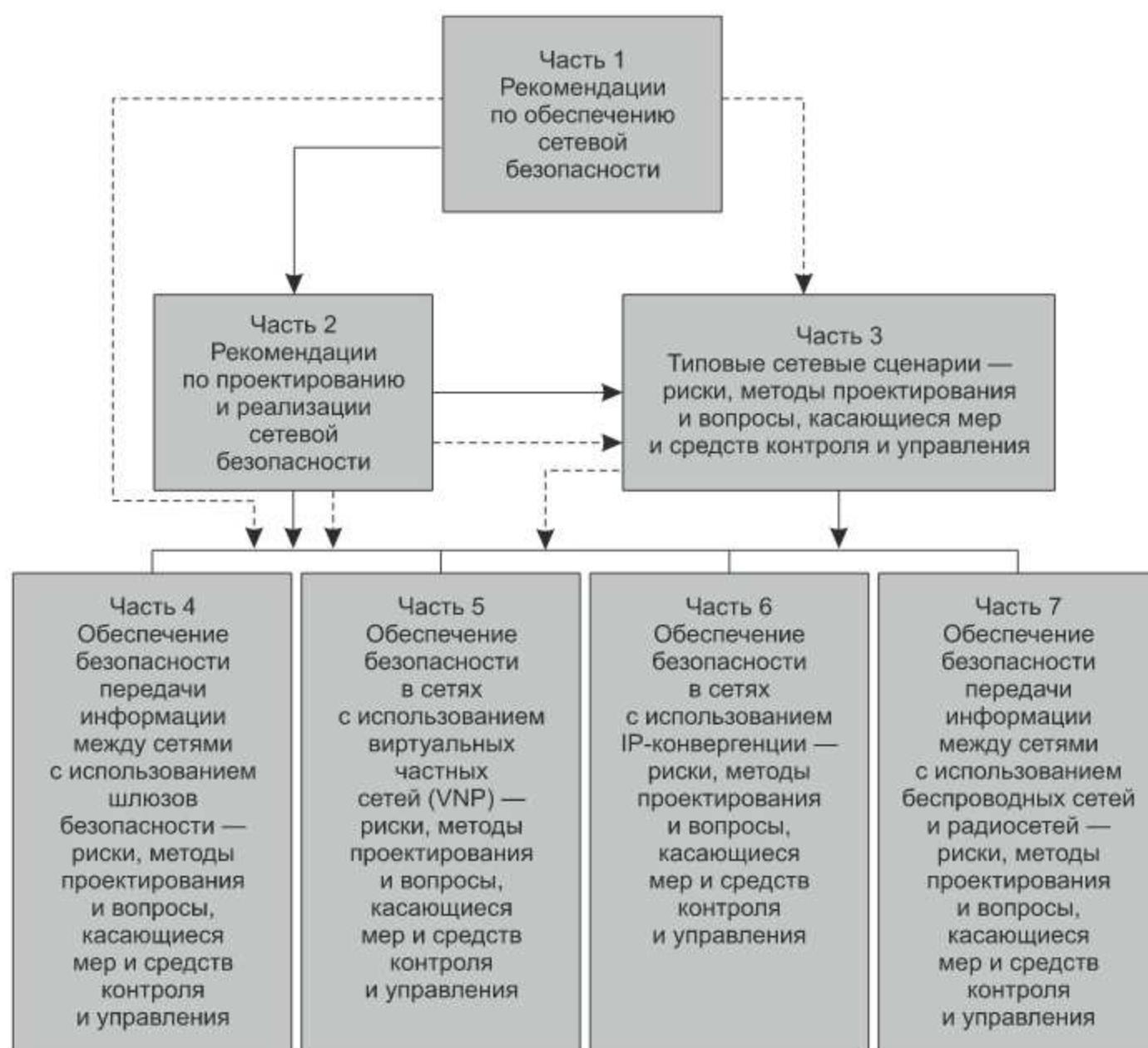


Рис. 3.8. Структура стандартов серии ИСО/МЭК 27033

- ◆ для ИСО/МЭК 27033-2 «Рекомендации по проектированию и реализации сетевой безопасности» — определение того, каким образом организации должны добиваться требуемого качества специализированных архитектур сетевой безопасности, проектирования и реализации, которые обеспечат уверенность в сетевой безопасности, соответствующей их среде деятельности. Данный стандарт предназначен для всего персонала, вовлеченного в планирование, проектирование и реализацию аспектов архитектуры сетевой безопасности;
- ◆ для ИСО/МЭК 27033-3 «Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления для типовых сетевых сценариев» — определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, связанных с типовыми сетевыми сценариями.

Предполагается, что следующие части ИСО/МЭК 27033 будут рассматривать:

- ◆ ИСО/МЭК 27033-4 «Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления для обеспечения безопасности передачи информации между сетями с использованием шлюзов безопасности» — определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности информационных потоков между сетями с использованием шлюзов безопасности;
- ◆ ИСО/МЭК 27033-5 «Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления для обеспечения безопасности виртуальных частных сетей» — определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности соединений, установленных с использованием VPN;
- ◆ ИСО/МЭК 27033-6 «IP-конвергенция» — определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности сетей с IP-конвергенцией, то есть с конвергенцией данных, речи и видео;
- ◆ ИСО/МЭК 27033-7 «Беспроводная связь» — определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности беспроводных сетей и радиосетей.

Национальные стандарты серии 27033 идентичны международным стандартам серии ISO/IEC 27033. Сейчас в Российской Федерации в качестве национальных стандартов введены в действие только части 27033-1 и 27033-3. Остальные части находятся в процессе подготовки.

3.6.2. Национальный стандарт ГОСТ Р ИСО / МЭК 27033-1–2011 – обзор и концепции безопасности сетей

Национальный стандарт Российской Федерации ГОСТ Р ИСО /МЭК 27033-1–2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» введен в действие 01.01.2012 г. взамен стандарта ГОСТ Р ИСО/МЭК 18028-1–2008. Он идентичен международному стандарту ISO/IEC 27033-1:2009 «Information technology – Security techniques – Network security – Part 1: Overview and concepts».

Стандарт определяет и описывает концепции, связанные с сетевой безопасностью, и представляет рекомендации по менеджменту сетевой безопасности. Он также:

- ◆ представляет рекомендации по идентификации и анализу рисков сетевой безопасности и дает определение требований сетевой безопасности;
- ◆ представляет обзор мер и средств контроля и управления, поддерживающих специализированные архитектуры сетевой безопасности и связанные с ними технические меры и средства контроля и управления, а также технические и нетехнические меры и средства контроля и управления, применяемые не только к сетям;
- ◆ знакомит с тем, как добиться высокого качества специализированных архитектур сетевой безопасности, связанных с типичными сетевыми сценариями;
- ◆ содержит краткое рассмотрение вопросов, связанных с реализацией и функционированием мер и средств контроля и управления сетевой безопасностью, постоянным мониторингом и проверкой их реализации.

Стандарт содержит также обзор сетевых терминов.

Демилитаризованная зона – пограничный сегмент сети (также известный как защищенная подсеть), выполняющий функции нейтральной зоны между сетями.

Отказ в обслуживании – прекращение санкционированного доступа к ресурсам системы или задержка операций и функций системы, приводящее в итоге к потере доступности для авторизованных пользователей.

Интернет – глобальная система взаимосвязанных сетей общедоступного пользования.

ПРИМЕЧАНИЕ

В законе № 149-ФЗ дано следующее определение: «информационно-телекоммуникационная сеть – технологическая система, предназначенная для

передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники».

Интерсеть — совокупность взаимосвязанных сетей, называемая объединенной сетью, или просто интерсетью.

Инtranет — частная компьютерная сеть, использующая интернет-протоколы и возможность сетевого соединения для безопасного коллективного использования части информации или операций организации ее сотрудниками.

Экстранет — расширение сети интранет организации, особенно через инфраструктуру общедоступной сети, делающее возможным совместное использование ресурсов организацией, другими организациями и лицами, с которыми она имеет дело, с предоставлением ограниченного доступа к своей сети интранет.

Межсетевой экран — вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и обратно, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности.

Концентратор — сетевое устройство, которое функционирует на первом уровне эталонной модели взаимодействия открытых систем.

ПРИМЕЧАНИЕ

Сетевые концентраторы не являются интеллектуальными устройствами, они обеспечивают только точки физического соединения для сетевых систем или ресурсов.

Коммутатор — устройство, обеспечивающее соединение сетевых устройств посредством внутренних механизмов коммутации, с технологией коммутации, обычно реализованной на втором или третьем уровне эталонной модели взаимодействия открытых систем.

Маршрутизатор — сетевое устройство, используемое для установления потоков данных между различными сетями и управления ими путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации.

Нарушитель — любое лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем и сетей или снижения доступности ресурсов информационной системы и сетевых ресурсов для законных пользователей.

Вторжение – несанкционированный доступ к сети или подсоединенной к сети системе, то есть преднамеренный или случайный несанкционированный доступ к информационной системе, включая злонамеренную деятельность против информационной системы или несанкционированное использование ресурсов в информационной системе.

Система обнаружения вторжений – специализированная система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования на вторжение в информационные системы и сети.

Вредоносное программное средство – программное средство, специально разработанное для повреждения или разрушения системы посредством нарушения ее конфиденциальности, целостности и/или доступности.

Сетевой менеджмент – процесс планирования, разработки, реализации, эксплуатации, мониторинга и поддержки сети.

Удаленный доступ – процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ.

Спам – незапрашиваемые сообщения электронной почты, содержание которых может быть вредоносным и/или мошенническим.

Спуфинг – маскировка под легального пользователя или сетевой ресурс.

Туннель – канал передачи данных между сетевыми устройствами, который устанавливают через существующую сетевую инфраструктуру.

Виртуальная локальная вычислительная сеть – независимая сеть, созданная с логической точки зрения внутри физической сети.

Сетевое администрирование – повседневная эксплуатация сети и управление сетевыми процессами и средствами, используемыми ею.

Сетевой анализатор – устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика.

Общий процесс достижения и поддержки необходимой сетевой безопасности стандарт определяет следующим образом:

- ◆ определение области/контекста, а затем оценка рисков безопасности (сбор информации о текущей и/или планируемой сетевой среде, идентификация и оценка рисков сетевой безопасности);
- ◆ идентификация поддерживающих мер и средств контроля и управления безопасностью;
- ◆ рассмотрение вариантов специализированной архитектуры/проекта сетевой безопасности с учетом сетевых сценариев и вопросов сетевых технологий;

- ◆ разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности;
- ◆ реализация и эксплуатация мер и средств контроля и управления безопасностью;
- ◆ мониторинг и проверка реализации.

Риски, с которыми сталкивается организация, могут быть связаны с проблемами несанкционированного доступа к информации, несанкционированной передачи информации, внесения вредоносной программы, отказа от факта приема или источника информации, отказа в обслуживании и недоступности информации или услуг. Указанные угрозы могут быть связаны с утратой:

- ◆ конфиденциальности информации и программы;
- ◆ целостности информации и программы;
- ◆ доступности информации и сетевых услуг;
- ◆ неотказуемости и подотчетности сетевых транзакций;
- ◆ подлинности информации (а также аутентичности сетевых пользователей и администраторов);
- ◆ достоверности информации и программы (в сетях и системах, соединенных с сетями);
- ◆ способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов и выполнение обязательств в отношении законодательства;
- ◆ способности контролировать злоупотребление санкционированным доступом.

Концептуальная модель сетевой безопасности, показывающая, где могут возникать разные виды рисков безопасности, представлена в стандарте в виде схемы, которая изображена на рис. 3.9.

Оценка риска сетевой безопасности производится в соответствии с рекомендациями, представленными в ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27005. Основные процессы оценки и менеджмента риска сетевой безопасности показаны на рис. 3.10 в формате стандарта.

Деятельность по менеджменту сетевой безопасности должна включать в себя:

- ◆ определение всех обязанностей, связанных с сетевой безопасностью, и назначение лица, ответственного за обеспечение безопасности;
- ◆ документально оформленную политику сетевой безопасности и операционные процедуры безопасности;

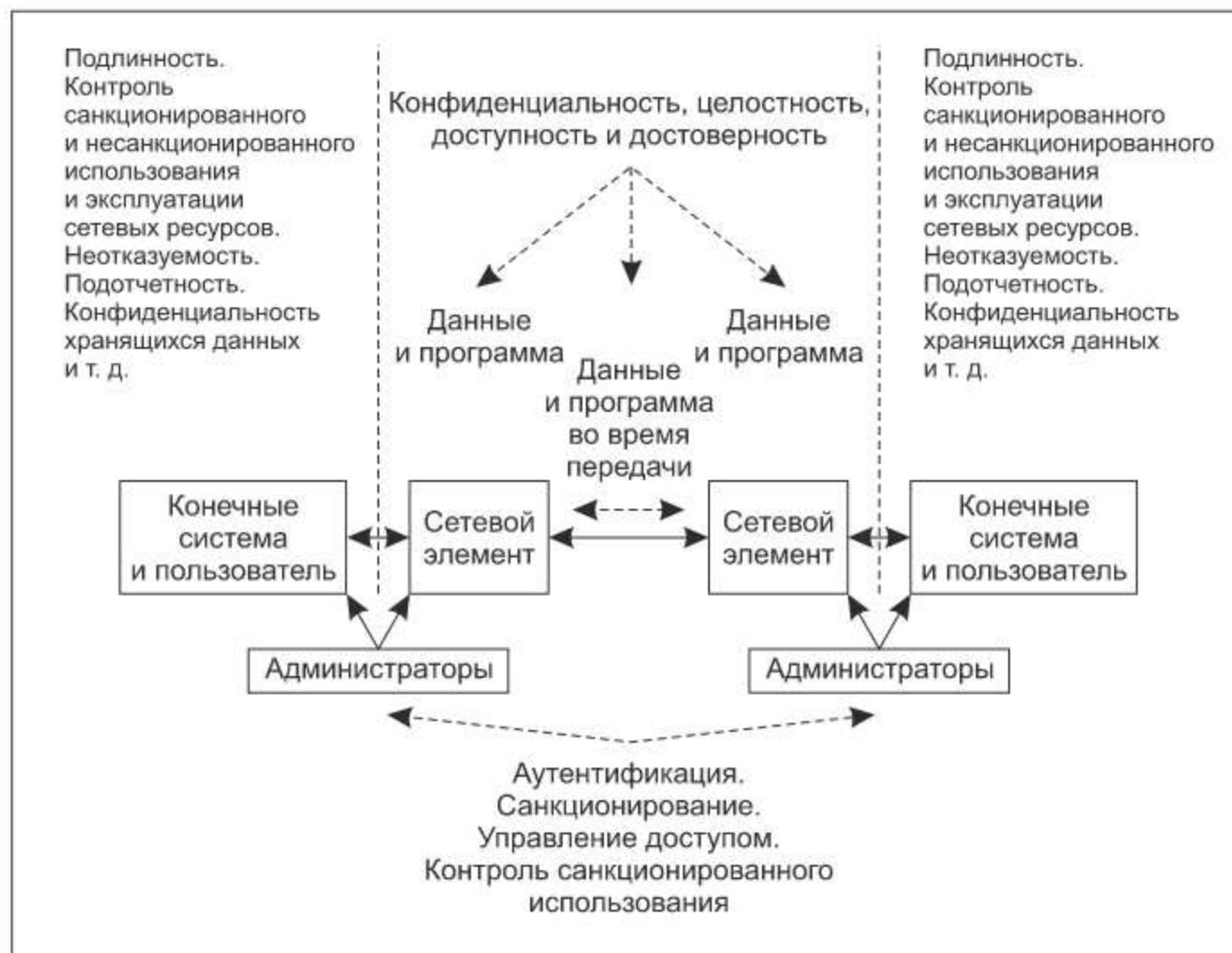


Рис. 3.9. Модель областей риска сетевой безопасности

- ◆ проверку соответствия требованиям безопасности, включая тестирование безопасности;
- ◆ документированные условия обеспечения безопасности для сетевого соединения с сотрудниками организации или сторонними организациями или лицами;
- ◆ документированные условия обеспечения безопасности для удаленных сетевых пользователей;
- ◆ план менеджмента инцидентов сетевой безопасности;
- ◆ документально оформленные и проверенные планы по обеспечению непрерывности деятельности/восстановлению после прерывания.

Политика сетевой безопасности организации должна быть реализуемой, легкодоступной для уполномоченных сотрудников организации и содержащей четкие формулировки:

- ◆ правил безопасного использования конкретных сетевых ресурсов, услуг и приложений;

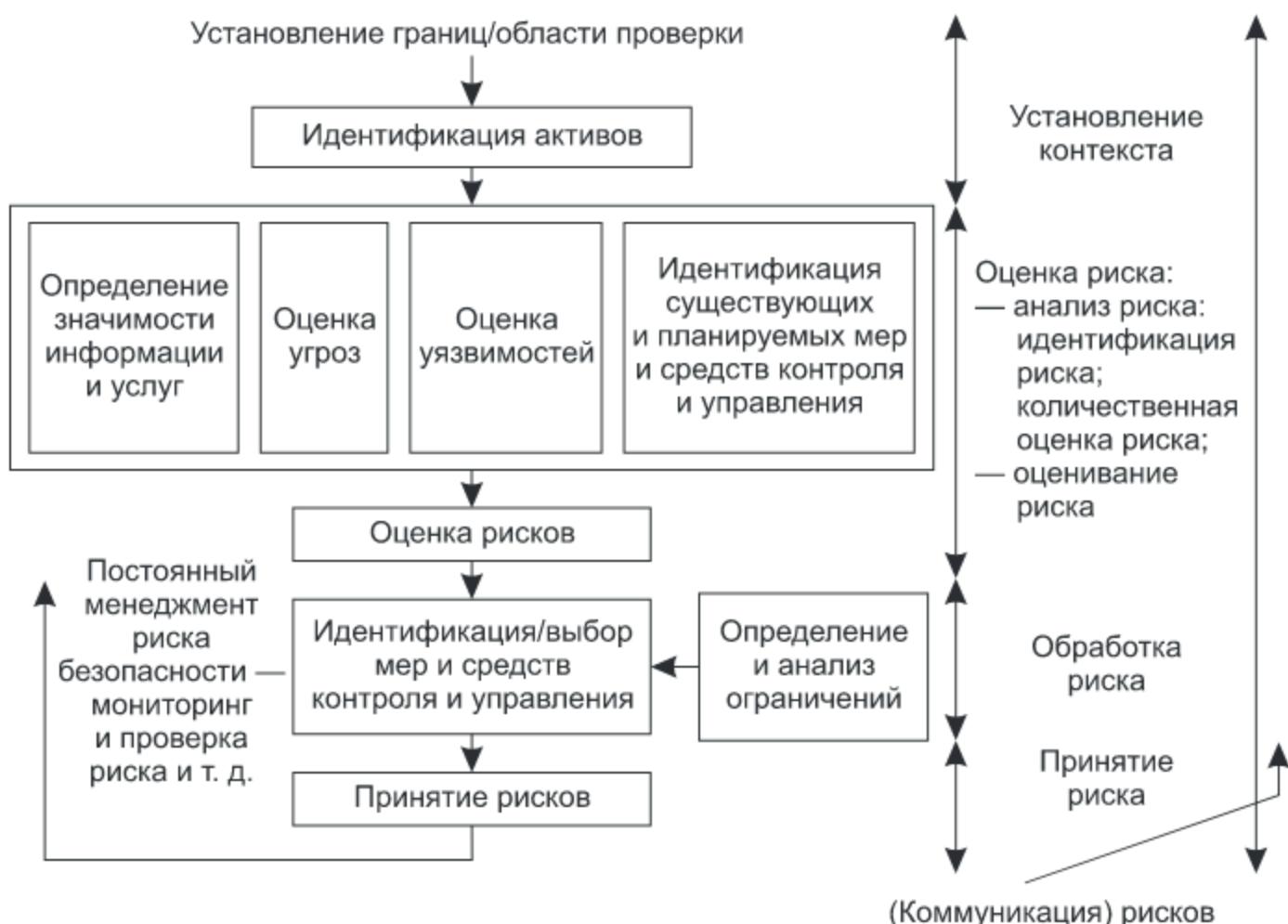


Рис. 3.10. Процессы оценки и менеджмента риска сетевой безопасности

- ◆ последствий невыполнения правил безопасности;
- ◆ отношения организации к неправильному использованию сети;
- ◆ логического обоснования политики и конкретных правил безопасности.

В связи с менеджментом сетевой безопасности стандарт рекомендует конкретные роли и обязанности, которые в зависимости от численности организации могут комбинироваться.

Высшее руководство должно:

- ◆ определять цели безопасности организации;
- ◆ инициировать, утверждать, доводить до сведения персонала и устанавливать политику, процедуры и правила безопасности организации, политику допустимого использования сетевых ресурсов;
- ◆ обеспечивать и приводить в исполнение политику обеспечения безопасности и допустимого использования сетевых ресурсов.

Руководители, осуществляющие сетевой менеджмент, должны:

- ◆ разрабатывать детальную политику сетевой безопасности;

- ◆ реализовывать политику сетевой безопасности и политику допустимого использования сетевых ресурсов;
- ◆ управлять взаимодействием с внешними сторонами и провайдерами услуг для обеспечения соответствия внутренней и внешней политикам сетевой безопасности.

Группа обеспечения сетевой безопасности должна:

- ◆ приобретать, разрабатывать, тестировать, проверять и поддерживать компоненты и инструментальные средства сетевой безопасности;
- ◆ устанавливать, обновлять, использовать и обеспечивать защиту сервисов и компонентов сетевой безопасности;
- ◆ выполнять необходимые ежедневные задачи по применению спецификаций, правил и параметров сетевой безопасности, которых требуют действующие политики сетевой безопасности;
- ◆ принимать меры по обеспечению защиты компонентов сетевой безопасности.

Пользователи сети должны:

- ◆ сообщать о своих требованиях к безопасности;
- ◆ соблюдать корпоративную политику безопасности;
- ◆ соблюдать корпоративные политики допустимого использования сетевых ресурсов;
- ◆ сообщать о событиях и инцидентах сетевой безопасности;
- ◆ обеспечивать обратную связь по вопросам эффективности сетевой безопасности.

Аудиторы (внутренние и внешние) должны:

- ◆ проводить проверки и аудит;
- ◆ проверять соблюдение политики сетевой безопасности;
- ◆ проверять и тестировать совместимость действующих правил сетевой безопасности с текущими требованиями основной деятельности организации и правовыми ограничениями.

В стандарте приведены примеры типовых сетевых сценариев:

- ◆ Услуги доступа сотрудников в Интернет. Базовым принципом должен быть принцип, разрешающий только те услуги, которые обеспечивают потребности организации.
- ◆ Расширенные услуги совместной работы (чат, видеоконференции и среды коллективного использования документов и т. п.).

- ◆ Услуги «бизнес – бизнес» и «бизнес – клиент».
- ◆ Услуги аутсорсинга.
- ◆ Сегментация сети.
- ◆ Мобильная связь.
- ◆ Сетевая поддержка для пользователей, находящихся в разъездах.
- ◆ Сетевая поддержка домашних офисов и офисов малых предприятий.

Подробные рекомендации по рискам безопасности, методам проектирования безопасности и мерам и средствам контроля и управления, необходимым для уменьшения последствий этих рисков во всех конкретных сценариях, подробно описаны в стандарте ИСО/МЭК 27033-3.

В приложении к стандарту подробно описаны риски безопасности, а также меры и средства контроля и управления безопасностью в конкретных сетевых технологиях:

- ◆ локальные вычислительные сети;
- ◆ глобальные вычислительные сети;
- ◆ беспроводные сети;
- ◆ радиосети;
- ◆ широкополосные сети;
- ◆ шлюзы безопасности;
- ◆ виртуальные частные сети;
- ◆ сети телефонной связи;
- ◆ IP-конвергенция;
- ◆ размещение информации на сервере веб-узлов;
- ◆ электронная почта в Интернете;
- ◆ маршрутизированный доступ к сторонним организациям;
- ◆ центр обработки и хранения данных.

3.6.3. Национальный стандарт ГОСТ Р ИСО/МЭК 27033-3–2014 – эталонные сетевые сценарии

Национальный стандарт Российской Федерации ГОСТ Р ИСО /МЭК 27033-3–2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» введен в действие 01.11.2015 г. Он идентичен международному стандарту ISO /

IEC 27033-3:2010 «Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues».

В стандарте изложены угрозы, методы проектирования и вопросы, касающиеся мер и средств контроля и управления, связанные с типовыми сетевыми сценариями. Для каждого сценария представлены подробные руководства по угрозам безопасности, методам проектирования безопасности и мерам и средствам контроля и управления.

Сценарии в стандарте упорядочены в зависимости:

- ◆ от типа доступа пользователя (является ли пользователь работающим внутри предприятия (внутренний), или пользователем является сотрудник, который получает доступ к корпоративным ресурсам извне, или пользователь является клиентом, поставщиком или деловым партнером (внешним));
- ◆ типа доступности информационных ресурсов (открытые, ограниченные или внешние ресурсы).

В стандарте рассмотрены следующие типовые сетевые сценарии:

- ◆ услуги доступа к Интернету для сотрудников;
- ◆ услуги «бизнес – бизнес»;
- ◆ услуги «бизнес – клиент»;
- ◆ расширенное применение услуг для совместного использования;
- ◆ сегментация сети;
- ◆ сетевая поддержка работы на дому или в малых предприятиях;
- ◆ мобильная связь;
- ◆ сетевая поддержка мобильных пользователей;
- ◆ услуги аутсорсинга.

Структура упорядочения типовых сетевых сценариев представлена в табл. 3.1.

Руководства, представленные в настоящем стандарте для каждого из определенных типовых сетевых сценариев, основаны на перечисленных далее подходах:

- ◆ проверка вводной информации и рамок сценария;
- ◆ описание угроз, соответствующих сценарию;
- ◆ анализ риска относительно обнаруженных уязвимостей;
- ◆ анализ влияния на бизнес рассматриваемых уязвимостей;

- ◆ определение рекомендаций по реализации обеспечения безопасности сети.

Таблица 3.1. Структура упорядочения сетевых сценариев

Доступность информационных ресурсов	Пользователи		
	Внутренние	Сотрудники, работающие вне предприятия	Внешние
Открытые	Услуги доступа к Интернету для сотрудников	–	Услуги «бизнес — клиент»
	Услуги «бизнес — бизнес»		
Ограниченные	Расширенное применение услуг для совместного использования	Мобильная связь	Расширенное применение услуг для совместного использования
	Услуги «бизнес — бизнес»	Сетевая поддержка мобильных пользователей	Услуги «бизнес — бизнес»
	Сегментация сети	–	Услуги «бизнес — клиент»
	Сетевая поддержка работы на дому или в малых предприятиях	–	–
Внешние	Услуги аутсорсинга	–	Услуги аутсорсинга

Первоочередным при оценке безопасности является определение активов, нуждающихся в защите. Безопасность сети также предполагает защиту различной деятельности, поддерживаемой в сети, такой как управленческая деятельность и получение данных конечных пользователей.

Каждый типовой сетевой сценарий исследуется в отношении известного набора угроз для выяснения того, какие угрозы могут быть применены. В приложении к стандарту приведен перечень известных отраслевых угроз. Этот перечень не следует рассматривать как исчерпывающий, но он может служить отправной точкой для анализа. Затем анализируются уязвимости, чтобы определить, каким образом угрозы могут быть реализованы в контексте конкретного рассматриваемого актива. Такой анализ поможет определить, какие ограничения отсутствуют и какие контрмеры требуется применить для достижения целей защиты.

ПРИМЕЧАНИЕ

Для определения перечня угроз и выделения актуальных угроз можно использовать банк данных угроз (размещен на сайте ФСТЭК), а также соответствующие методические документы ФСТЭК, рассмотренные ранее в данном учебном пособии.

При проектировании контрмер и реализации мер и средств контроля и управления стандарт не только требует сохранения конфиденциальности, целостности и доступности информации, но и затрагивает другие свойства, такие как подлинность, неотказуемость и достоверность.

Услуги доступа к сети Интернет для сотрудников. Основные угрозы безопасности:

- ◆ вирусные атаки и внедрение вредоносных программ;
- ◆ утечка информации;
- ◆ несанкционированное использование и доступ;
- ◆ ответственность за несоблюдение нормативов;
- ◆ снижение доступности сети связи, вызванное недостаточной пропускной способностью.

Услуги «бизнес – бизнес». Основные угрозы безопасности:

- ◆ вирусные атаки и внедрение вредоносных программ;
- ◆ использование вредоносных программ приводит к проникновению в системы, ведущему к сбоям или несанкционированному доступу к конфиденциальной информации;
- ◆ уязвимости веб-браузеров или других веб-приложений могут быть использованы вредоносными программами, что приведет к заражению вирусом и установке троянов;
- ◆ атаки типа «отказ в обслуживании» (DoS) и «распределенный отказ в обслуживании» (DDoS) на порталы или расширенные сети услуг «бизнес – бизнес»;
- ◆ инсайдерские атаки с помощью авторизованных партнеров по бизнесу;
- ◆ фальсификация информационного наполнения транзакции (сообщения не передаются получателю или данные изменяются в процессе передачи).

Услуги «бизнес – клиент». Основные угрозы безопасности:

- ◆ вирусные атаки и внедрение вредоносных программ;
- ◆ неавторизованный доступ к серверным базам данных;
- ◆ сбор действительных идентификаторов и имен учетных записей пользователей;

- ◆ несанкционированный доступ к системам или сетям со злым умыслом, чтобы скопировать, изменить или уничтожить данные;
- ◆ незаконная расшифровка содержания, приводящая к нарушению авторских прав и краже содержания;
- ◆ атаки «отказ в обслуживании»;
- ◆ подделка информационного наполнения транзакции.

Расширенное применение услуг для совместного использования. Основные угрозы безопасности:

- ◆ неавторизованный доступ, ведущий к раскрытию конфиденциальной информации;
- ◆ злоупотребление совместным использованием инструментальных средств с целью незаконного пользования материалами, охраняемыми авторским правом, получения конфиденциальных данных и навязывания пользователям нежелательной или пропагандистской информации;
- ◆ вирусные атаки и внедрение вредоносных программ;
- ◆ снижение доступности сети связи;
- ◆ перегрузка сети с легитимным трафиком;
- ◆ уязвимости эксплуатируемого протокола, используемые в услугах для совместного использования.

Сегментация сети. Основные угрозы безопасности:

- ◆ ответственность за несоблюдение законодательства;
- ◆ утечка данных;
- ◆ нарушение конфиденциальности, например когда данные заказчика/клиента доступны из стран, из которых они не должны быть доступны;
- ◆ нарушение требований конфиденциальности конкретной страны;
- ◆ риски, связанные с репутацией, влекущие за собой неудовлетворение ожиданий заказчика/клиента в отношении конфиденциальности или непрозрачности.

Сетевая поддержка работы на дому или в малых предприятиях. Основные угрозы безопасности:

- ◆ неавторизованный доступ;
- ◆ использование учетных записей гостя и настроек по умолчанию;
- ◆ вирусные атаки и введение вредоносных программ;
- ◆ несанкционированное разглашение конфиденциальной информации;
- ◆ отсутствие шифрования данных, хранящихся в системах и передающихся через домашние сети или сети малого бизнеса;

- ◆ злоупотребление возможностями доступа, такими как беспроводной доступ в Интернет через домашние сети или сети малых предприятий;
- ◆ недостаточное обучение конечных пользователей передовым практикам осведомленности и соблюдения безопасности;
- ◆ недостоверность предположений касательно защиты интранета, так как сетевые шлюзы, используемые при работе на дому или в малых предприятиях, не обеспечивают такой же уровень защиты, как шлюзы, использующиеся для соединения филиалов организации.

Мобильная связь. Основные угрозы безопасности:

- ◆ несанкционированный доступ к информации, хранящейся на мобильных устройствах, вследствие слабого управления доступом или недостаточной защиты конфиденциальной информации, недостаточной информированности и неадекватных паролей, слабой конфигурации, хакерских атак с использованием мошеннических устройств, отсутствия осведомленности конечных пользователей о требованиях обеспечения ИБ;
- ◆ несанкционированное разглашение местоположения конфиденциальных данных и информации вследствие получения услуг, связанных с определением местоположения, которые могут раскрывать несанкционированным третьим лицам информацию о положении пользователя, что затрагивает неприкосновенность частной жизни, подслушивания, вовлечения неадекватно защищенных третьих лиц в процесс передачи информации, использования открытого текста или недостаточно защищенных протоколов передачи;
- ◆ несанкционированная модификация/удаление хранимой информации (включая программное средство) вследствие ввода вредоносных программ, использования уязвимостей в базовой операционной системе;
- ◆ спам, приводящий к повышенной плате за обслуживание, возможности фишинг-атак, атакам «отказ в обслуживании»;
- ◆ кража или случайная потеря, приводящая к потере важных данных, проблемам конфиденциальности, когда конфиденциальные данные, хранящиеся на устройстве, не защищены должным образом, бесконтрольному резервному копированию данных.

Сетевая поддержка мобильных пользователей. Основные угрозы безопасности:

- ◆ несанкционированный доступ из-за неправильного использования технической поддержки мобильных пользователей сети;
- ◆ компрометация шлюзов безопасности, используемых на границе сети интранет;

- ◆ несанкционированный доступ к данным, хранящимся на устройствах мобильного пользователя;
- ◆ снижение доступности сети связи.

Услуги аутсорсинга. Основные угрозы безопасности:

- ◆ несанкционированный доступ к другим внутренним системам (когда поставщик получает доступ к внутренним системам для удаленной поддержки и технического обслуживания);
- ◆ злоупотребление удаленными портами обслуживания;
- ◆ злоупотребление правами администратора;
- ◆ несанкционированное раскрытие поставщиком услуг конфиденциальных данных;
- ◆ пренебрежение правами интеллектуальной собственности;
- ◆ неправильное обращение с носителями информации;
- ◆ использование небезопасных методов передачи информации;
- ◆ внедрение вредоносных программ;
- ◆ недостаточная безопасность при разработке программного средства и процедур выпуска программного средства;
- ◆ небезопасная передача файлов и данных;
- ◆ небезопасные практики совместного использования режима онлайн;
- ◆ ответственность за несоблюдение законодательства;
- ◆ отсутствие понимания норм и законов конкретной страны об ответственности, если поставщик услуг находится в другой стране;
- ◆ недостаточные правовые требования к конфиденциальности и защите данных, применяемые в стране, где находится поставщик.

Для каждого из указанных выше типовых сценариев после перечисления угроз стандарт рекомендует соответствующие методы проектирования безопасности и меры и средства контроля и управления.

3.7. Стандарты по безопасности сетей электросвязи (ГОСТ Р 52448–2005, ГОСТ Р 53110–2008)

Проблемам обеспечения безопасности сетей электросвязи посвящены следующих два национальных стандарта Российской Федерации:

- ◆ ГОСТ Р 52448–2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения», введен в действие 01.01.2007 г.;
- ◆ ГОСТ Р 53110–2008 «Система обеспечения информационной безопасности. Сети связи общего пользования. Общие положения», введен в действие 01.10.2009 г.

ГОСТ 52448–2005 предназначен для применения организациями, которые связаны с созданием и эксплуатацией сетей электросвязи, являющихся составными компонентами сети связи общего пользования единой сети электросвязи Российской Федерации. Основными функциями сетей электросвязи являются прием, обработка, хранение, передача и предоставление информации пользователям и органам государственного управления для ее последующего применения. Сети электросвязи предназначены для оказания услуг связи любому пользователю путем предоставления открытых информационных ресурсов и информации, не содержащей сведений, составляющих государственную тайну, или информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Стандарт определяет терминологию, цели, задачи, принципы и основные положения обеспечения безопасности сетей электросвязи.

Под электросвязью понимаются любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Необходимость рассмотрения проблем обеспечения безопасности сетей электросвязи обусловлена:

- ◆ динамикой развития сетей электросвязи и их интеграцией с глобальными сетями связи, в том числе с Интернетом;
- ◆ совершенствованием применяемых ИТ;
- ◆ ростом числа пользователей услугами связи и расширением спектра предоставления услуг связи;
- ◆ увеличением объемов хранимой и передаваемой информации;
- ◆ территориальной рассредоточенностью сложных информационно-телекоммуникационных структур;
- ◆ недостаточным количеством механизмов обеспечения безопасности в сетях электросвязи.

Основными задачами обеспечения безопасности сетей электросвязи являются:

- ◆ своевременное выявление, оценка и прогнозирование источников угроз безопасности;

- ◆ выявление и устранение уязвимостей в средствах связи и сетях электросвязи;
- ◆ предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных воздействий нарушителей;
- ◆ организация системы пропуска приоритетного трафика;
- ◆ совершенствование и стандартизация применяемых мер обеспечения безопасности сетей электросвязи.

К основным угрозам безопасности сетей электросвязи могут быть отнесены следующие:

- ◆ уничтожение информации и/или других ресурсов;
- ◆ искажение или модификация информации;
- ◆ мошенничество;
- ◆ кража, утечка, потеря информации и/или других ресурсов;
- ◆ несанкционированный доступ;
- ◆ отказ в обслуживании.

Нарушителями безопасности сетей электросвязи могут быть:

- ◆ террористы и террористические организации;
- ◆ конкурирующие организации и структуры;
- ◆ спецслужбы иностранных государств и блоков государств;
- ◆ криминальные структуры;
- ◆ взломщики программных продуктов ИТ, использующихся в системах связи;
- ◆ бывшие сотрудники организаций связи;
- ◆ недобросовестные сотрудники и партнеры;
- ◆ пользователи услугами связи и др.

Безопасность сети электросвязи характеризуется основными ее критериями: конфиденциальностью инфокоммуникационной структуры сети электросвязи, целостностью информации и услуг связи, доступностью информации и услуг связи, подотчетностью действий в сети.

Нарушение этих характеристик может иметь следующие последствия для деятельности оператора связи:

- ◆ «низкое» потенциальное воздействие может привести к ограниченному неблагоприятному эффекту;
- ◆ «умеренное» потенциальное воздействие может привести к серьезному неблагоприятному эффекту;

- ◆ «высокое» потенциальное воздействие может привести к тяжелому или катастрофическому неблагоприятному эффекту.

В соответствии с используемой оператором связи методикой оценки рисков и с учетом вероятности возникновения угрозы и потенциального воздействия нарушителя, реализующего данную угрозу, должен определяться риск возможного нанесения ущерба сети электросвязи: незначительный, существенный, критический.

Требования к безопасности сетей электросвязи устанавливают федеральные органы исполнительной власти в области связи на основании законодательства в области связи и защиты информации. Требования включают:

- ◆ организационные требования безопасности;
- ◆ технические требования безопасности;
- ◆ функциональные требования безопасности;
- ◆ требования доверия к безопасности.

Последние два вида требований определяются в соответствии со стандартами серии ГОСТ Р ИСО/МЭК 15408.

Система обеспечения безопасности сетей электросвязи является элементом системы ИБ Российской Федерации. В общем случае ее архитектура может содержать следующие уровни безопасности:

- ◆ уровень управления безопасностью (осуществляется управление безопасностью сетей, координируемое центральным органом);
- ◆ организационно-административный уровень (включает службы безопасности организации связи);
- ◆ уровень безопасности инфокоммуникационной структуры (содержит механизмы обеспечения безопасности и другие средства, обеспечивающие защиту процесса обработки и передачи информации в сети);
- ◆ уровень безопасности услуг (осуществляется контроль качества предоставляемых услуг связи);
- ◆ уровень сетевой безопасности (поддержка безопасности сетевых протоколов);
- ◆ уровень физической безопасности (физическая охрана помещений, контроль доступа и т. п.).

Стандарт ГОСТ Р 53110–2008 определяет правовые, организационные и технические направления обеспечения ИБ сетей электросвязи, входящих в состав сети связи общего пользования. Он распространяет положения по обеспечению безопасности сетей электросвязи, установленные ГОСТ Р 52448, на систему обеспечения ИБ сети связи общего пользования,

определяя ее как комплекс взаимодействующих систем обеспечения информационной безопасности сетей электросвязи, входящих в состав сети связи общего пользования.

Стандарт устанавливает общий подход к:

- ◆ формированию и проведению в организации связи единой политики информационной безопасности;
- ◆ принятию управленческих решений по внедрению практических мер, реализующих организационные и функциональные требования безопасности;
- ◆ координации деятельности структурных подразделений организации связи при проведении работ по проектированию, построению, реконструкции и эксплуатации сети с соблюдением требований безопасности, определяемых федеральными органами исполнительной власти, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации.

Дополнительно к задачам обеспечения ИБ, определенных в ГОСТ 52448, в организации связи должно предусматриваться выполнение следующих задач:

- ◆ создание, реализация, поддержка функционирования, мониторинг и совершенствование системы обеспечения ИБ на основе использования процессного подхода к управлению ИБ, определенного в ГОСТ Р ИСО/МЭК 27001 по менеджменту ИБ;
- ◆ анализ рисков ИБ, определение способов обработки рисков и мероприятий по их снижению;
- ◆ обеспечение изолированности средств связи, участвующих в управлении сетями электросвязи, от внешних сетей и рабочих станций, обслуживающего сеть персонала;
- ◆ обеспечение контролируемого доступа обслуживающего персонала к системе управления сетями электросвязи;
- ◆ обеспечение централизованной аутентификации обслуживающего сети персонала при их доступе к средствам связи;
- ◆ паспортизация организаций связи по требованиям к ИБ.

Основными процессами системы менеджмента ИБ, определяющими функционирование системы обеспечения ИБ, являются управление рисками, внутренний аудит, управление инцидентами, управление изменениями.

В стандарте определены и подробно описаны следующие направления обеспечения ИБ: правовое, организационное, техническое.

Создание системы обеспечения ИБ сетей электросвязи должно предусматривать формирование в организации связи организационно-штатной структуры, непосредственно выполняющей мероприятия и действия по обеспечению ИБ сети электросвязи.

Для установления соответствия сети электросвязи требованиям ИБ по инициативе оператора связи проводится подтверждение соответствия (аттестация) в форме добровольной сертификации. Аттестация сети электросвязи на соответствие требованиям безопасности должна осуществляться специализированными сертификационными центрами или лабораториями по методикам, разработанным в системе добровольной сертификации ИБ сетей электросвязи.

Кроме рассмотренных ранее документов функционирование сетей электросвязи регламентируется базовым Федеральным законом от 07.07.2003 г. № 126-ФЗ «О связи», а также рядом нормативных документов Правительства РФ, в частности:

- ◆ Постановлением от 25.06.2009 г. № 532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации»;
- ◆ Постановлением от 10.09.2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи»;
- ◆ Постановлением от 23.01.2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных»;
- ◆ Постановлением от 21.04.2005 г. № 241 «О мерах по организации оказания универсальных услуг связи»;
- ◆ Распоряжением от 15.04.2013 г. № 611-р «Об утверждении перечня нарушений целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации».

3.8. Защита от угроз, реализуемых через скрытые каналы (ГОСТ Р 53113.1, ГОСТ Р 53113.2)

Среди документов в области защиты информационных технологий и автоматизированных систем от угроз ИБ, реализуемых с использованием скрытых каналов, следует отметить два национальных стандарта Российской Федерации:

- ◆ ГОСТ Р 53113.1–2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз

информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»;

- ◆ ГОСТ Р 53113.2–2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».

Развитие, внедрение и использование распределенных информационных систем и технологий, использование импортных программно-аппаратных средств привели к появлению класса угроз информационной безопасности, связанных с использованием так называемых скрытых информационных каналов, невидимых для традиционных средств защиты информации.

Традиционные средства обеспечения ИБ, такие как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, контролируют только информационные потоки, которые проходят по каналам, предназначенным для их передачи. Возможность обмена информацией вне этих рамок посредством скрытых каналов не учитывается. Опасность СК для информационных технологий и автоматизированных систем и других активов организации связана с отсутствием контроля средствами защиты информационных потоков, что может привести к утечке информации и нарушить целостность информационных ресурсов и программного обеспечения в компьютерных системах.

СК используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на АС, которая не обнаруживается средствами контроля и защиты. Опасность СК основана на предположении о том, что нарушитель имеет постоянный доступ к информационным ресурсам и возможность воздействовать через эти каналы на информационную систему для нанесения максимального ущерба.

Для обеспечения защиты информации, обрабатываемой в АС, необходимо выявлять и нейтрализовывать все возможные информационные каналы несанкционированного действия, в том числе скрытые.

Существенным моментом защищенности систем ИТ и АС является доверие к системам защиты. В системах, требующих обеспечения повышенного уровня доверия, должны учитываться угрозы безопасности, возникающие вследствие наличия возможности несанкционированного действия с помощью СК. Требования доверия к безопасности информации установлены в ГОСТ Р ИСО/МЭК 15408-3, в соответствии с которым для систем с оценочным уровнем доверия, начиная с ОУД5, предусмотрено проведение

обязательного анализа СК. Таким образом, требование анализа СК в Российской Федерации является необходимым условием безопасного функционирования систем, обрабатывающих ценную информацию или использующих импортное аппаратно-программное обеспечение.

Стандарт ГОСТ Р 53113.1–2008 устанавливает классификацию СК, определяет задачи, решаемые при проведении анализа СК, а также устанавливает порядок проведения анализа для ИТ и АС. Он предназначен для использования заказчиками, разработчиками и пользователями ИТ при формировании ими требований к разработке, приобретению и применению продуктов и систем ИТ, которые предназначены для обработки, хранения или передачи информации, подлежащей защите. Стандарт предназначен также для использования органами сертификации и испытательными лабораториями при оценке безопасности и сертификации безопасности ИТ и АС.

В стандарте введен ряд терминов.

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Информационная система — организационно упорядоченная совокупность документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Вредоносная программа — программа, предназначенная для несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы.

Скрытый канал — не предусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Стандарт определяет следующий порядок действий (этапы) по определению степени опасности СК для активов организации, выявлению и противодействию СК:

- ◆ классификация активов в зависимости от степени опасности атак с использованием СК с учетом возможных угроз безопасности активам и анализ рисков;
- ◆ анализ СК, включающий в себя их идентификацию (определение источника и получателя) и оценку опасности, которую несет их скрытое функционирование;
- ◆ реализация мероприятий по защите от угроз, реализуемых с использованием СК;
- ◆ организация контроля за противодействием СК.

Противодействие опасным СК может осуществляться с помощью следующих средств и методов:

- ◆ построение архитектуры ИТ или АС, позволяющей перекрыть СК или сделать их пропускную способность настолько низкой, что каналы становятся неопасными;
- ◆ использование технических средств, позволяющих перекрывать СК или снижать их пропускную способность до уровня ниже заданного;
- ◆ использование программно-технических средств, позволяющих выявлять работу опасных СК в процессе эксплуатации системы;
- ◆ применение организационно-технических мер, позволяющих ликвидировать СК или уменьшить их пропускную способность до безопасного значения.

Угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

- ◆ внедрение вредоносных программ и данных;
- ◆ подачу злоумышленником команд агенту для выполнения;
- ◆ утечку криптографических ключей или паролей;
- ◆ утечку отдельных информационных объектов.

Системами, наиболее сильно подверженными атакам с использованием СК, являются:

- ◆ многопользовательские распределенные системы;
- ◆ системы с выходом в глобальные сети;
- ◆ системы, использующие криптографические средства защиты;
- ◆ системы, использующие многоуровневую (мандатную) политику разграничения доступа;
- ◆ системы, программно-аппаратные агенты в которых не могут быть обнаружены (в связи с использованием программного и аппаратного обеспечения с недоступным исходным кодом и в связи с отсутствием конструкторской документации).

В зависимости от степени опасности атак с использованием СК защищаемые активы организации подразделяют на следующие классы:

- ◆ 1-й класс – активы, содержащие информацию, степень подверженности которой атакам, реализуемым с использованием СК, определяет собственник;
- ◆ 2-й класс – активы, содержащие информацию ограниченного доступа или персональные данные и обрабатываемые в системах, имеющих

- технические интерфейсы с открытыми сетями или компьютерными системами общего доступа, а также компьютерными системами, не предполагающими защиту от утечки по техническим каналам;
- ◆ 3-й класс — активы, содержащие сведения, составляющие государственную тайну.

Кроме того, существует особый класс активов, которые уязвимы с точки зрения угроз, реализуемых с использованием СК с низкой пропускной способностью:

- ◆ класс А — активы, связанные с функционированием критически важных объектов;
- ◆ класс Б — активы, содержащие ключевую/парольную информацию, в том числе ключи криптографических систем защиты информации и пароли доступа к иным активам.

В стандарте ГОСТ Р 53113.2–2009 установлены подробные рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов в соответствии с этапами, определенными в первой части стандарта. Он предназначен как для заказчиков, разработчиков и пользователей ИТ в процессе формирования требований по защите информации на стадиях разработки, приобретения и применения ИТ-продуктов и АС в соответствии с требованиями нормативных правовых документов, так и для органов сертификации и испытательных лабораторий при проведении подтверждения соответствия ИТ и АС требованиям к обеспечению безопасности информации.

Стандарт устанавливает типовой порядок организации противодействия СК, который может уточняться с учетом условий и особенностей применения информационных технологий в АС.

Организация защиты ИТ и АС от атак с использованием СК включает в себя процедуры их выявления и подавления. Набор применяемых методов выявления и/или подавления СК должен определяться исходя из модели угроз безопасности организации. Мероприятия по защите от атак с использованием СК должны быть интегрированы в систему информационной безопасности организации.

3.9. Стандарты по уязвимостям ИС (ГОСТ Р 56545, ГОСТ Р 56546)

В августе 2015 г. Росстандарт утвердил два национальных стандарта по классификации и описанию уязвимостей информационных систем:

- ◆ ГОСТ Р 56545–2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;
- ◆ ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».

Оба стандарта введены в действие 01.04.2016 г.

Действие стандартов распространяется на деятельность по защите информации, связанную с выявлением, описанием, устранением или исключением возможности использования уязвимостей ИС при разработке, внедрении и эксплуатации ИС.

В стандарте ГОСТ Р 56545–2015 приняты правила описания уязвимостей, которые могут быть использованы специалистами по информационной безопасности при создании и ведении базы данных уязвимостей ИС, разработке средств контроля (анализа) защищенности информации, разработке моделей угроз безопасности информации и проектировании систем защиты информации, проведении работ по идентификации, выявлению уязвимостей, их анализу и устранению.

В стандарте ГОСТ Р 56546–2015 принята классификация уязвимостей ИС в зависимости от области их происхождения, типов недостатков ИС и мест возникновения (проявления).

Стандарт не распространяется на уязвимости ИС, связанные с утечкой информации по техническим каналам.

Под уязвимостью ИС в стандарте понимается недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, которые могут быть использованы для реализации угроз безопасности информации.

Стандарт вводит также определение нескольких видов уязвимостей.

Уязвимость кода – уязвимость, появившаяся в процессе разработки программного обеспечения.

Уязвимость конфигурации – уязвимость, появившаяся в процессе задания конфигурации ПО и технических средств ИС.

Уязвимость архитектуры – уязвимость, появившаяся в процессе проектирования ИС.

Уязвимость организационная – уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в ИС и/или несоблюдением правил эксплуатации средств ЗИ ИС, требований организационно-распорядительных документов по ЗИ и/или несвоевременном выполнении соответствующих действий должностным лицом или подразделением по защите информации.

Уязвимость многофакторная — уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.

Уязвимости ИС по области происхождения подразделяются на следующие классы:

- ◆ уязвимости кода;
- ◆ уязвимости конфигурации;
- ◆ уязвимости архитектуры;
- ◆ организационные уязвимости;
- ◆ многофакторные уязвимости.

Уязвимости ИС по месту возникновения подразделяются на:

- ◆ уязвимости в общесистемном ПО;
- ◆ уязвимости в прикладном ПО;
- ◆ уязвимости в специальном ПО;
- ◆ уязвимости в технических средствах;
- ◆ уязвимости в портативных технических средствах;
- ◆ уязвимости в сетевом оборудовании;
- ◆ уязвимости в средствах защиты информации.

Уязвимости по типам недостатков ИС подразделяются на:

- ◆ недостатки, связанные с неправильной настройкой параметров программного обеспечения;
- ◆ недостатки, связанные с неполнотой проверки вводимых данных;
- ◆ недостатки, связанные с возможностью прослеживания пути доступа к каталогам;
- ◆ недостатки, связанные с возможностью перехода по ссылкам;
- ◆ недостатки, связанные с возможностью внедрения команд ОС;
- ◆ недостатки, связанные с межсайтовым скрипtingом (выполнением сценариев);
- ◆ недостатки, связанные с вычислениями;
- ◆ недостатки, связанные с внедрением произвольного кода;
- ◆ недостатки, связанные с управлением ресурсами, полномочиями, привилегиями и доступом;
- ◆ недостатки, связанные с аутентификацией;

- ◆ недостатки, связанные с криптографическими преобразованиями (недостатки шифрования).

3.10. Комплекс стандартов по информационной безопасности Банка России (ИББС)

Комплекс документов Банка России в области информационной безопасности организаций банковской системы Российской Федерации состоит из нескольких стандартов и рекомендаций в области стандартизации. С момента выхода первых версий документов они регулярно пересматривались с учетом изменяющихся требований безопасности. Последними версиями документов являются следующие:

- ◆ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0–2014 (пятая редакция принята и введена в действие распоряжением Банка России от 17.05.2014 г. № Р-399 с 01.06.2014 г. взамен ИББС-1.0–2010);
- ◆ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» СТО БР ИББС-1.1–2007 (принят и введен в действие распоряжением Банка России от 28.04.2007 г. № Р-345 с 01.05.2007 г.);
- ◆ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014» СТО БР ИББС-1.2–2014 (четвертая редакция принята и введена в действие распоряжением Банка России от 17.05.2014 г. № Р-399 с 01.06.2014 г. взамен ИББС-1.2–2010);
- ◆ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» РС БР ИББС-2.0–2007 (приняты и введены в действие распоряжением Банка России от 28.04.2007 г. № Р-348 с 01.05.2007 г.);
- ◆ рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской

- Федерации требованиям СТО БР ИББС-1.0» РС БР ИББС-2.1–2007 (приняты и введены в действие распоряжением Банка России от 28.04.2007 г. № Р-347 с 01.05.2007 г.);
- ◆ рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» РС БР ИББС-2.2–2009 (приняты и введены в действие распоряжением Банка России от 11.11.2009 г. № Р-1190 с 01.01.2010 г.);
 - ◆ рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» РС БР ИББС-2.5–2014 (приняты и введены в действие распоряжением Банка России от 17.05.2014 г. № Р-400 с 01.06.2014 г.);
 - ◆ рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» РС БР ИББС-2.6–2014 (приняты и введены в действие распоряжением Банка России от 10.07.2014 г. № Р-556 с 01.09.2014 г.);
 - ◆ рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности» РС БР ИББС-2.7–2015 (приняты и введены в действие приказом Банка России от 19.02.2015 г. № ОД-392 с 01.05.2015 г.);
 - ◆ рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации» РС БР ИББС-2.8–2015 (приняты и введены в действие приказом Банка России от 19.02.2015 г. № ОД-393 с 01.05.2015 г.).

В 2010 г. Банком России были приняты два рекомендательных документа, касающихся защиты персональных данных в банковской сфере:

- ◆ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации». РС БСР ИББС-2.3–2010;
- ◆ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз

безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации». РС БСР ИББС-2.4–2010.

Оба эти документа были отменены с 01.06.2014 г. в связи с вводом в действие обновленных документов ИББС-1.0–2014, ИББС-1.2–2014, ИББС-2.5–2014 и ИББС-2.8–2015, в которых были полностью учтены вопросы защиты персональных данных в соответствии с изменившимся законодательством в области персональных данных. В частности, требования по защите персональных данных определялись на основании уровня защищенности ПДн при их обработке в ИСПДн, установленных Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 и Приказом ФСТЭК России от 18.02.2013 г. № 21.

Последние версии стандартов ИББС опираются на идеологию стандартов серии ГОСТ Р ИСО/МЭК 27000. Система менеджмента ИБ организаций банковской системы образуется реализацией четырех групп процессов:

- ◆ планирование системы обеспечения ИБ (планирование);
- ◆ реализация системы обеспечения ИБ (реализация);
- ◆ мониторинг и анализ системы обеспечения (проверка);
- ◆ поддержка и улучшение системы ИБ (совершенствование).

В качестве основных источников угроз ИБ определены:

- ◆ неблагоприятные события природного, техногенного и социального характера;
- ◆ террористы и криминальные элементы;
- ◆ зависимость от поставщиков/провайдеров/партнеров/клиентов;
- ◆ сбои, отказы, разрушения/повреждения программных и технических средств;
- ◆ работники организации БС РФ, реализующие угрозы ИБ с использованием lawfully предоставленных им прав и полномочий (внутренние нарушители ИБ);
- ◆ работники организации БС РФ, реализующие угрозы ИБ вне lawfully предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации БС РФ, но осуществляющие попытки НСД (внешние нарушители ИБ);
- ◆ несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Стандартом определены общие базовые требования по обеспечению информационной безопасности для различных видов деятельности:

- ◆ назначения и распределения ролей и обеспечения доверия к персоналу;
- ◆ эксплуатации автоматизированных банковских систем на стадиях жизненного цикла;
- ◆ управления доступом и регистрацией;
- ◆ использования средств антивирусной защиты;
- ◆ использования ресурсов сети Интернет;
- ◆ использования средств криптографической защиты информации;
- ◆ выполнения банковских платежных и информационных технологических процессов;
- ◆ обработки персональных данных.

Для реализации, эксплуатации, контроля и поддержания на должном уровне системы обеспечения информационной безопасности рекомендуется реализовать ряд процессов СМИБ, сгруппированных в виде циклической модели Деминга: «планирование – реализация – проверка – совершенствование».

Для успешного функционирования СМИБ стандарт рекомендует выполнить следующие группы требований:

- ◆ к организации и функционированию службы ИБ;
- ◆ определению/коррекции области действия СОИБ;
- ◆ выбору/коррекции подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ;
- ◆ разработке планов обработки рисков нарушения ИБ;
- ◆ разработке и корректировке внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- ◆ принятию руководством организации решений о реализации и эксплуатации СОИБ;
- ◆ реализации планов обработки рисков нарушения ИБ;
- ◆ разработке и организации реализации программ по обучению и повышению осведомленности в области ИБ;
- ◆ организации обнаружения инцидентов безопасности и реагирования на них;
- ◆ организации обеспечения непрерывности бизнеса и его восстановления после прерываний;
- ◆ мониторингу СОИБ и контролю защитных мер;
- ◆ проведению самооценки ИБ;
- ◆ проведению аудита ИБ;

- ◆ анализу функционирования СОИБ;
- ◆ анализу СОИБ со стороны руководства организации;
- ◆ принятию решений по тактическим улучшениям СОИБ;
- ◆ принятию решений по стратегическим улучшениям СОИБ.

Контрольные вопросы и задания к главе 3

1. Дайте определения понятиям «инцидент информационной безопасности», «угроза», «уязвимость», «риск».
2. Назовите этапы менеджмента инцидентов ИБ.
3. Опишите организационную структуру системы обеспечения безопасности ИТТ.
4. Какие стандарты относятся к менеджменту ИБ?
5. Какие стандарты относятся к безопасности сетей?
6. Опишите структуру стандартов семейства 27000.
7. В чем заключается процессный подход к СМИБ?
8. Каковы основные фазы внедрения СМИБ?
9. Какие основные положения должен содержать документ «Политика информационной безопасности»?
10. Какие нормативные документы в области ИБ (политики) должны быть разработаны в организации?
11. Опишите процесс менеджмента риска ИБ.
12. В чем заключается процесс обработки риска ИБ?
13. Назовите основные виды сетевых соединений в организации.
14. Дайте определения понятиям «интранет», «экстранет», «система обнаружения вторжений».
15. Опишите процесс обеспечения необходимой сетевой безопасности.
16. Каковы основные действия по менеджменту сетевой безопасности?
17. Какие основные положения должен содержать документ «Политика сетевой безопасности»?
18. Назовите основные обязанности пользователей сетей.
19. Назовите возможные типы сетевых сценариев и основные виды угроз для них.
20. Какие национальные стандарты Российской Федерации посвящены проблемам обеспечения безопасности сетей электросвязи?
21. Каковы основные задачи обеспечения безопасности сетей электросвязи?

22. Каковы основные угрозы безопасности сетей электросвязи?
23. Какие виды требований предъявляются к безопасности сетей электросвязи?
24. Опишите архитектуру системы обеспечения безопасности сетей электросвязи.
25. Какие национальные стандарты определяют меры по защите информации от угроз с использованием скрытых каналов?
26. Дайте определение термину «скрытый канал».
27. В чем заключается опасность наличия скрытых каналов?
28. Каковы этапы работ по защите от угроз, использующих скрытые каналы?
29. Какие угрозы могут быть реализованы с помощью СК?
30. Какие ИТ-системы наиболее подвержены атакам с использованием СК?
31. Назовите основные документы по информационной безопасности организаций банковской системы Российской Федерации.

Глава 4. Национальные стандарты Российской Федерации на основе «Общих критериев»

4.1. История создания «Общих критериев» и национальных стандартов на их основе

Все стандарты в области информационной безопасности можно разбить на две большие группы.

1. Оценочные стандарты, предназначенные для оценки ИС и средств защиты информации по требованиям безопасности.
2. Стандарты, описывающие спецификации, регламентирующие различные аспекты защиты информации.

Международный оценочный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», известный под названием «Общие критерии», представляет собой результат последовательных усилий ряда стран по разработке единых критериев оценки безопасности ИТ.

Начиная с 1970-х гг., службами безопасности США проводились исследования в области формальных методов оценки безопасности ИТ. В начале 1980-х гг. был разработан набор критериев TCSEC (Trusted Computer System Evaluation Criteria), который стал известен как «Оранжевая книга», а в 1993 г. были разработаны «Федеральные критерии безопасности информационных технологий». В период с 1991 по 1993 гг. аналогичные критерии были разработаны и в других странах: «Гармонизированные критерии европейских стран», «Канадские критерии оценки доверенных компьютерных продуктов».

В 1993 г. правительственные организации Великобритании, Германии, Канады, Нидерландов, США и Франции начали разработку «Общих критериев» (Common Criteria for IT Security Evaluation). Версия 1.0 документа была завершена в январе 1996 г. и одобрена международной организацией по стандартизации (ISO) уже в апреле 1996 г. В мае 1998 г. была опубликована версия 2.0. На основе версии 2.0 в июне 1999 г. был принят международный стандарт ISO/IEC 15408, который состоял из трех частей:

- ◆ 15408-1:1999 «Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель»;
- ◆ 15408-2:1999 «Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности»;
- ◆ 15408-3:1999 «Критерии оценки безопасности ИТ. Часть 3. Требования доверия к безопасности».

С целью унификации процедуры сертификации по «Общим критериям» практически одновременно разрабатывались версии документа, известного под названием «Общая методология оценки», который в дальнейшем был принят в качестве международного стандарта ISO/IEC 18045 «Information technology – Security techniques – Methodology for IT security evaluation».

В 2000 г. ряд стран подписали Соглашение о взаимном признании сертификатов на изделия ИТ, полученных на основе «Общих критериев». Участие в Соглашении предполагает соблюдение двух условий: признание сертификатов, выданных органами по сертификации других стран-участниц, а также возможность осуществления сертификации. Соглашение о взаимном признании оценок на конец 2013 г. подписали 26 стран. В рамках Соглашения в 17 странах действуют аккредитованные органы по сертификации.

Российская Федерация также присоединилась к работам по проведению сертификации в соответствии с методологией международного стандарта 15408.

В 2002 г. Постановлением Госстандарта Российской Федерации от 4.04.2002 г. № 133-ст был принят стандарт ГОСТ Р ИСО/МЭК 15408–2002 (3 части), который содержал полный аутентичный текст международного стандарта ISO/IEC 15408:1999. Стандарт был введен в действие 01.01.2004 г.

Стандарт состоит из трех отдельных, но взаимосвязанных частей.

- ◆ Часть 1 «Введение и общая модель» (15408-1) является введением в стандарт. В ней определяются общие понятия и принципы оценки безопасности ИТ и приводится общая модель оценки.
- ◆ Часть 2 «Функциональные компоненты безопасности» (15408-2) устанавливает совокупность функциональных компонентов, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать функциональные требования к объекту

оценки. ИСО/МЭК 15408-2 содержит каталог функциональных компонентов, систематизированных по семействам и классам.

- ◆ Часть 3 «Компоненты доверия к безопасности» (15408-3) устанавливает совокупность компонентов доверия, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать требования доверия к объекту оценки. ИСО/МЭК 15408-3 содержит каталог компонентов доверия, систематизированных по семействам и классам. Кроме того, в ИСО/МЭК 15408-3 определены критерии оценки профилей защиты и заданий по безопасности и представлены семь предопределенных пакетов доверия, которые названы оценочными уровнями доверия.

Также в 2002 г. Гостехкомиссией России были разработаны руководящие документы (из трех частей), соответствующие данному стандарту, которые были направлены на обеспечение практического использования ГОСТ Р ИСО/МЭК 15408–2002 в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ. Руководящие документы предназначались также для органов сертификации и испытательных лабораторий, аккредитованных в системе сертификации средств ЗИ по требованиям безопасности информации, для использования при проведении оценки и сертификации безопасности ИТ. К сожалению, эти руководящие документы в дальнейшем не изменялись в связи с принятием новых версий стандарта.

В 2008 г. стандарт, принятый в 2002 г., был заменен на новую версию, ГОСТ Р ИСО/МЭК 15408–2008 (3 части), которая была идентична международному стандарту ISO/IEC 15408:2005.

Наконец, в 2012 г. была произведена очередная замена части 1 стандарта 2008 г. на версию ГОСТ Р ИСО/МЭК 15408-1–2012, которая введена в действие 01.12.2013 г. и идентична международному стандарту ISO/IEC 15408-1:2009.

В 2013 г. приняты вторая и третья обновленные части ГОСТ Р ИСО/МЭК 15408-2–2013 и ГОСТ Р ИСО/МЭК 15408-3–2013. Они введены в действие 01.09.2014 г. и идентичны международным стандартам ISO/IEC 15408-2:2008 и 15408-3:2008 соответственно.

Наряду с этим стандартом претерпел ряд изменений и соответствующий национальный стандарт на основе международного ISO/IEC 18045. Последняя его версия, ГОСТ Р ИСО/МЭК 18045–2013, принята в 2013 г. и введена в действие 01.07.2014 г.

На сегодняшний день ISO/IEC 15408 является самым полным и современным оценочным стандартом. На его основе формируются два вида

используемых на практике нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты определенного класса (например, межсетевые экраны прикладного уровня).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых позволит решить поставленные задачи по обеспечению безопасности (например, межсетевой экран прикладного уровня Х-1 версии 1.1). ЗБ служит основой для проведения оценки ОО с целью демонстрации соответствия его требованиям безопасности. Поэтому один и тот же ПЗ можно использовать в качестве шаблона для множества различных ЗБ, которые будут применяться в различных оценках. Обычно ЗБ описывает требования для ОО и его формирует разработчик ОО, в то время как ПЗ описывает общие требования для некоторого типа ОО и поэтому обычно разрабатывается сообществом пользователей или разработчиков.

Стандарт предназначен для трех групп специалистов: разработчиков, оценщиков и пользователей объекта оценки. Он также может служить справочным материалом для всех, кто интересуется вопросами безопасности ИТ или несет ответственность за них, например:

- ◆ лиц, ответственных за техническое состояние оборудования, и сотрудников служб безопасности, ответственных за определение и выполнение политики и требований безопасности организации в области ИТ;
- ◆ аудиторов, как внутренних, так и внешних, ответственных за оценку адекватности безопасности ИТ-решения;
- ◆ проектировщиков систем безопасности, ответственных за характеристики безопасности продуктов ИТ;
- ◆ аттестующих, ответственных за приемку ИТ-решения в эксплуатацию в конкретной среде;
- ◆ заявителей, заказывающих оценку и обеспечивающих ее проведение;
- ◆ органов оценки, ответственных за руководство и надзор за программами проведения оценок безопасности ИТ.

Под объектом оценки в стандарте понимается аппаратно-программный продукт или информационная система с соответствующей документацией. Объект оценки рассматривается в конкретной среде безопасности, в которую включается все, что имеет отношение к его безопасности, а именно:

- ◆ законодательная среда — законы и нормативные акты, затрагивающие ОО;

- ◆ административная среда – положения политик безопасности, учитывающие особенности ОО;
- ◆ процедурная среда – физическая среда ОО и меры физической защиты, персонал и его свойства, принятые эксплуатационные и иные процедуры;
- ◆ программно-техническая среда – назначение объекта оценки и предполагаемые области его применения, активы, которые требуют защиты средствами ОО.

В процессе оценки достигается определенный уровень уверенности в том, что функциональные возможности безопасности продуктов ИТ, а также меры доверия, предприняты по отношению к продуктам ИТ, отвечают предъявляемым требованиям. Результаты оценки могут помочь потребителям решить, отвечают ли продукты ИТ их потребностям в безопасности.

Стандарт ИСО/МЭК 15408 направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования (конфиденциальность, целостность и доступность). Однако некоторые аспекты безопасности ИТ находятся вне рамок стандарта:

- ◆ Стандарт не содержит критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к функциональным возможностям безопасности ИТ. Однако безопасность в значительной степени может достигаться или поддерживаться административными мерами, такими как организационные меры, меры управления персоналом, меры управления физической защитой и процедурные меры.
- ◆ Не затрагивается оценка некоторых специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения.
- ◆ Не рассматривается методология оценки, в рамках которой могут применяться конкретные критерии. Данная методология приведена в ИСО/МЭК 18045.
- ◆ Не рассматривается административно-правовая структура, в рамках которой критерии могут применяться органами оценки.
- ◆ Вне области действия стандарта находятся процедуры использования результатов оценки при аттестации.
- ◆ Не входят в стандарт критерии для оценки специфических качеств криптографических алгоритмов.

4.2. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1-2012

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» введен в действие 01.12.2013 г. взамен ранее принятого стандарта ГОСТ Р ИСО/МЭК 15408-1-2008. Он идентичен международному стандарту ISO/IEC 15408-1:2009 «Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model».

Стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки. В нем представлены краткий обзор и описание всех частей ИСО/МЭК 15408, определены термины и сокращения, используемые во всех частях стандарта, установлены основные понятия объекта оценки, контекста оценки, описана целевая аудитория, которой адресованы критерии оценки. Представлены основные положения, необходимые для оценки продуктов ИТ.

Стандарт вводит 148 понятий, часть из которых приведена далее. Следует отметить, что в предыдущей версии стандарта (15408-1-2008) содержалось всего 64 термина и некоторые из них определялись несколько иначе.

Объект оценки — совокупность программного, программно-аппаратного и/или аппаратного обеспечения, возможно, сопровождаемая руководствами.

Класс — совокупность семейств, объединенных общим назначением.

Семейство — совокупность компонентов, которые направлены на достижение сходной цели, но различаются акцентами или строгостью.

Компонент — наименьшая выбираемая совокупность элементов, на которой могут основываться требования.

Элемент — неделимое изложение некоторой потребности в безопасности.

Оценочный уровень доверия — набор требований доверия, представляющий некоторое положение на предопределенной шкале доверия и составляющий пакет доверия.

Профиль защиты — независимое от реализации изложение потребностей в безопасности для некоторого типа ОО.

Задание по безопасности — зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного ОО.

Цель безопасности — изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

Требование безопасности — требование, изложенное на стандартизированном языке и направленное на достижение целей безопасности для ОО.

Оценка задания по безопасности — оценивание ЗБ по определенным критериям.

Среда функционирования — среда, в которой функционирует ОО.

Безопасность в ИСО/МЭК 15408 рассматривается с использованием совокупности базовых понятий безопасности: актив, владелец актива, риск, угрозы, контрмеры, источники угроз. Взаимосвязь этих понятий в стандарте представлена схемой, приведенной на рис. 4.1.

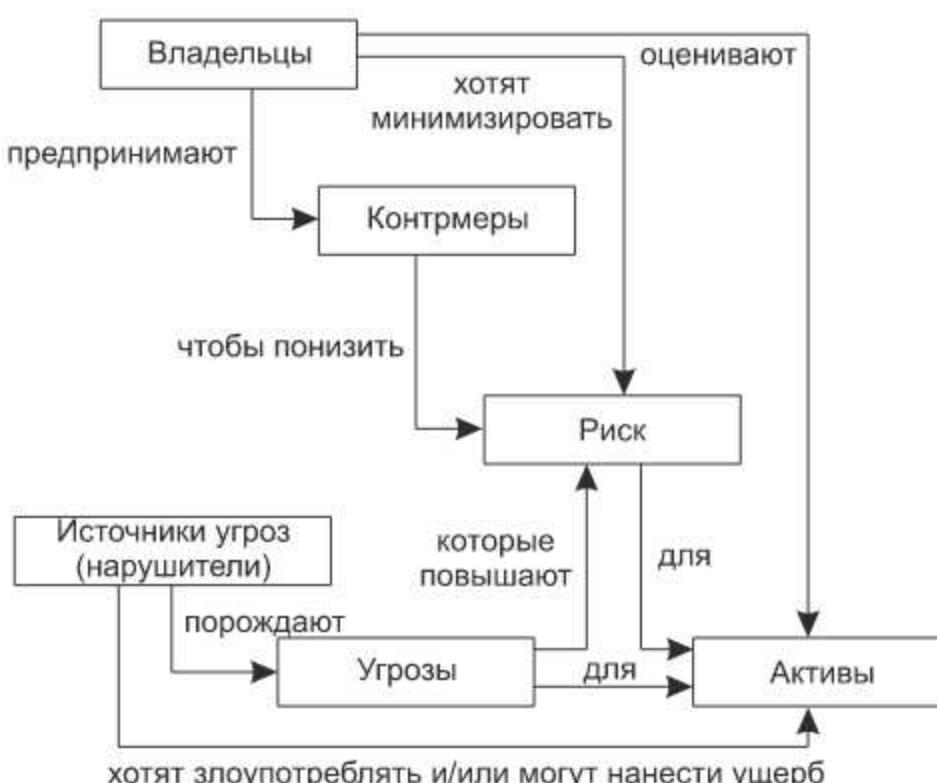


Рис. 4.1. Взаимосвязь понятий безопасности

Владельцы информации оценивают активы и предпринимают соответствующие контрмеры для их защиты от угроз, которые порождаются нарушителями с целью несанкционированного доступа к активам и нанесения ущерба организации. Контрмеры предпринимаются с целью понижения риска активам до некоторого приемлемого уровня, который определяется организацией в зависимости от ценности актива и возможного ущерба от реализации угроз безопасности.

Предпринимая контрмеры, организации должны получить уверенность в том, что они являются корректными и достаточными для минимизации риска до приемлемого уровня. Такая уверенность достигается оценкой контрмер. Взаимосвязь понятий при оценке предпринимаемых владельцами активов контрмер представлена в стандарте в виде схемы, приведенной на рис. 4.2.

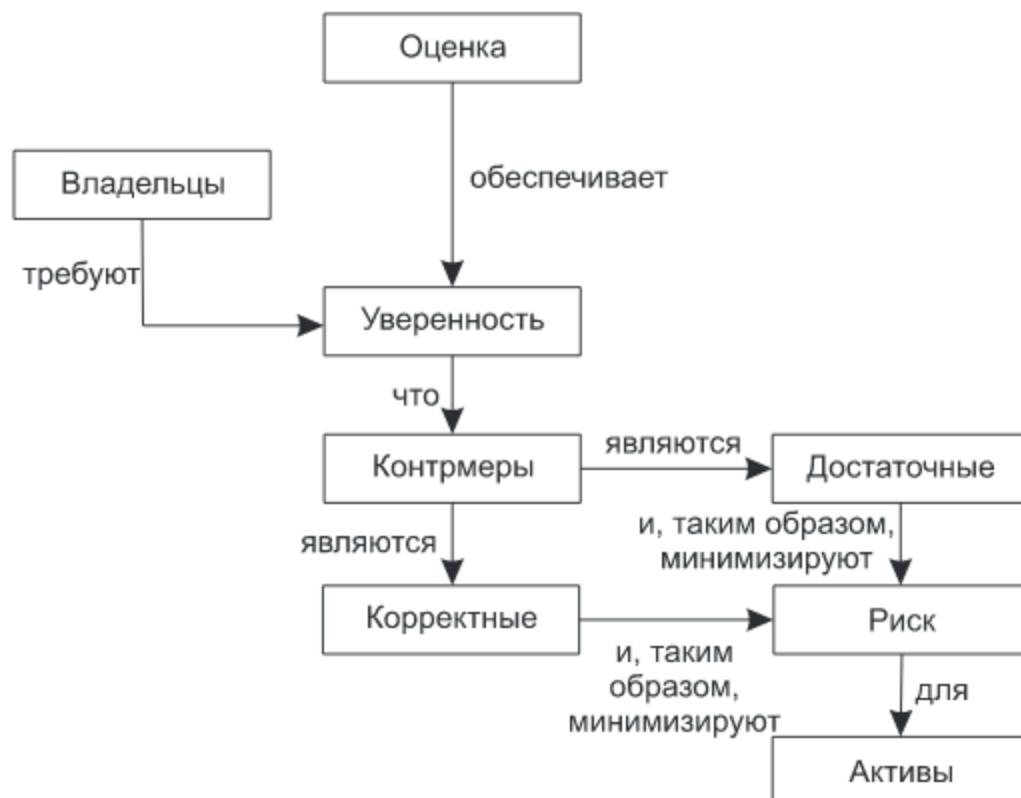


Рис. 4.2. Взаимосвязь понятий при оценке контрмер

При оценке достаточность контрмер анализируется через конструкцию, называемую заданием по безопасности. ЗБ начинается с описания активов и угроз этим активам. Затем в задании по безопасности описываются контрмеры (в форме целей безопасности) и демонстрируется, что данные контрмеры являются достаточными, чтобы противостоять описанным угрозам.

В задании по безопасности контрмеры делятся на две группы:

- ◆ цели безопасности для ОО – они описывают контрмеры, корректность которых будет определяться при оценке;
- ◆ цели безопасности для среды функционирования – они описывают контрмеры, корректность которых не будет определяться при оценке.

В задании по безопасности для ОО, корректность контрмер которого будут оценивать, требуется дальнейшая детализация целей безопасности для ОО в функциональных требованиях безопасности. ФТБ предъявляются к функциям безопасности и реализующим их механизмам безопасности. Эти ФТБ формулируют на стандартном языке, описанном во второй части стандарта (ИСО/МЭК 15408-2).

Таким образом, в задании по безопасности демонстрируется следующее:

- ◆ ФТБ удовлетворяют целям безопасности для ОО;
- ◆ цели безопасности для ОО и цели безопасности для среды функционирования противостоят угрозам;

- ◆ следовательно, ФТБ и цели безопасности для среды функционирования противостоят угрозам.

Из этого следует, что корректный ОО (удовлетворяющий ФТБ) в сочетании с корректной средой функционирования (удовлетворяющей целям безопасности для среды функционирования) будет противостоять угрозам.

В ИСО/МЭК 15408 среда функционирования не оценивается, и предполагается, что она является на 100 % правильным отражением целей безопасности для среды функционирования.

Для определения корректности ОО могут выполняться различные виды деятельности, например:

- ◆ тестирование ОО;
- ◆ исследование различных проектных представлений ОО;
- ◆ исследование физической безопасности среды разработки ОО.

Задание по безопасности обеспечивает структурированное описание этих видов деятельности для определения корректности в форме требований доверия к безопасности, которые формулируются на стандартном языке, описанном в ИСО/МЭК 15408-3. Требования доверия предъявляются к технологии и процессу разработки и эксплуатации ОО и призваны гарантировать адекватность реализации механизмов безопасности.

По стандарту ИСО/МЭК 15408 признают два типа оценки: оценка ЗБ/ОО и оценка ПЗ. Оценка ЗБ/ОО проходит в два этапа:

- ◆ оценка ЗБ – на этом этапе определяют достаточность ОО и среды функционирования;
- ◆ оценка ОО – на этом этапе определяют корректность ОО.

Оценку ЗБ выполняют путем применения критериев оценки заданий по безопасности (которые определены в разделе ASE ИСО/МЭК 15408-3). Конкретный способ применения критериев ASE определяется используемой методологией оценки.

Оценка ОО является более комплексной. Основные исходные данные для оценки ОО: свидетельства оценки, которые включают ОО и ЗБ, а также, как правило, исходные данные, получаемые из среды разработки, такие как проектная документация или результаты тестирования разработчиком. Оценка ОО заключается в применении ТДБ (из задания по безопасности) к свидетельствам оценки. Конкретный способ применения конкретного ТДБ определяется используемой методологией оценки.

Результатом процесса оценки ОО будет:

- ◆ либо утверждение, что не все ТДБ удовлетворены и поэтому не достигнут заданный уровень доверия к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ;
- ◆ либо утверждение, что все ТДБ удовлетворены и поэтому достигнут заданный уровень доверия к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ.

Оценка ОО может быть выполнена после завершения разработки ОО или параллельно с разработкой ОО.

Кроме понятий ПЗ и ЗБ в стандарте введено понятие «пакет» — это именованный набор требований безопасности. Пакеты делятся на

- ◆ функциональные пакеты, включающие только ФТБ;
- ◆ пакеты доверия, включающие только ТДБ.

Смешанные пакеты, включающие как ФТБ, так и ТДБ, недопустимы. Пакет может быть определен какой-либо стороной и предназначен для многократного использования. В настоящее время не существует критериев оценки пакетов, поэтому любой набор ФТБ или ТДБ может быть пакетом. Примерами пакетов доверия являются ОУД, определенные в ИСО/МЭК 15408-3.

Оценки профилей защиты позволяют создавать каталоги (реестры) оцененных ПЗ. Стандарт ИСО/МЭК 15408-3 содержит критерии оценки, которые оценщику необходимо принять во внимание для того, чтобы установить, является ли ПЗ полным, непротиворечивым, технически правильным и, следовательно, пригодным для использования при разработке ЗБ.

Оценка ЗБ дает промежуточные результаты, которые затем используются при оценке ОО.

ИСО/МЭК 15408-3 содержит критерии оценки, которые оценщику необходимо принять во внимание для того, чтобы установить, существует ли достаточное доверие к тому, что ОО удовлетворяет ФТБ из ЗБ. Оценки ЗБ/ОО позволяют создавать каталоги (реестры) оцененных ОО.

После оценки ЗБ и ОО у владельцев активов имеется доверие к тому, что ОО вместе со средой функционирования противостоят конкретным угрозам. При этом владелец активов должен тщательно проверить следующее:

- ◆ соответствует ли определение проблемы безопасности в ЗБ конкретной проблеме безопасности владельца активов;
- ◆ соответствует ли среда функционирования у владельца активов (или может ли быть обеспечено ее соответствие) целям безопасности для среды функционирования, описанным в ЗБ.

Следует иметь в виду, что после ввода оцененного ОО в эксплуатацию сохраняется возможность проявления в ОО ранее неизвестных ошибок или уязвимостей.

В приложениях А и В стандарта изложено обязательное содержание задания по безопасности и профиля защиты. На рис. 4.3 и 4.4 представлены структурные схемы ЗБ и ПЗ, как они изображены в стандарте.



Рис. 4.3. Структурная схема ЗБ

ЗБ обычно содержит:

- ◆ раздел «Введение ЗБ», в котором дано описание ОО на трех различных уровнях абстракции;
- ◆ раздел «Утверждения о соответствии», указывающий, утверждается ли в ЗБ о соответствии каким-либо ПЗ и/или пакетам, и если да, то каким ПЗ и/или пакетам;
- ◆ раздел «Определение проблемы безопасности», в котором указываются угрозы, политика безопасности организации и предположения;
- ◆ раздел «Цели безопасности», показывающий, каким образом решение проблемы безопасности распределено между целями безопасности для ОО и целями безопасности для среды функционирования ОО;

- ◆ раздел «Определение расширенных компонентов», в котором могут быть определены новые компоненты (то есть компоненты, не содержащиеся в ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3). Эти новые компоненты необходимы, чтобы определить расширенные функциональные требования и расширенные требования доверия;
- ◆ раздел «Требования безопасности», в котором цели безопасности для ОО преобразованы в изложение на стандартизированном языке. Этот стандартизованный язык представляет собой форму представления ФТБ. Кроме того, в рассматриваемом разделе определяют ТДБ;
- ◆ раздел «Краткая спецификация ОО», показывающий, как ФТБ реализованы в ОО.



Рис. 4.4. Структурная схема ПЗ

Профиль защиты содержит:

- ◆ раздел «Введение ПЗ», включающий описание типа ОО;
- ◆ раздел «Утверждения о соответствии», указывающий, утверждается ли в ПЗ о соответствии каким-либо ПЗ и/или пакетам, и если да, то каким ПЗ и/или пакетам;
- ◆ раздел «Определение проблемы безопасности», в котором указываются угрозы, политика безопасности и предположения;

- ◆ раздел «Цели безопасности», показывающий, каким образом решение проблемы безопасности распределено между целями безопасности для ОО и целями безопасности для среды функционирования ОО;
- ◆ раздел «Определение расширенных компонентов», в котором могут быть определены новые компоненты (не содержащиеся в ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3). Эти новые компоненты необходимы, чтобы определить расширенные функциональные требования и расширенные требования доверия;
- ◆ раздел «Требования безопасности», в котором цели безопасности для ОО преобразованы в изложение на стандартизированном языке. Этот стандартизованный язык представляет собой форму представления ФТБ. Кроме того, в рассматриваемом разделе определяют ТДБ.

4.3. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2-2013

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» введен в действие 01.09.2014 г. взамен ранее принятого стандарта ГОСТ Р ИСО/МЭК 15408-2-2008. Он идентичен международному стандарту ISO/IEC 15408-2:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components».

Данная часть стандарта устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также содержит каталог функциональных компонентов безопасности, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов ИТ, которые могут быть предъявлены к объекту оценки.

ОО может включать ресурсы в виде электронных носителей данных (таких, как основная память, дисковое пространство), периферийных устройств (таких, как принтеры) и вычислительных возможностей (таких, как процессорное время), которые могут использоваться для обработки и хранения информации и являются предметом оценки.

Оценка прежде всего подтверждает, что в отношении ресурсов ОО применяется конкретный набор функциональных требований безопасности, определяющих правила, по которым ОО управляет использованием своих ресурсов и доступом к ним и, таким образом, к информации и сервисам, контролируемым ОО.

ОО может быть единым продуктом, включающим аппаратные, программно-аппаратные и программные средства.

Существуют два типа пользователей, учитываемых в стандарте: человек-пользователь и внешняя сущность ИТ. Человека-пользователя можно дифференцировать как локального человека-пользователя, взаимодействующего непосредственно с ОО через устройства ОО (такие, как рабочие станции), и как удаленного человека-пользователя, взаимодействующего с ОО через другой продукт ИТ.

Для структуризации функциональных требований в стандарте введена иерархия «класс – семейство – компонент – элемент». Классы определяют наиболее общую (предметную) группировку требований. Семейства в пределах класса различаются по строгости и другим характеристикам требований. Компонент – минимальный набор требований, фигурирующий как целое. Элемент – неделимое требование. Принципиальная упрощенная модель такой иерархии приведена на рис. 4.5.

Каждый функциональный класс содержит имя класса, представление класса и одно или несколько функциональных семейств. Имя класса содержит информацию, необходимую для идентификации функционального класса и отнесения его к определенной категории. Информация о категории представлена кратким именем, состоящим из трех букв латинского алфавита (например, FIA – идентификация и аутентификация).

Имя семейства содержит описательную информацию, необходимую для того, чтобы идентифицировать и категорировать функциональное семейство. Каждое функциональное семейство имеет уникальное имя. Информация о категории состоит из краткого имени, включающего в себя семь символов. Первые три символа идентичны краткому имени класса, далее следуют символ подчеркивания и краткое имя семейства в виде XXX_YYY. Уникальная краткая форма имени семейства предоставляет основное имя ссылки для компонентов (например, FIA_UID – идентификация пользователя).

Идентификация компонента включает в себя описательную информацию, необходимую для идентификации, категорирования, записи и реализации перекрестных ссылок компонента. Для каждого функционального компонента предоставляется следующее:

- ◆ уникальное имя, отражающее предназначение компонента;
- ◆ краткое имя, uniquely отражающее класс и семейство, которым компонент принадлежит, а также номер компонента в семействе;
- ◆ список иерархических связей, содержащий имена других компонентов.

Например, компонент с именем FIA_UID.1 означает «выбор момента идентификации». Он устанавливает требования по идентификации

пользователей. Автор ПЗ/ЗБ может указать конкретные действия, которые могут быть выполнены до завершения процесса идентификации пользователя.

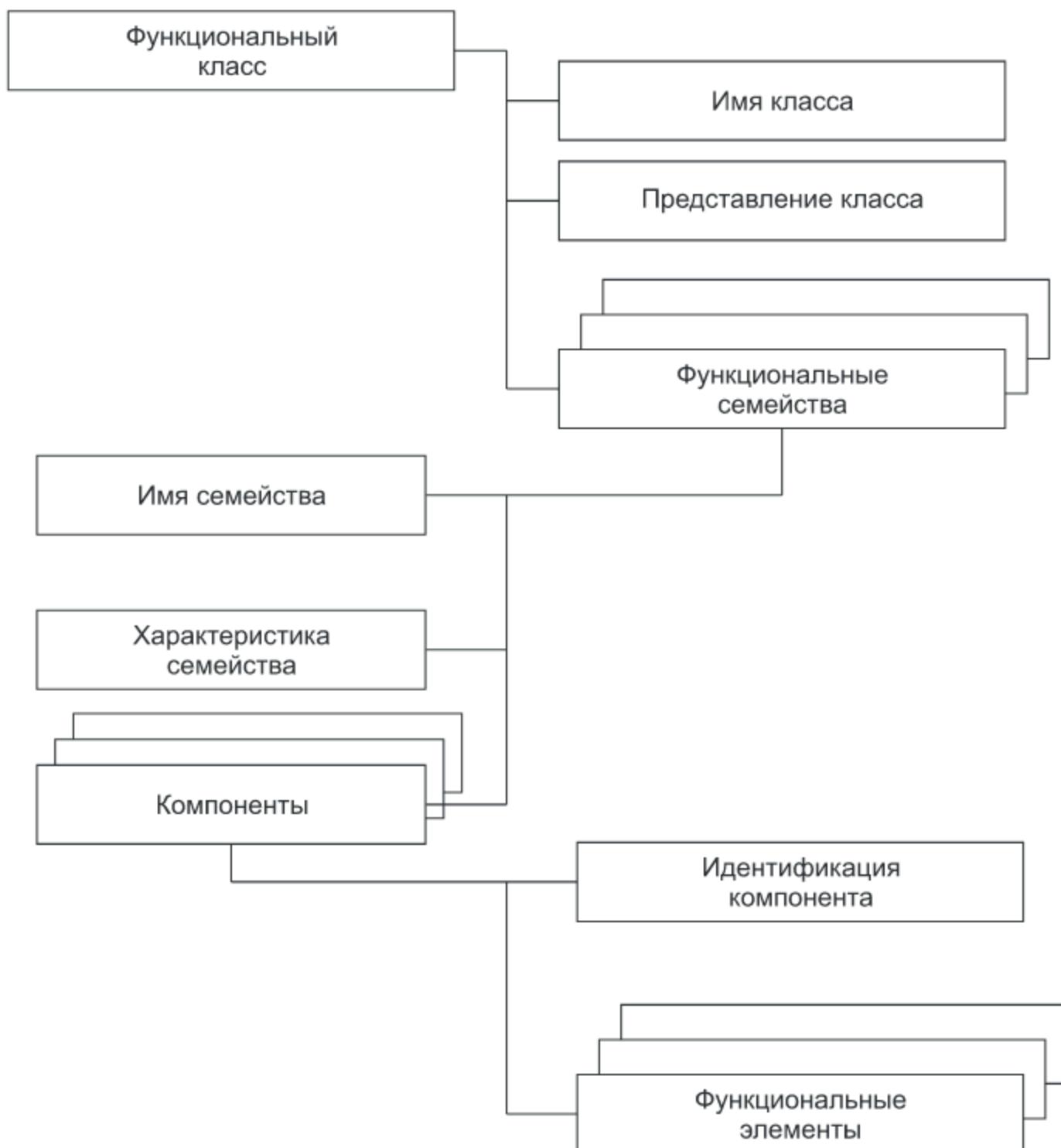


Рис. 4.5. Иерархия функциональных требований

Компонент с именем FIA_UID.2 означает «идентификация до любых действий пользователя». Он содержит требование обязательной идентификации пользователей, причем до идентификации пользователя функциональные возможности безопасности объекта оценки не допускают выполнение им никаких действий.

Во второй части стандарта ИСО/МЭК 15408-2-2013 содержится систематизированный каталог функциональных требований безопасности, разбитый на 11 классов, 65 семейств и 133 компонента. В версии стандарта 2008 г. были описаны 11 классов, 66 семейств и 135 компонентов.

Список имен функциональных классов приведен в табл. 4.1.

Таблица 4.1. Список функциональных классов

Имя класса	Количество семейств	Количество компонентов
FAU — аудит безопасности	6	15
FCO — связь	2	4
FCS — криптографическая поддержка	2	5
FDP — защита данных пользователя	13	31
FIA — идентификация и аутентификация	6	14
FMT — управление безопасностью	7	14
FPR — приватность	4	10
FPT — защита ФБО	14	23
FRU — использование ресурсов	3	6
FTA — доступ к ОО	6	9
FTP — доверенный маршрут/канал	2	2

Для примера в табл. 4.2 представлена расшифровка семейств для класса FIA.

Таблица 4.2. Список семейств класса FIA

Имя	Наименование	Характеристика
FIA_AFL	Отказы аутентификации	Задается реакция на неудачные запросы аутентификации
FIA_ATD	Определение атрибутов пользователя	Определяет требования для ассоциации атрибутов безопасности с пользователями
FIA_SOS	Спецификация секретов	Задаются требования к механизмам проверки качества и генерации секретов
FIA_UAU	Аутентификация пользователя	Задаются требования к реализации механизма аутентификации
FIA_UID	Идентификация пользователя	Задается порядок идентификации пользователя. Определяются действия, доступные до идентификации
FIA_USB	Связывание «пользователь — субъект»	Определяется связь атрибутов безопасности пользователя с субъектом, действующим от его имени

4.4. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3-2013

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» введен в действие 01.09.2014 г. взамен ранее принятого стандарта ГОСТ Р ИСО/МЭК 15408-3-2008. Он идентичен международному стандарту ISO/IEC 15408-3:2008 «Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance components».

Данная часть ИСО/МЭК 15408 устанавливает требования доверия и включает оценочные уровни доверия, определяющие шкалу для измерения доверия для ОО, составные пакеты доверия, определяющие шкалу для измерения доверия для составных ОО, отдельные компоненты доверия, из которых составлены уровни и пакеты доверия, а также критерии для оценки ПЗ и ЗБ.

Основной концепцией стандарта является обеспечение доверия, основанное на оценке продукта ИТ, который должен соответствовать определенным критериям безопасности. Нарушения безопасности ИТ возникают вследствие преднамеренного использования или непреднамеренной активации уязвимостей нарушителями при применении ИТ по назначению. Следует предпринять ряд шагов для предотвращения уязвимостей, возникающих в продуктах ИТ. По возможности уязвимости следует:

- ◆ устраниТЬ, то есть предпринять активные действия для их выявления, а затем удаления или нейтрализации;
- ◆ минимизировать, то есть предпринять активные действия для уменьшения до допустимого остаточного уровня возможного ущерба от любого проявления уязвимостей;
- ◆ отслеживать, то есть предпринять активные действия для обнаружения любой попытки использовать остаточные уязвимости с тем, чтобы ограничить ущерб.

В соответствии со стандартом доверие рассматривается как основа для уверенности в том, что продукт ИТ отвечает целям безопасности. Стандарт обеспечивает доверие с использованием активного исследования — оценки продукта ИТ для определения его свойств безопасности.

Методы оценки могут включать в себя:

- ◆ анализ и проверку процессов и процедур;
- ◆ проверку того, что процессы и процедуры действительно применяются;
- ◆ анализ соответствия между представлениями проекта ОО;
- ◆ анализ соответствия каждого представления проекта ОО требованиям;
- ◆ верификацию доказательств;
- ◆ анализ руководств;
- ◆ анализ разработанных функциональных тестов и предоставленных результатов;
- ◆ независимое функциональное тестирование;
- ◆ анализ уязвимостей, включающий предположения о недостатках;
- ◆ тестирование проникновения.

Все требования доверия в стандарте сгруппированы в 8 классов, 38 семейств и 88 компонентов, которые, в свою очередь, содержат элементы доверия. В предыдущей версии стандарта 2008 г. были установлены 10 классов, 44 семейства и 93 компонента.

Иерархическая структура представления требований доверия («класс – семейство – компонент – элемент») примерно соответствует аналогичной структуре функциональных требований, определенной в стандарте ИСО/МЭК 15408-2. Структура требований доверия, как она представлена в стандарте, изображена на рис. 4.6.

В табл. 4.3 приведен перечень классов требований доверия.



Рис. 4.6. Иерархия требований доверия

Таблица 4.3. Классы требований доверия

Имя класса	Количество семейств	Количество компонентов
APE — оценка ПЗ	6	8
ASE — оценка ЗБ	7	10
ADV — разработка	6	19
AGD — руководства	2	2
ALC — поддержка жизненного цикла	7	21
ATE — тестирование	4	12
AVA — оценка уязвимостей	1	5
ACO — композиция	5	11

В табл. 4.4 приведены характеристики семейств доверия для некоторых классов.

Таблица 4.4. Характеристики семейств доверия

Имя	Наименование	Характеристика
<i>Класс ATE — тестирование</i>		
ATE_COV	Покрытие	Предъявляются требования к анализу полноты функциональных тестов, проведенных разработчиком
ATE_DPT	Глубина	Определяется уровень детализации, на котором разработчик проверяет ОО
ATE_FUN	Функциональное тестирование	Задаются требования к содержанию функционального тестирования разработчиком
ATE_IND	Независимое тестирование	Определяется порядок независимого контроля результатов тестирования
<i>Класс AGD — руководства</i>		
AGD_OPE	Руководство пользователя по эксплуатации	Задаются требования к составу и содержанию руководств для всех типов пользователей
AGD_PRE	Подготовительные процедуры	Задаются требования к описанию порядка приемки и установки ОО

В стандарте введено понятие ОУД. Уровни представляют собой рассчитанную на многократное использование комбинацию требований доверия, содержащую не более одного компонента из каждого семейства. ОУД образуют возрастающую шкалу (от 1-го до 7-го), которая позволяет соотнести получаемый уровень доверия со стоимостью и самой возможностью достижения этой степени доверия.

Предполагается, что на практике при разработке ПЗ и ЗБ будут использоваться эти стандартные ОУД либо ОУД, дополненные новыми и компонентами. Сводное описание оценочных уровней доверия представлено в табл. 4.5. Следует обратить внимание на то, что не все семейства и компоненты, описанные в стандарте, включены в ОУД. Предполагается, что эти семейства и их компоненты будут использоваться для усиления конкретных ОУД в тех ПЗ и ЗБ, для которых они полезны.

ОУД1 предусматривает функциональное тестирование. Он применим, когда требуется некоторая уверенность в правильном функционировании ОО, а угрозы безопасности не рассматриваются как серьезные. Он будет полезен там, где требуется независимо полученное доверие к утверждению, что было уделено должное внимание защите информации с низким уровнем значимости. ОУД1 обеспечивает оценку ОО путем независимого тестирования на соответствие спецификации и экспертизы представленной документации. Предполагается, что оценка по ОУД1 может успешно проводиться без помощи разработчика ОО и с минимальными затратами. При оценке на этом уровне следует предоставить свидетельство, что ОО функционирует в соответствии с его документацией.

ОУД2 предусматривает структурное тестирование. Он содержит требование сотрудничества с разработчиком для получения информации о проекте и результатах тестирования. ОУД2 применим, когда разработчикам или пользователям требуется независимо подтвержденный уровень доверия от невысокого до умеренного при отсутствии доступа к полной документации по разработке. Такая ситуация может возникать при обеспечении безопасности разработанных ранее (наследуемых) систем или при ограниченной доступности разработчика.

ОУД2 обеспечивает значимое увеличение доверия по сравнению с ОУД1, требуя тестирования ОО и анализа уязвимостей разработчиком, а также независимое тестирование, основанное на более детализированных спецификациях ОО.

ОУД3 предусматривает методическое тестирование и проверку. Он применим, когда разработчикам или пользователям требуется независимо подтвержденный умеренный уровень доверия на основе всестороннего исследования ОО и процесса его разработки без существенных затрат на изменение технологии проектирования.

ОУД3 обеспечивает значимое увеличение доверия по сравнению с ОУД2, требуя более полного покрытия тестированием функциональных возможностей и механизмов безопасности и/или процедур безопасности, что дает некоторую уверенность в том, что в ОО не будут внесены искажения во время разработки.

Таблица 4.5. Описание оценочных уровней доверия

Класс доверия	Семейство доверия	Компоненты доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC	-	1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP	-	-	-	1	1	2	2
	ADV_INT	-	-	-	-	2	3	3
	ADV_SPM	-	-	-	-	-	1	1
	ADV_TDS	-	1	2	3	4	5	6
Руководства	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL	-	1	1	1	1	1	1
	ALC_DVS	-	-	1	1	1	2	2
	ALC_FLR	-	-	-	-	-	-	-
	ALC_LCD	-	-	1	1	1	1	2
	ALC_TAT	-	-	-	1	2	3	3
Оценка задания по безопасности	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD	-	1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Тестирование	ATE_COV	-	1	2	2	2	3	3
	ATE_DPT	-	-	1	2	3	3	4
	ATE_FUN	-	1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_VAN	1	2	2	3	4	5	5

ОУД4 предусматривает методическое проектирование, тестирование и углубленную проверку. Он позволяет разработчику достичь максимального доверия путем применения надлежащего проектирования безопасности. ОУД4 является самым высоким уровнем, на который экономически целесообразно ориентироваться при оценке уже существующих продуктов.

Поэтому ОУД4 применим, когда разработчикам или пользователям требуется независимо подтвержденный уровень доверия от умеренного до высокого в ОО общего назначения и имеется готовность нести дополнительные, связанные с обеспечением безопасности производственные затраты.

ОУД4 также обеспечивает доверие посредством использования мер управления средой разработки и дополнительного управления конфигурацией ОО, включая автоматизацию и свидетельство о безопасности процедур поставки. ОУД4 обеспечивает значимое увеличение доверия по сравнению с ОУД3, требуя более детального описания проекта, представления реализации для всех ФБО и улучшенных механизмов и/или процедур, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки.

ОУД5 предусматривает полуформальное проектирование и тестирование. Он позволяет разработчику достичь максимального доверия путем проектирования безопасности, основанного на строгой коммерческой практике разработки и поддержанного умеренным применением специализированных методов проектирования безопасности. Поэтому ОУД5 применим, когда разработчикам или пользователям требуется независимо получаемый высокий уровень доверия для запланированной разработки со строгим подходом к разработке, не влекущим за собой излишних затрат на применение узкоспециализированных методов проектирования безопасности.

ОУД5 также обеспечивает доверие посредством использования контроля среды разработки и всестороннего управления конфигурацией ОО. Он обеспечивает значимое увеличение доверия по сравнению с ОУД4, требуя полуформального описания проекта, более структурированной (и, следовательно, лучше анализируемой) архитектуры и улучшенных механизмов и/или процедур, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки.

ОУД6 предусматривает полуформальную верификацию и тестирование проекта. Он позволяет разработчикам достичь высокого доверия путем применения методов проектирования безопасности в строго контролируемой среде разработки с целью получения высококачественного ОО для защиты высоко оцениваемых активов от значительных рисков. Поэтому ОУД6 применим для разработки безопасных ОО с целью использования в условиях высокого риска, где ценность защищаемых активов оправдывает дополнительные затраты. Доверие дополнительно достигается применением формальной модели выбранной политики безопасности ОО, а также проекта ОО.

Анализ поддержан независимым тестированием ФБО, свидетельством разработчика о тестировании, основанном на функциональной спецификации, проекте ОО, выборочным независимым подтверждением результатов тестирования разработчиком и независимым анализом уязвимостей,

демонстрирующим противостояние попыткам проникновения нарушителей с высоким потенциалом нападения.

ОУД6 обеспечивает значимое увеличение доверия по сравнению с ОУД5, требуя проведения более всестороннего анализа, структурированного представления реализации, более стройной структуры (например, с разбиением на уровни), более всестороннего независимого анализа уязвимостей, а также улучшенного управления конфигурацией и улучшенного контроля среды разработки.

ОУД7 предусматривает формальную верификацию проекта и тестирование. Он применим при разработке безопасных ОО для использования в условиях чрезвычайно высокого риска и/или там, где высокая ценность активов оправдывает повышенные затраты. Доверие дополнительно достигается применением формальной модели выбранной политики безопасности ОО. Анализ поддержан независимым тестированием ФБО, свидетельством разработчика о тестировании, основанном на функциональной спецификации, проекте ОО и представлении реализации, полным независимым подтверждением результатов тестирования разработчиком и независимым анализом уязвимостей, демонстрирующим противостояние попыткам проникновения нарушителей с высоким потенциалом нападения.

ОУД7 обеспечивает значимое увеличение доверия по сравнению с ОУД6, требуя более всестороннего анализа, использующего формальные представления и формальное соответствие, а также всестороннего тестирования.

В целом рынок ИТ составляют производители, предлагающие отдельные продукты и технологии. Бывают случаи, когда производители аппаратного обеспечения ПК могут предлагать также прикладное программное обеспечение и/или операционные системы, а производитель микросхем (чипов) может разработать специализированную ОС под свой чипсет. Но в основном наблюдаются ситуации, когда ИТ-решения реализуются несколькими производителями.

Иногда существует потребность в доверии к объединению (композиции) компонентов в дополнение к доверию, полученному для каждого отдельного компонента. Недостаточность информации, предоставленной разработчиком компонента, на который полагается другой компонент, приводит к тому, что разработчик зависимого компонента не имеет доступа к информации, необходимой для оценки базового и зависимого компонентов по ОУД2 и выше. Таким образом, хотя оценка зависимого компонента может быть проведена на любом уровне доверия, для объединения нескольких компонентов с ОУД2 и выше необходимо повторно использовать свидетельства и результаты оценки, проведенной разработчиком.

Для оценки составного ОО разработчиком предоставляется ЗБ, в котором идентифицируются все пакеты доверия, которые применимы к составному

ОО, предоставляя доверие составной сущности путем получения доверия, достигнутого при оценке компонентов.

Цель рассмотрения композиции компонентов в ЗБ – подтвердить совместимость компонентов с точки зрения среды функционирования и требований, а также оценить соответствие ЗБ составного ОО заданиям по безопасности его компонентов и представленных в этих ЗБ политик безопасности.

Для оценки составных ОО в ГОСТ Р ИСО/МЭК 15408-3-2013 по сравнению с ГОСТ Р ИСО/МЭК 15408-3-2008 введено новое понятие «составной пакет доверия». СоПД образуют возрастающую шкалу, которая позволяет соотнести уровень полученного доверия с затратами и возможностью достижения этой степени доверия для составных ОО.

СоПД применяются к составным ОО, которые содержат компоненты, прошедшие (или проходящие) оценку как ОО-компоненты. Отдельные компоненты должны быть сертифицированы по ОУД или другому пакету доверия, указанному в ЗБ.

Хотя зависимый компонент может быть оценен с использованием ранее оцененных и сертифицированных базовых компонентов для удовлетворения требований, предъявляемых к ИТ-платформе в среде функционирования, это не обеспечивает какого-либо формального уровня доверия к взаимодействию компонентов или к учету возможного появления уязвимостей при объединении компонентов. Составные пакеты доверия учитывают такие взаимодействия и на более высоких уровнях доверия обеспечивают то, что интерфейсы между компонентами являются предметом тестирования. Также выполняется анализ уязвимостей составного ОО с целью учета возможного появления уязвимостей вследствие объединения компонентов.

В табл. 4.6 представлен обзор СоПД. В столбцах указаны иерархически упорядоченные СоПД, в строках – семейства доверия. Каждая цифра в полученной матрице определяет конкретный компонент доверия. Важно отметить, что лишь небольшая часть семейств и компонентов доверия из ИСО/МЭК 15408-3 включена в составные пакеты доверия. Это связано с тем, что они основываются на результатах оценки ранее оцененных компонентов, и в связи с этим нельзя говорить, что они не обеспечивают значимое и требуемое доверие.

СоПД иерархически упорядочены, поскольку каждый последующий обеспечивает большее доверие, чем все СоПД более низкого уровня. Увеличение доверия от СоПД к СоПД достигается путем замены компонента доверия на более высокий по иерархии компонентов доверия из того же семейства доверия (то есть усилением строгости, области охвата и/или глубины) и путем добавления компонентов доверия из других семейств доверия (то есть путем добавления новых требований).

Таблица 4.6. Описание составных пакетов доверия

Класс доверия	Семейство доверия	Компоненты доверия в СоПД		
		СоПД-А	СоПД-В	СоПД-С
Композиция	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
Руководства	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	1	1
	ALC_CMS	2	2	2
Оценка задания по безопасности	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD	-	1	1
	ASE_TSS	1	1	1

Составной уровень доверия А (СоПД-А) предусматривает структурную композицию. Он применим, когда составной ОО интегрирован и требуется уверенность в корректности безопасного функционирования результирующей композиции. Поэтому СоПД-А применим в тех случаях, когда разработчикам или пользователям требуется независимо подтвержденный уровень доверия к безопасности от низкого до умеренного при отсутствии прямой доступности полной информации о разработке. СоПД-А обеспечивает доверие путем анализа задания по безопасности для составного ОО.

Составной уровень доверия В (СоПД-В) предусматривает методическую композицию. Он применим в тех случаях, когда разработчикам или пользователям требуется независимо подтвержденный умеренный уровень доверия к безопасности на основе всестороннего исследования составного ОО и процесса его разработки без существенного реинжиниринга (восстановления процесса проектирования). СоПД-В демонстрирует значительное увеличение уровня доверия по сравнению с СоПД-А, требуя более полного охвата тестированием функциональных возможностей безопасности.

Составной уровень доверия С (СоПД-С) предусматривает методическую композицию, тестирование и проверку. Он позволяет разработчику достичь максимального доверия на основе точного анализа взаимосвязей между компонентами составного ОО, который, несмотря на строгость, не требует полного доступа ко всем свидетельствам базового компонента. Поэтому СоПД-С применим, когда разработчикам или пользователям требуется независимо подтвержденный уровень доверия к безопасности от умеренного до высокого для ОО общего назначения и они готовы нести дополнительные затраты на проектирование, связанные с обеспечением безопасности. Пакет дает значительное увеличение уровня доверия по сравнению с СоПД-В, требуя большего описания проекта и демонстрации противостояния нарушителям с более высоким потенциалом нападения.

4.5. Национальный стандарт ГОСТ Р ИСО/МЭК 18045–2013

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 18045–2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» введен в действие 01.07.2014 г. взамен ранее принятого стандарта ГОСТ Р ИСО/МЭК 18045–2008. Он идентичен международному стандарту ISO/IEC 18045:2008 «Information technology – Security techniques – Methodology for IT security evaluation».

Стандарт описывает минимум действий, выполняемых оценщиком при проведении оценки по ИСО/МЭК 15408. Потенциальными пользователями этого стандарта являются оценщики, применяющие ИСО/МЭК 15408, и органы по сертификации, подтверждающие действия оценщика, а также заявители оценки, разработчики, авторы ПЗ/ЗБ и другие стороны, заинтересованные в безопасности ИТ.

Термин «методология» в стандарте определен как система принципов, процедур и процессов, применяемых для оценки безопасности ИТ.

Общая модель методологии оценки представлена на рис. 4.7. Каждый тип оценки (оценка ПЗ, оценка ОО, оценка ЗБ) проводится в рамках единого процесса и включает четыре общие задачи для оценщика:

- ◆ задачу получения исходных данных для оценки;
- ◆ задачу выполнения подвидов деятельности по оценке;
- ◆ задачу оформления результатов оценки;
- ◆ задачу демонстрации технической компетентности органу по оценке.

Общая модель определяет следующие роли: заявителя, разработчика, оценщика и органа оценки. Заявитель предъявляет запрос об оценке и отвечает за поддержание процесса оценки. Разработчик создает ОО и отвечает за представление необходимых для оценки свидетельств (тестовая документация, проектная документация, исходный код или схемы аппаратуры).

Оценщик выполняет задачи оценки, требуемые в контексте оценки: получает свидетельства, выполняет подвиды деятельности по оценке и предоставляет результаты оценивания органу оценки. Оценщик выносит вердикт относительно выполнения требований ИСО/МЭК 15408.

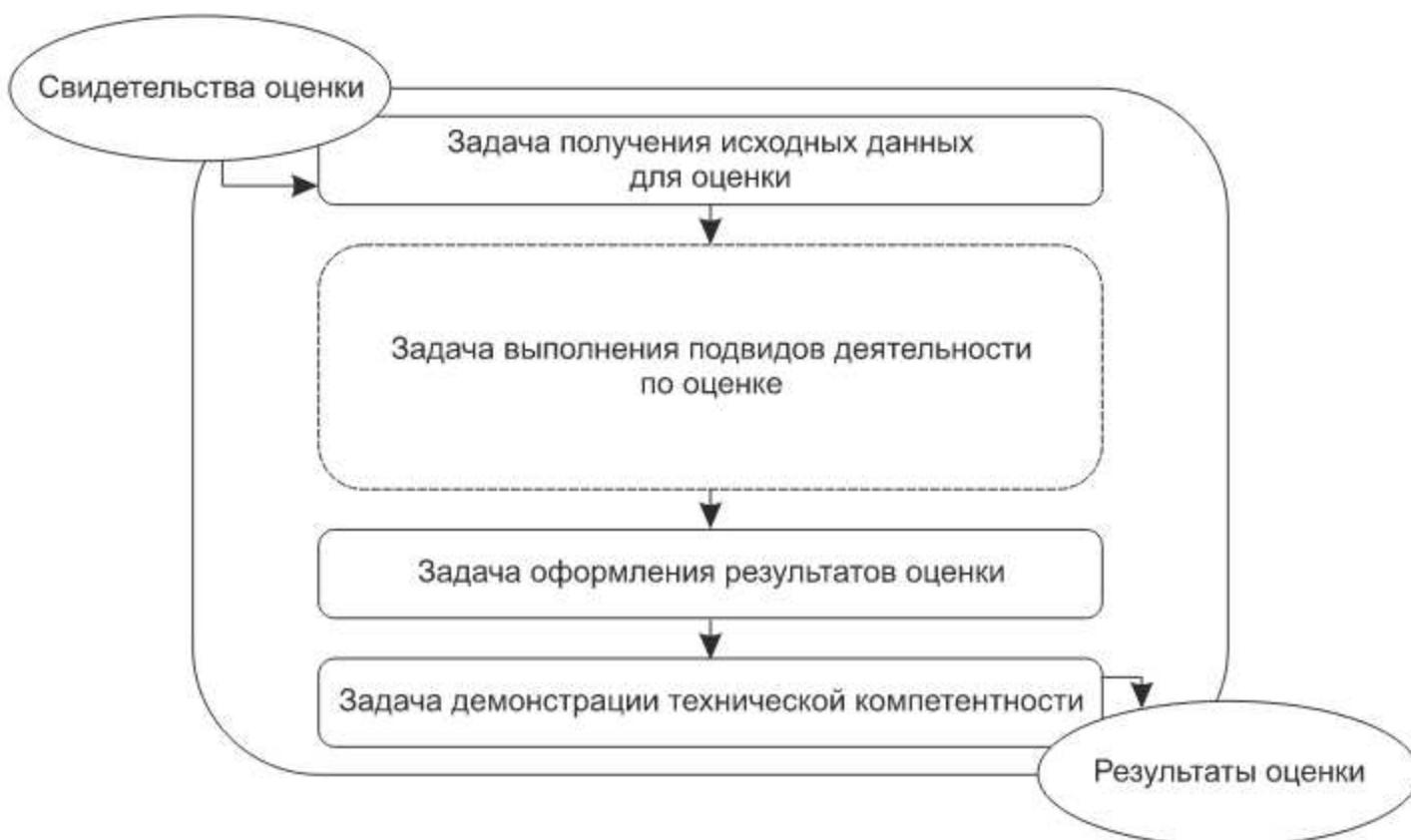


Рис. 4.7. Общая модель оценки

Орган оценки устанавливает и поддерживает систему оценки, контролирует процесс оценки, проводимый оценщиком, выпускает отчеты о сертификации, а также сертификаты, основанные на результатах оценки, предоставленных оценщиком.

В стандарте различаются три взаимоисключающих вида вердикта.

1. Условиями положительного вердикта являются завершение оценщиком элемента действий оценщика из ИСО/МЭК 15408 и определение того, что требования к оцениваемому ПЗ, ЗБ или ОО выполнены.
2. Условиями отрицательного вердикта являются завершение оценщиком элемента действий оценщика из ИСО/МЭК 15408 и определение того, что требования к оцениваемому ПЗ, ЗБ или ОО не выполнены или что

свидетельства оценки не являются логически связанными и однозначно понятными, а также при выявлении явной несогласованности в свидетельствах оценки.

3. Все вердикты поначалу неокончательные и остаются такими до вынесения положительного или отрицательного вердикта.

Общий вердикт положительный тогда и только тогда, когда все составляющие вердикта положительные.

Во время проведения оценки оценщик может получить доступ к коммерческой или иной защищаемой информации заявителя и разработчика, поэтому системы оценки могут предъявить к оценщику требования по обеспечению конфиденциальности свидетельств оценки. Требования конфиденциальности затрагивают многие аспекты проведения оценки, включая получение, обработку, хранение и дальнейшее использование свидетельств оценки.

Результаты оценки оформляются в виде технического отчета об оценке, имеющего структуру, представленную на рис. 4.8.

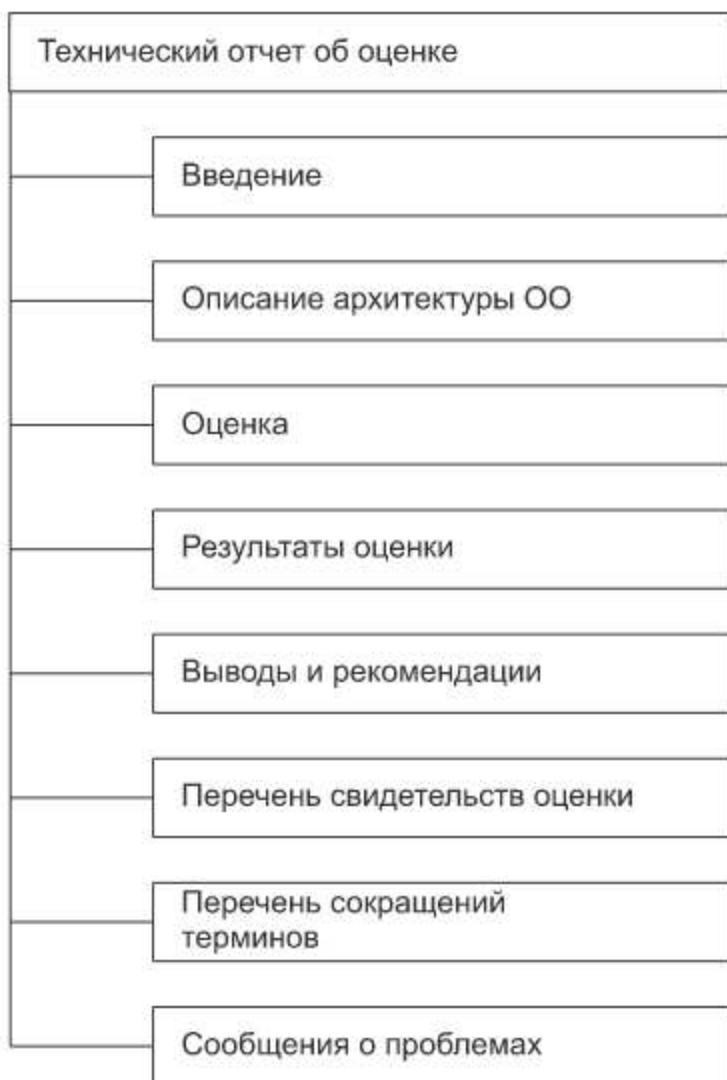


Рис. 4.8. Структура отчета об оценке

Введение должно содержать следующую информацию:

- ◆ идентификаторы системы оценки;
- ◆ идентификаторы контроля конфигурации ТОО (название, дата, номер версии и т. д.);
- ◆ идентификаторы контроля конфигурации ЗБ и ОО;
- ◆ ссылку на ПЗ;
- ◆ идентификатор разработчика;
- ◆ идентификатор заявителя;
- ◆ идентификатор оценщика.

Оценщик должен привести в отчете высокоуровневое описание объекта оценки и его главных компонентов.

В разделе «Оценка» оценщик должен привести сведения о методах оценки, технологии, инструментальных средствах и применяемых стандартах. Оценщик может сослаться на критерии оценки, методологию и интерпретации, использованные при оценке ОО, или на устройства, применяемые при тестировании, а также может включить в отчет информацию о правовых или законодательных аспектах, организации работ, конфиденциальности и т. д.

В разделе «Результаты оценки» для каждого вида деятельности приводятся название рассматриваемого вида деятельности и вердикт, сопровождаемый обоснованием, для каждого компонента доверия.

В разделе «Выводы и рекомендации» оценщик должен привести выводы по результатам оценки об удовлетворении ОО требованиям своего ЗБ, а также дать рекомендации, которые могут быть полезны для органа оценки. Эти рекомендации могут указывать на недостатки продукта ИТ, обнаруженные во время оценки, или упоминать о его свойствах, которые особенно полезны.

Оценщик о каждом свидетельстве оценки должен привести в отчете следующую информацию:

- ◆ наименование составителя свидетельства (например, разработчик, заявитель);
- ◆ название свидетельства;
- ◆ уникальную ссылку на свидетельство (например, дату составления и номер версии).

Оценщик должен привести в отчете перечень всех сокращений, используемых в ТОО.

В разделе «Сообщения о проблемах» оценщик должен привести полный перечень, уникально идентифицирующий все СП, подготовленные во время оценки, а также их статус.

СП предоставляют оценщику механизм для запроса разъяснений (например, от органа оценки о применении требований) или для определения проблемы по одному из аспектов оценки. При отрицательном вердикте оценщик должен представить СП для отражения результата оценки. Для каждого СП в перечне следует привести идентификатор СП, а также название или аннотацию.

В любом СП оценщик должен привести следующее:

- ◆ идентификатор оцениваемого ПЗ или ОО;
- ◆ задачу/подвид деятельности по оценке, при выполнении которой/которого проблема была выявлена;
- ◆ суть проблемы;
- ◆ оценку ее серьезности (например, приводит к отрицательному вердикту, задерживает выполнение оценки или требует решения до завершения оценки);
- ◆ наименование организации, ответственной за решение вопроса;
- ◆ рекомендуемые сроки решения;
- ◆ определение влияния на оценку отсутствия решения проблемы.

В стандарте подробно описаны методология оценки и указания по организации процесса оценки для каждого из восьми классов требований доверия согласно ИСО/МЭК 15408-3–2013 (APE, ASE, ADV, AGD, ALC, ATE, AVA, ACO), приведенных ранее в табл. 4.3.

В приложении к стандарту представлено общее руководство по учету зависимостей между различными видами и подвидами деятельности и действиями по оценке, которые необходимо учитывать оценщику в процессе оценки.

4.6. Национальный стандарт ГОСТ Р ИСО/МЭК 51583–2014

Национальный стандарт Российской Федерации ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» введен в действие 01.09.2014 г. Стандарт введен впервые.

Он распространяется на создаваемые и модернизируемые информационные автоматизированные системы, в отношении которых законодательством

или заказчиком установлены требования по их защите, и устанавливает содержание и порядок выполнения работ на стадиях и этапах создания АС в защищенном исполнении, содержание и порядок выполнения работ по защите информации о создаваемой (модернизируемой) АСЗИ.

Положения данного стандарта дополняют положения комплекса стандартов по АС в части порядка создания АС в защищенном исполнении:

- ◆ ГОСТ 34.003–90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ◆ ГОСТ 34.201–89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ◆ ГОСТ 34.601–90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ◆ ГОСТ 34.602–89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ◆ ГОСТ 34.603–92 «Информационная технология. Виды испытаний автоматизированных систем».

Кроме того, стандарт рекомендует использовать при создании АСЗИ следующие национальные стандарты: ИСО/МЭК 15408 (3 части), ИСО/МЭК 27002, ИСО/МЭК 27005, ИСО/МЭК 19791, ИСО/МЭК 18045, ИСО/МЭК 15446.

В стандарте введены следующие термины.

Мероприятия по защите информации — совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

Обработка информации — выполнение любого действия (операции) или совокупности действий (операций) с информацией (например, сбор, накопление, ввод, вывод, прием, передача, запись, хранение, регистрация, преобразование, отображение и т. п.), совершаемых с заданной целью.

Система защиты информации автоматизированной системы — совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий

и технических средств (формулировка совпадает с таковой в федеральном законе № 149-ФЗ).

Целью создания системы ЗИ в АСЗИ является обеспечение ЗИ от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа, реализация права на доступ к информации.

Обеспечение ЗИ в АСЗИ достигается заданием, реализацией и контролем выполнения требований о защите информации:

- ◆ к процессу хранения, передачи и обработки защищаемой в АСЗИ информации;
- ◆ системе ЗИ;
- ◆ взаимодействию АСЗИ с другими АС;
- ◆ условиям функционирования АСЗИ;
- ◆ содержанию работ по созданию (модернизации) АСЗИ на различных стадиях и этапах ее создания (модернизации);
- ◆ организациям (должностным лицам), участвующим в создании (модернизации) и эксплуатации АСЗИ;
- ◆ документации на АСЗИ;
- ◆ АСЗИ в целом.

Процесс создания АСЗИ должен представлять собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнения которых необходимо и достаточно для создания АСЗИ, соответствующей требованиям к ней.

Для АСЗИ, создаваемой на базе действующей АС, разрабатывают ТЗ на создание системы ЗИ, в которое включают требования к системе ЗИ.

Для подтверждения соответствия системы ЗИ в АСЗИ в реальных условиях эксплуатации требованиям безопасности информации осуществляется аттестация АСЗИ на соответствие требованиям безопасности информации. Аттестация АСЗИ проводится до ввода АСЗИ в постоянную эксплуатацию.

Создание системы ЗИ АСЗИ обеспечивается следующим комплексом работ:

- ◆ формированием требований к системе ЗИ АСЗИ;
- ◆ разработкой (проектированием) системы ЗИ АСЗИ;
- ◆ внедрением системы ЗИ АСЗИ;

- ◆ аттестацией АСЗИ на соответствие требованиям безопасности информации и вводом ее в действие;
- ◆ сопровождением системы ЗИ в ходе эксплуатации АСЗИ.

Внедрение системы ЗИ АСЗИ включает:

- ◆ установку и настройку СЗИ;
- ◆ разработку организационно-распорядительных документов, определяющих мероприятия по ЗИ в ходе эксплуатации АСЗИ;
- ◆ предварительные испытания системы ЗИ АСЗИ;
- ◆ опытную эксплуатацию и доработку системы ЗИ АСЗИ;
- ◆ приемочные испытания системы ЗИ АСЗИ;
- ◆ аттестацию АСЗИ на соответствие требованиям безопасности информации.

На этапе «Подготовка персонала» проводят:

- ◆ обучение персонала АСЗИ и проверку его способности обеспечивать функционирование системы ЗИ и АСЗИ в целом;
- ◆ проверку и подготовку специалистов структурного подразделения или должностного лица (работника), ответственных за ЗИ в АСЗИ.

На этапе «Проведение опытной эксплуатации» выполняют:

- ◆ проверку функционирования системы ЗИ в составе АСЗИ, в том числе реализованных мер ЗИ;
- ◆ анализ выявленных в ходе опытной эксплуатации системы ЗИ уязвимостей АСЗИ, доработку, наладку системы ЗИ;
- ◆ проверку готовности пользователей и администраторов к эксплуатации системы ЗИ АСЗИ;
- ◆ оформление акта о завершении опытной эксплуатации системы ЗИ АСЗИ.

Аттестацию АСЗИ на соответствие требованиям безопасности информации организует заказчик, проводит организация, имеющая лицензию на данный вид деятельности, до ввода АСЗИ в эксплуатацию с использованием информационных ресурсов, подлежащих защите. Аттестация содержит оценку соответствия системы ЗИ требованиям безопасности информации в реальных условиях эксплуатации, проводимую в соответствии с требованиями нормативных правовых актов и методических документов уполномоченного федерального органа исполнительной власти, а также национальных стандартов в области защиты информации.

Составной частью работ по созданию АСЗИ является защита информации о создаваемой АСЗИ.

Основными видами работ по ЗИ о создаваемых (модернизируемых) АСЗИ являются:

- ◆ разработка замысла ЗИ о создаваемой (модернизируемой) АСЗИ;
- ◆ определение защищаемой информации о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания;
- ◆ определение носителей защищаемой информации о создаваемой (модернизируемой) АСЗИ и их уязвимостей, актуальных угроз безопасности информации;
- ◆ определение и технико-экономическое обоснование организационных и технических мероприятий, которые необходимо проводить в интересах ЗИ о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания;
- ◆ обоснование, разработка и/или закупка средств, необходимых для ЗИ о создаваемой (модернизируемой) АСЗИ;
- ◆ обоснование и разработка мероприятий по контролю состояния ЗИ о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания;
- ◆ разработка документов, регламентирующих организацию и осуществление ЗИ о создаваемой (модернизируемой) АСЗИ.

К защищаемой информации о создаваемой (модернизируемой) АСЗИ относят:

- ◆ цель и задачи ЗИ в АСЗИ;
- ◆ перечень составных частей (сегментов) АСЗИ, участвующих в обработке защищаемой в АСЗИ информации;
- ◆ состав возможных уязвимостей АСЗИ, возможных последствий от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальность, целостность, доступность);
- ◆ структурно-функциональные характеристики АСЗИ, включающие структуру и состав АСЗИ, физические, функциональные и технологические взаимосвязи между составными частями АСЗИ и взаимосвязи с иными системами, режимы обработки информации в АСЗИ в целом и в ее отдельных составных частях;
- ◆ меры и СЗИ, применяемые в АСЗИ;
- ◆ сведения о реализации системы ЗИ в АСЗИ.

Применительно к конкретной АСЗИ перечень защищаемой информации устанавливает заказчик.

Общее руководство работами по ЗИ при создании (модернизации) АСЗИ осуществляется один из заместителей руководителя организации (предприятия), реализующей ее разработку (модернизацию), или уполномоченное лицо.

В дополнение к рассмотренному стандарту с 01.07.2015 г. введены в действие еще три национальных стандарта, касающихся различных аспектов защиты автоматизированных систем в защищенном исполнении от преднамеренных силовых электромагнитных воздействий:

- ◆ ГОСТ Р 56093–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования»;
- ◆ ГОСТ Р 56103–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения»;
- ◆ ГОСТ Р 56115–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования».

Под преднамеренным силовым электромагнитным воздействием понимается электромагнитное воздействие, осуществляемое путем применения излучателей электромагнитного поля или магнитного поля, генераторов напряжения и тока и приводящее к наводкам с амплитудой, длительностью и энергией, вызывающим нарушение нормального функционирования электронных устройств.

Под защитой информации от преднамеренного воздействия понимается деятельность, направленная на предотвращение преднамеренного силового воздействия различной физической природы на защищаемую информацию от сбоя технических и программных средств ИС, приводящего к искажению, уничтожению, блокированию доступа к информации, уничтожению или нарушению функционирования носителя информации, а также к нарушению самого информационного процесса.

Стандарт ГОСТ Р 56115–2014 распространяется на средства защиты автоматизированных систем в защищенном исполнении от преднамеренных силовых электромагнитных воздействий. В стандарте приводится классификация этих средств защиты АСЗИ по виду предотвращаемой угрозы, специальным свойствам, назначению, местоположению, степени защиты, а также устанавливаются различные требования к их функционированию и безопасности.

Стандарт ГОСТ Р 56093–2014 распространяется на средства обнаружения преднамеренных силовых электромагнитных воздействий на технические

средства АСЗИ. Он устанавливает требования к средствам обнаружения факта преднамеренных силовых электромагнитных воздействий на АСЗИ, а также к средствам обнаружения, которые обеспечивают формирование данных о характеристиках преднамеренных силовых электромагнитных воздействий.

Стандарт ГОСТ Р 56103–2014 устанавливает общие положения по организации и содержанию работ по построению системы защиты АСЗИ от преднамеренных силовых электромагнитных воздействий. Работы по защите АС от таких воздействий являются составной частью комплекса работ, выполняемых согласно ГОСТ Р 51583, и распространяются как на стадию создания АСЗИ, так и на процесс ее эксплуатации.

Необходимость защиты АС от электромагнитных воздействий обусловлена:

- ◆ существованием разнообразных видов воздействий на АС по цепям электропитания, линиям связи, металлоконструкциям, посредством электромагнитного поля, деструктивное воздействие которых может привести к искажению, уничтожению или блокированию информации;
- ◆ наличием и доступностью приобретения/изготовления технических средств, являющихся источниками электромагнитных воздействий;
- ◆ значительностью функциональных нарушений штатной деятельности технических средств АС при оказании на них преднамеренных электромагнитных воздействий.

4.7. Национальный стандарт ГОСТ Р ИСО/МЭК 19791–2008

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 19791–2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» введен в действие 01.10.2009 г. Он идентичен международному стандарту ISO/IEC/TR 19791:2006 «Information technology – Security techniques – Security assessment of operational systems».

Стандарт содержит дополнительные правила (процедуры) к международным стандартам серии ИСО/МЭК 15408 в интересах оценки безопасности АС. Требования, установленные в стандартах серии ИСО/МЭК 15408, обеспечивают задание и определение функциональных возможностей безопасности продуктов и систем, входящих в состав информационных технологий. Однако стандарты этой серии не рассматривают некоторые критические (важные) аспекты безопасности АС, которые должны быть четко специфицированы для их эффективного оценивания.

В стандартах серии ИСО/МЭК 15408 рассматриваются только технические меры безопасности и родственные им управленческие меры. В АС технические меры безопасности и организационные меры безопасности объединены для защиты информации и других активов организации.

Настоящий стандарт содержит критерии оценки и рекомендации по оценке аспектов безопасности, связанных как с информационными технологиями, так и с применением их в АС. Он прежде всего предназначен для тех, кто связан с разработкой, интеграцией, развертыванием АС и управлением их безопасностью, а также для организаций, оказывающих услуги по оценке соответствия.

Стандарт устанавливает:

- ◆ определение и модель АС;
- ◆ описание расширений концепции оценки безопасности с помощью стандартов серии ИСО/МЭК 15408, необходимых для оценки АС;
- ◆ методологию и процесс выполнения оценки безопасности АС;
- ◆ дополнительные критерии оценки безопасности, охватывающие те аспекты АС, которые не были охвачены критериями оценки безопасности в стандартах серии ИСО/МЭК 15408.

Он дает возможность включать продукты безопасности, оцененные в соответствии с требованиями стандартов серии ИСО/МЭК 15408, в АС и проводить оценку как единого целого с использованием настоящего стандарта.

В стандарте дается формулировка ряда терминов.

Меры обеспечения безопасности – управленческие, организационные и технические меры обеспечения безопасности, применяемые в информационной системе для защиты и доступности системы и ее информации.

Управленческие меры безопасности – меры безопасности информационной системы, направленные на менеджмент рисков и менеджмент информационной безопасности информационных систем.

Организационные меры безопасности – меры безопасности информационной системы, которые реализуются и выполняются главным образом операторами, а не системами.

Технические меры безопасности – меры безопасности информационной системы, которые реализуются и выполняются самой информационной системой через механизмы, содержащиеся в аппаратных, программных или программно-аппаратных компонентах системы.

Автоматизированная система – информационная система, включая элементы, не связанные с информационной технологией, рассматриваемые с учетом условий ее эксплуатации.

Анализ рисков – системный подход к определению величины риска.

Оценка рисков – процесс, включающий в себя идентификацию, анализ и оценивание рисков.

Менеджмент рисков – весь процесс идентификации, контроля и управления или минимизации подозрительных (неопределенных) событий, которые могут оказаться негативное воздействие на ресурсы системы.

Обработка рисков – процесс выбора и реализации мер обеспечения безопасности для изменения рисков.

Уязвимость – недостатки или слабости в проекте или реализации информационной системы, включая меры обеспечения безопасности, которые могут быть преднамеренно или непреднамеренно использованы для оказания неблагоприятного воздействия на активы организации или ее функционирование.

В целях настоящего стандарта автоматизированная система определена как информационная система (включая ее аспекты, не связанные с ИТ), рассматриваемая в контексте среды ее эксплуатации. Проблемы безопасности в АС порождаются не только из-за проблем с продуктами, но и из-за проблем в самой АС в реальной среде эксплуатации (например, неправильной настройки параметров управления доступом или правил фильтрации межсетевого экрана, плохой организации каталогов файлов и др.). Кроме того, в случае использования сети уровень безопасности АС, подключенной к этой сети, может затрагивать другие АС, которые должны взаимодействовать с ней.

Требования стандарта базируются на трехэтапном подходе к обеспечению необходимого уровня безопасности АС, представленном в стандарте в виде схемы, изображенной на рис. 4.9:

- ◆ оценивание рисков безопасности применительно к рассматриваемой системе;
- ◆ уменьшение рисков для противодействия рискам безопасности посредством выбора обеспечения безопасности или устранения этих рисков;
- ◆ аттестация для подтверждения того, что риски, остающиеся в системе после применения мер обеспечения безопасности, являются приемлемыми для эксплуатации системы.

В стандарте используется подход к оценке безопасности, основанный на модели оценки, определенной в стандартах серии ИСО/МЭК 15408, но распространенный на все типы мер обеспечения безопасности.

Оценка АС состоит из следующих этапов:

- ◆ определение целей безопасности для АС, которые уменьшат неприемлемые риски до приемлемого уровня;

- ◆ выбор и спецификация технических и организационных мер безопасности, которые соответствуют целям безопасности АС, с учетом уже реализованных мер обеспечения безопасности;
- ◆ определение конкретных измеримых требований доверия как к техническим, так и к организационным мерам обеспечения безопасности для достижения необходимого уровня уверенности в том, что АС соответствует целям безопасности;
- ◆ фиксирование принятых решений в задании по безопасности;
- ◆ оценка конкретной АС с тем, чтобы сделать вывод о ее соответствии ЗБ;
- ◆ периодическая переоценка как рисков безопасности АС, так и способности АС противостоять этим рискам.

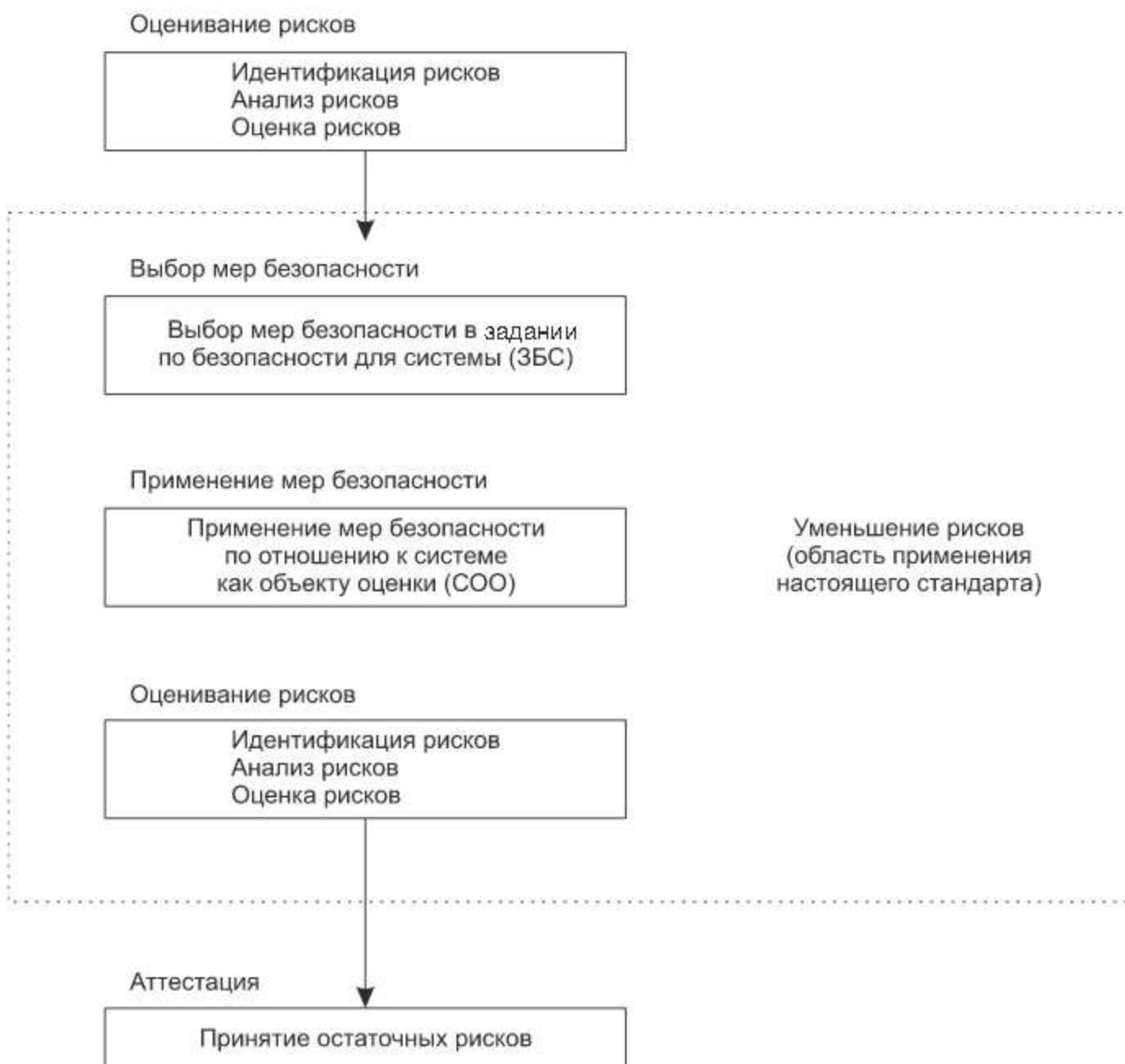


Рис. 4.9. Процесс обеспечения безопасности АС

Считается, что жизненный цикл АС состоит из следующих стадий: разработка/интеграция, установка, эксплуатация системы и модификация. Меры обеспечения безопасности АС должны подвергаться оценке в течение всего жизненного цикла системы.

На стадии разработки/интеграции первым действием по обеспечению безопасности должна быть идентификация и оценка рисков для АС. Затем доверенное должностное лицо организации (аттестующее лицо) должно рассмотреть предполагаемые остаточные риски и подтвердить, что они являются приемлемыми. В целях повышения эффективности риски безопасности, идентифицированные при оценке рисков как неприемлемые, должны быть уменьшены в соответствии с выбранными требованиями по безопасности до приемлемого уровня остаточных рисков.

Проект АС должен быть записан в задании по безопасности для АС, в котором должно содержаться описание требований по безопасности, включая риски, которым надо противодействовать, и цели безопасности, которые необходимо реализовать с помощью технических и организационных мер безопасности.

Затем создается или приобретается программное обеспечение для систем и бизнес-приложения, включая технические меры безопасности, и система интегрируется, конфигурируется и испытывается разработчиком. Одновременно создается организационная структура безопасности, формируются политики, правила и процедуры безопасности, которые интегрируются в систему.

После этого делается оценка АС, которая должна подтвердить, что все риски, детализированные в ЗБ АС, которым должны противодействовать меры обеспечения безопасности, определены как приемлемые для системы.

На стадии установки (внедрения) для использования в среде эксплуатации внедряют и подготавливают технические и организационные меры безопасности.

На стадии эксплуатации системы необходимо собирать и оценивать записи об эксплуатации технических и организационных мер безопасности. Обычно при эксплуатации системы необходимо определить ряд критически важных мер обеспечения безопасности АС с целью непрерывного мониторинга для проверки их постоянной эффективности.

На стадии модификации любые предполагаемые или фактические изменения АС, выходящие за рамки регламентного обслуживания, должны изучаться, анализироваться и при необходимости тестироваться для определения их воздействия на безопасность АС перед внедрением в процесс эксплуатации.

Процесс оценки АС подобен процессу оценки по стандартам серии ИСО/МЭК 15408. Типичное различие между оценкой АС и оценкой продукта по стандартам серии ИСО/МЭК 15408 заключается в том, что при оценке АС

фактическая среда эксплуатации рассматривается полностью (все меры обеспечения безопасности, реализованные в среде эксплуатации), тогда как при оценке продукта среда эксплуатации подробно не рассматривается, а описывается как предположения, которые не подтверждаются во время оценки.

В принципе, разница между характеристиками продукта ИТ и автоматизированной системы с точки зрения оценки безопасности невелика. Однако оценка АС может быть значительно сложнее оценки продукта по стандартам серии ИСО/МЭК 15408 по следующим причинам.

- ◆ АС может состоять из коммерческих продуктов и заказных разработок ИТ, объединенных в доменах безопасности. Состав каждого домена безопасности системы может основываться на нескольких факторах, таких как используемая технология, предоставленные функциональные возможности и критичность защищаемых активов.
- ◆ АС может содержать многочисленные примеры одного и того же продукта (например, многочисленные копии АС, предоставляемые одним и тем же продавцом) или различные многочисленные примеры продуктов одинакового типа (например, многочисленные межсетевые экраны, поставляемые различными продавцами).
- ◆ АС может иметь политики безопасности, применимые к одним доменам безопасности и не применимые к другим.
- ◆ различные остаточные риски могут быть приемлемыми в различных доменах.

Особым вопросом является доверие к эффективности мер обеспечения безопасности, реализующих функции безопасности системы. Областями, для которых требуются дополнительные компоненты доверия к управлению автоматизированными системами, являются:

- ◆ общая структура безопасности и размещение компонентов в структуре;
- ◆ конфигурация компонентов, составляющих АС;
- ◆ политики, правила и процедуры менеджмента, управляющие функционированием АС;
- ◆ требования и правила взаимодействия с другими АС;
- ◆ мониторинг не связанных с ИТ мер обеспечения безопасности во время стадии эксплуатации жизненного цикла системы.

В стандарте (приложение А) определены концепция и содержание задания по безопасности для АС (ЗБ АС) и профиля защиты для АС (ПЗ АС).

В приложении В стандарта определены функциональные требования к мерам обеспечения безопасности АС.

Стандарт предусматривает для технических мер безопасности использование классов, определенных в ИСО/МЭК 15408-2: FAU, FCO, FCS, FDP, FIA, FMT, FPR, FPT, FTA, FTP, FAU.

Дополнительно определены следующие семь новых классов для организационных мер безопасности:

- ◆ администрирование (FOD) – специфицирует требования к организационным мерам, связанным с администрированием;
- ◆ системы ИТ (FOS) – специфицирует требования к организационным мерам, поддерживающие использование систем ИТ и оборудования;
- ◆ активы пользователей (FOA) – специфицирует требования к организационным мерам, связанные с управлением активами пользователей;
- ◆ бизнес (FOB) – специфицирует требования к организационным мерам, связанные с бизнес-процессами и функциями;
- ◆ аппаратура и оборудование (FOP) – специфицирует требования к организационным мерам, связанные с оборудованием, аппаратурой и зданиями (сооружениями);
- ◆ третьи стороны (FOT) – специфицирует требования к организационным мерам, связанные с третьими сторонами;
- ◆ управление (FOM) – специфицирует требования к организационным мерам, связанные с деятельностью по менеджменту безопасности.

Для каждого нового класса функциональных требований определены соответствующие семейства и компоненты. Например, для класса FOD определены следующие 6 семейств и 10 компонентов:

- ◆ FOD_POL – администрирование политик:
 - FOD_POL.1 – политика безопасности;
 - FOD_POL.2 – политика защиты данных и приватности;
- ◆ FOD_PSN – администрирование по отношению к персоналу:
 - FOD_PSN.1 – должности и обязанности персонала;
 - FOD_PSN.2 – обеспечение осведомленности о ИБ;
- ◆ FOD_RSM – администрирование управления рисками:
 - FOD_RSM.1 – менеджмент рисков внутри организации;
 - FOD_RSM.2 – менеджмент рисков, связанных с доступом третьих сторон;
- ◆ FOD_INC – администрирование управления инцидентами:
 - FOD_INC.1 – инциденты безопасности;

- ◆ FOD_ORG – администрирование организации безопасности:
 - FOD_ORG.1 – обязанности по координации безопасности;
 - FOD_ORG.2 – обязанности заседания руководства;
- ◆ FOD_SER – администрирование соглашений об услугах:
 - FOD_SER.1 – договоры по сетевым услугам.

В приложении С стандарта определены следующие дополнительные 10 требований доверия к безопасности АС, кроме требований ИСО/МЭК 15408-3:

- ◆ оценка профиля защиты для АС (ASP) – специфицирует требования к оценке профилей защиты для АС;
- ◆ оценка ЗБ АС (ASS) – специфицирует требования к оценке заданий по безопасности для АС;
- ◆ руководства для АС (AOD) – специфицирует требования к оценке руководств для автоматизированных систем;
- ◆ документация по проектированию архитектуры АС и конфигурационная документация (ASD) – специфицирует требования к оценке документации по конфигурированию и проектированию АС;
- ◆ управление конфигурацией АС (AOC) – специфицирует требования к оценке управления конфигурацией АС;
- ◆ тестирование АС (AOT) – специфицирует требования к оценке тестирования АС;
- ◆ анализ уязвимостей АС (AOV) – специфицирует требования к оценке анализа уязвимостей АС;
- ◆ поддержка жизненного цикла АС (AOL) – специфицирует требования к оценке поддержки жизненного цикла АС;
- ◆ безопасная установка системы (ASL) – специфицирует требования к оценке безопасной установки системы;
- ◆ регистрация и запись в АС (ASO) – специфицирует требования к оценке регистрации и мониторинга организационных мер безопасности.

Для каждого нового класса требований доверия к безопасности АС определены соответствующие семейства и компоненты. Например, для класса AOD определены следующие 4 семейства и 7 компонентов:

- ◆ AOD_OCD – спецификация конфигурации АС (2 компонента);
- ◆ AOD_ADMIN – руководство администратора АС (2 компонента);
- ◆ AOD_USR – руководство пользователя АС (2 компонента);
- ◆ AOD_GVR – верификация руководств (1 компонент).

4.8. Национальный стандарт ГОСТ Р ИСО/МЭК 15446–2008

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 15446–2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» введен в действие 01.10.2009 г. Он идентичен международному стандарту ISO/IEC TR 15446:2004 ISO/IEC TR 15446:2004 «Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets».

Настоящий стандарт представляет собой информационный технический отчет ИСО, предназначенный для использования только в качестве руководства по разработке различных частей ПЗ и ЗБ продуктов и систем ИТ в соответствии с комплексом стандартов ИСО/МЭК 15408. По своему содержанию и структуре его не следует рассматривать как стандарт для оценки ПЗ и ЗБ.

Руководство предназначено для разработчиков и оценщиков профилей защиты и заданий по безопасности, а также может представлять интерес для пользователей ПЗ и ЗБ.

В стандарте приводится пример содержания ПЗ:

1. Введение ПЗ:
 - 1) идентификация ПЗ;
 - 2) аннотация ПЗ.
2. Описание ОО.
3. Среда безопасности ОО:
 - 1) предположения безопасности;
 - 2) угрозы;
 - 3) политика безопасности организации.
4. Цели безопасности:
 - 1) цели безопасности для ОО;
 - 2) цели безопасности для среды.
5. Требования безопасности ИТ:
 - 1) функциональные требования безопасности ОО;
 - 2) требования доверия к безопасности ОО;
 - 3) требования безопасности для ИТ-среды.
6. Замечания по применению.

7. Обоснование:

- 1) обоснование целей безопасности;
- 2) обоснование требований безопасности.

В разделе «Введение ПЗ» идентифицируется ПЗ и приводится его аннотация в форме, наиболее подходящей для включения в каталоги и реестры ПЗ.

В раздел «Описание ОО» включают сопроводительную информацию об ОО (или типе ОО), предназначенную для пояснения его назначения и требований безопасности.

В раздел ПЗ «Среда безопасности ОО» включают описание аспектов среды безопасности ОО, которые должны учитываться для объекта оценки (детальное описание предположений безопасности, определяющих границы среды безопасности, угроз активам, требующим защиты (включая описание этих активов), и политика безопасности организации, которой должен соответствовать ОО).

В раздел ПЗ «Цели безопасности» включают краткое изложение предполагаемой реакции на аспекты среды безопасности как с точки зрения целей безопасности, которые должны быть удовлетворены ОО, так и с точки зрения целей безопасности, которые должны быть удовлетворены ИТ- и не ИТ-мерами в пределах среды ОО.

В раздел ПЗ «Требования безопасности ИТ» включают функциональные требования безопасности ОО, требования доверия к безопасности, а также требования безопасности программного, программно-аппаратного и аппаратного обеспечения ИТ-среды ОО. Требования безопасности ИТ должны быть определены путем использования, где это возможно, функциональных компонентов и компонентов доверия к безопасности в соответствии с ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3.

В раздел ПЗ «Замечания по применению» допускается включать любую дополнительную информацию, которую разработчик ПЗ считает полезной.

В разделе ПЗ «Обоснование» демонстрируется то, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ и соответствующий ОО учитывает идентифицированные аспекты среды безопасности.

Существует также целый ряд необязательных разделов и подразделов, которые могут включаться в ПЗ. Возможны разные уровни детализации некоторых подразделов. Раздел «Обоснование» может быть оформлен в виде отдельного документа.

Пример содержания задания по безопасности представлен далее.

1. Введение ЗБ:
 - 1) идентификация ЗБ;
 - 2) аннотация ЗБ.
2. Описание ОО.
3. Среда безопасности ОО:
 - 1) предположения безопасности;
 - 2) угрозы;
 - 3) политика безопасности организации.
4. Цели безопасности:
 - 1) цели безопасности для ОО;
 - 2) цели безопасности для среды ОО.
5. Требования безопасности ИТ:
 - 1) функциональные требования безопасности ОО;
 - 2) требования доверия к безопасности ОО;
 - 3) требования безопасности для ИТ-среды.
6. Краткая спецификация ОО:
 - 1) функции безопасности ОО;
 - 2) меры обеспечения доверия к безопасности.
7. Утверждения о соответствии ПЗ:
 - 1) ссылка на ПЗ;
 - 2) уточнение ПЗ;
 - 3) дополнение ПЗ.
8. Обоснование:
 - 1) обоснование целей безопасности;
 - 2) обоснование требований безопасности;
 - 3) обоснование краткой спецификации ОО;
 - 4) обоснование утверждений о соответствии ПЗ.

В разделе «Введение ЗБ» идентифицируется ЗБ и ОО и приводится аннотация ЗБ в форме, наиболее подходящей для включения в перечень оцененных (сертифицированных) продуктов ИТ.

В раздел ЗБ «Описание ОО» включают сопроводительную информацию об ОО, предназначенную для пояснения его назначения и требований безопасности. Этот раздел должен включать в себя также описание конфигурации, в которой ОО подлежит оценке.

В раздел ЗБ «Среда безопасности ОО» включают описание аспектов среды безопасности ОО, которые должны учитываться объектом оценки, в частности, предположений безопасности, определяющих границы среды безопасности, угроз активам, требующим защиты (включая описание этих активов), политику безопасности организации, которой должен соответствовать ОО.

В раздел ЗБ «Цели безопасности» включают краткое изложение предполагаемой реакции на аспекты среды безопасности как с точки зрения целей безопасности, которые должны соответствовать ОО, так и с точки зрения целей безопасности, которые должны соответствовать ИТ- и не ИТ-мерам в пределах среды ОО.

В раздел ЗБ «Требования безопасности ИТ» включают функциональные требования безопасности ОО, требования доверия к безопасности, а также требования безопасности программного, программно-аппаратного и аппаратного обеспечения ИТ-среды ОО. Требования безопасности ИТ должны быть определены путем использования, где это возможно, функциональных компонентов и компонентов доверия к безопасности в соответствии с ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3.

В раздел «Краткая спецификация ОО» включают описание функций безопасности ИТ, реализуемых ОО и соответствующих специфицированным функциональным требованиям безопасности, а также любых мер доверия к безопасности, соответствующих специфицированным требованиям доверия к безопасности.

В разделе «Утверждения о соответствии ПЗ» идентифицируются ПЗ, о соответствии которым заявляется в ЗБ, а также любые дополнения или уточнения целей или требований из этих ПЗ.

В разделе ЗБ «Обоснование» демонстрируют, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, соответствующий ОО учитывает определенные аспекты среды безопасности ИТ и функции безопасности ИТ и меры доверия к безопасности соответствуют требованиям безопасности ОО.

Как и для ПЗ, при разработке ЗБ допускается отступать от вышеуказанной структуры путем включения дополнительных и исключения необязательных разделов (и/или подразделов).

При сопоставлении содержания ЗБ и ПЗ становится очевидной взаимосвязь между ними вследствие высокой степени общности данных документов. Если в ЗБ утверждается, что оно соответствует ПЗ, и при этом не специфицируются дополнительные функциональные требования и требования доверия к безопасности, то содержание сходных разделов может быть идентично содержанию соответствующих разделов ПЗ. В таких случаях рекомендуется

ссылка в ЗБ на содержание ПЗ с добавлением (там, где необходимо) деталей, отличающих ЗБ от ПЗ.

Стандарт приводит подробное описание содержания каждого из вышеуказанных разделов ПЗ и ЗБ.

В стандарте имеется также раздел, содержащий методические рекомендации по формированию пакетов требований безопасности. Концепция пакета требований представлена в ИСО/МЭК 15408. Оценочные уровни доверия к безопасности, определенные в ИСО/МЭК 15408-3, необходимо рассматривать как пример оформления пакетов требований доверия к безопасности.

В одном из приложений приведены примеры угроз, политики безопасности организации, предположений безопасности, целей безопасности в форме, рекомендуемой для ПЗ и ЗБ. Они могут быть адаптированы для использования в конкретных ПЗ и ЗБ.

Одно из приложений стандарта содержит руководство по разработке ПЗ и ЗБ в части криптографических аспектов ОО.

В ряде приложений стандарта проиллюстрировано его применение на рабочих примерах профилей защиты применительно к межсетевому экрану, системе управления базами данных (СУБД) и третьей доверенной стороне.

4.9. Национальные стандарты по биометрической аутентификации серии ГОСТ Р 52633

Комплекс национальных стандартов, устанавливающих требования к разработке и тестированию средств высоконадежной биометрической аутентификации, состоит из семи документов.

- ◆ ГОСТ Р 52633.0–2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации» (введен 01.04.2007 г.).
- ◆ ГОСТ Р 52633.1–2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации» (введен 01.01.2010 г.).
- ◆ ГОСТ Р 52633.2–2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации» (введен 01.10.2010 г.).

- ◆ ГОСТ Р 52633.3–2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора» (введен 01.12.2011 г.).
- ◆ ГОСТ Р 52633.4–2011 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия – код доступа» (введен 01.09.2012 г.).
- ◆ ГОСТ Р 52633.5–2011. «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия – код доступа» (введен 01.04.2012 г.).
- ◆ ГОСТ Р 52633.6–2012 «Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу “Свой”» (введен 01.12.2012 г.).

В стандартах используются следующие термины.

Биометрическая аутентификация – аутентификация пользователя, осуществляемая путем предъявления им своего биометрического образа.

Биометрические данные – данные с выходов первичных измерительных преобразователей физических величин, совокупность которых образует биометрический образ конкретного человека.

Биометрические параметры – параметры, полученные после предварительной обработки биометрических данных.

Биометрическая идентификация – преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие.

Биометрический образ – образ человека, полученный с выходов первичных измерительных преобразователей физических величин, подвергающийся далее масштабированию и иной первичной обработке с целью извлечения из него контролируемых биометрических параметров человека.

Биометрический образ «Свой» – биометрический образ легального пользователя.

Биометрический образ «Чужой» – биометрический образ злоумышленника, пытающегося преодолеть биометрическую защиту.

Вероятность ошибки первого рода – вероятность ошибочного отказа «своему» пользователю в биометрической аутентификации.

Вероятность ошибки второго рода – вероятность ошибочной аутентификации «чужого» как «своего» (ошибочная аутентификация).

Высоконадежная биометрическая аутентификация – биометрическая аутентификация с приемлемой вероятностью ошибок первого рода и гарантированно малой вероятностью ошибок второго рода, сопоставимой

по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора.

Средства биометрической аутентификации могут быть отнесены к высоконадежным, только если в их состав введены криптографические механизмы аутентификации, работающие совместно с биометрическими механизмами аутентификации через преобразование нечетких (неоднозначных) биометрических образов в однозначный криптографический ключ или длинный пароль.

Сейчас в СВБА используются следующие биометрические механизмы:

- ◆ анализ кровеносных сосудов глазного дна;
- ◆ анализ радужной оболочки глаза;
- ◆ двухмерный и трехмерный анализ геометрических особенностей лица в видимом и инфракрасном спектре света;
- ◆ анализ особенностей геометрии ушных раковин;
- ◆ анализ особенностей голоса;
- ◆ анализ особенностей папиллярных рисунков пальцев;
- ◆ анализ геометрии ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони;
- ◆ анализ рисунка кровеносных сосудов, складок кожи тыльной стороны ладони;
- ◆ анализ рукописного почерка;
- ◆ анализ клавиатурного почерка;
- ◆ анализ геометрического соотношения частей тела;
- ◆ анализ особенностей походки.

СВБА классифицируют по способам их технической реализации, уровню безопасности окружающей их среды, типам носителей информации, используемых для хранения аутентификационной информации, их ориентации на различные типы политик управления информационной безопасностью, стойкости использованных в них криптографических механизмов к атакам подбора.

Особенности каждого из классов средств биометрической аутентификации должны быть отражены в профиле защиты по ГОСТ Р ИСО/МЭК 15408.

Структурная схема обработки информации в средствах высоконадежной биометрической аутентификации изображена на рис. 4.10 в формате, представленном в стандарте.

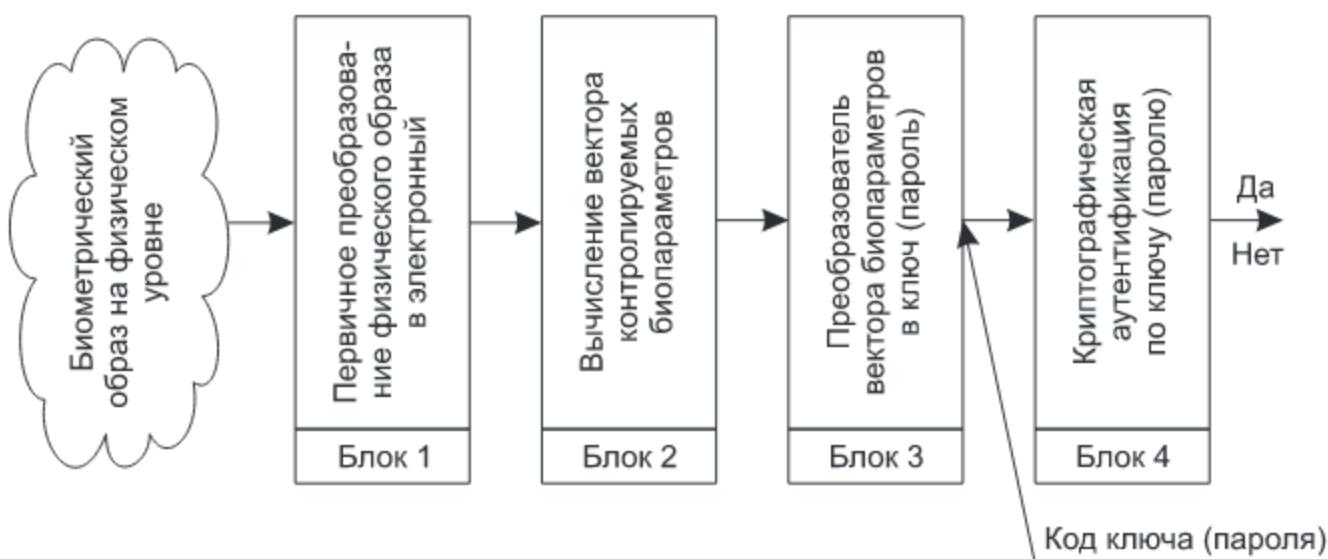


Рис. 4.10. Структурная схема обработки информации в СВБА

Стандартом установлены основные показатели и характеристики для средств высоконадежной биометрической аутентификации, перечень угроз и способов обеспечения информационной безопасности при применении СВБА, правила их приемки (поставки), а также требования к тестированию (испытаниям).

4.10. Краткий обзор некоторых стандартов

В данном разделе приведены короткие аннотации нескольких национальных стандартов в области защиты информации.

Национальный стандарт ГОСТ Р 52447–2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества» введен в действие 01.01.2007 г. Он распространяется на основные средства защиты информации и средства контроля эффективности защиты информации, входящие в состав техники защиты информации. Стандарт устанавливает номенклатуру основных показателей качества средств защиты информации от утечки по техническим каналам и несанкционированного доступа, а также средств контроля эффективности защиты информации.

Состав и структура характеризуемых свойств средств, входящих в состав техники ЗИ, отражает номенклатуру показателей и включает следующие признаки классификации: свойства средств, способ выражения показателей, количество характеризуемых свойств средств, способ оценки показателей и стадии их определения.

Для классификации техники ЗИ используют следующие признаки:

- ◆ функциональное назначение ЗИ (контроль эффективности ЗИ);

- ◆ вид предотвращаемых угроз (НСД, НСВ, утечка информации по техническим каналам);
- ◆ решаемые задачи;
- ◆ функциональная сложность (средство, комплекс, система);
- ◆ метод защиты (пассивные, активные);
- ◆ место установки (наземные, воздушные, морские и космические);
- ◆ сфера применения (специального назначения, общего применения);
- ◆ конструктивное исполнение (встроенные в объект защиты, выполненные в виде отдельного образца изделия);
- ◆ вид исполнения (технические, программные, программино-технические средства).

В стандарте приведена номенклатура показателей средств защиты информации и средств контроля эффективности защиты информации от утечки по техническим каналам (радиоконтроля, контроля лазерных излучений, телевизионного контроля, программных средств защиты и др.).

Национальный стандарт ГОСТ Р 53115–2008 «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства» введен в действие 01.10.2009 г. Стандарт распространяется на технические средства обработки информации и устанавливает методы их испытаний на соответствие требованиям защищенности от несанкционированного доступа, а также методы измерения побочных электромагнитных излучений и наводок.

Национальный стандарт ГОСТ Р 53131–2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения» введен в действие 01.10.2009 г. Он является модифицированным по отношению к международному стандарту ISO/IEC TR 24762:2008 «Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services».

В стандарте представлены рекомендации по планированию деятельности, связанной с восстановлением функций и механизмов безопасности информационных и телекоммуникационных технологий после чрезвычайных ситуаций в контексте общего процесса обеспечения непрерывности деятельности организации. Он предназначен для персонала (служб безопасности) организаций, а также для внутренних и внешних провайдеров

(поставщиков) услуг, участвующих в обеспечении информационной безопасности организации.

Под чрезвычайной ситуацией в организации понимается внезапное, незапланированное катастрофическое событие, которое не позволяет организации выполнять критичные бизнес-процессы в требуемом для бизнеса объеме.

Национальный стандарт **ГОСТ Р ИСО/МЭК 27034-1-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия»** введен в действие 01.06.2015 г. Он идентичен международному стандарту ISO/IEC 27034-1:2011 «Information technology – Security techniques – Application security – Part 1: Overview and concepts».

Организациям необходимо обеспечивать защиту приложений от уязвимостей, которые могут быть свойственны самому приложению (например, дефекты программных средств), могут появляться в течение жизненного цикла приложений (например, в результате изменений приложения) или возникать в результате использования приложений в не предназначенных для них условиях.

Приложения могут быть получены путем внутренней разработки, аутсорсинга или покупки готового стандартного продукта. Примерами приложений являются кадровые системы, финансовые системы, системы обработки текстов, системы менеджмента взаимодействия с клиентами, межсетевые экраны, антивирусные системы и системы обнаружения вторжений.

Целью стандарта ИСО/МЭК 27034 является содействие организациям в планомерной интеграции безопасности на протяжении жизненного цикла приложений. Он содержит общий обзор безопасности приложений, а также определения, понятия, принципы и процессы, касающиеся обеспечения безопасности приложений.

Стандарт полезен для следующих групп лиц: руководителей, лиц, отвечающих за приобретение и эксплуатацию, поставщиков, аудиторов, пользователей.

Международная версия стандарта ISO/IEC 27034 состоит из шести частей:

1. Обзор и общие понятия.
2. Нормативная структура организации.
3. Процесс менеджмента безопасности приложений.
4. Валидация безопасности приложений.
5. Структура данных управления безопасностью протоколов и приложений.
6. Руководство по безопасности для конкретных приложений.

Валидация согласно стандарту означает «подтверждение посредством представления объективных свидетельств того, что требования, предназначенные для конкретного использования или применения, выполнены».

Обеспечение безопасности приложений — это процесс применения мер и средств контроля и управления и измерений к приложениям организации с целью осуществления менеджмента риска, возникающего в результате их использования. Меры и средства контроля и управления и измерения могут применяться к самому приложению (его процессам, компонентам, программным средствам и результатам), его данным (конфигурационным данным, данным пользователей, данным организации) и ко всей технологии, процессам и действующим субъектам, вовлеченным в жизненный цикл приложения.

Безопасность приложений обеспечивает защиту критических данных, вычисляемых, используемых, хранимых и передаваемых приложением. Эта защита обеспечивает уверенность не только в доступности, целостности и конфиденциальности данных, но и в неотказуемости и аутентификации пользователей, имеющих к ним доступ.

Согласно ИСО/МЭК 27005 требования безопасности приложений идентифицируются посредством оценки риска и обработки риска и диктуются такими факторами, как спецификации приложений, целевая среда приложений, критические данные.

Национальный стандарт ГОСТ Р 56824–2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» принят Росстандартом России 03.12.2015 г. с вводом в действие 01.06.2016 г. В целом стандарт разработан на основе положений и принципов Гражданского кодекса Российской Федерации (часть 4) об охране результатов интеллектуальной деятельности и федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в части вопросов, касающихся функционирования сети Интернет.

Стандарт устанавливает единый понятийный аппарат и выделяет специфические риски, относящиеся к использованию интеллектуальной собственности в сети Интернет.

Все объекты интеллектуальной собственности, по поводу которых возникают отношения по их использованию в сети Интернет, в стандарте подразделяются на два типа:

- ◆ охраняемые результаты интеллектуальной деятельности и средства индивидуализации, созданные в сети Интернет;
- ◆ охраняемые результаты интеллектуальной деятельности и средства индивидуализации, используемые в сети Интернет.

К первому типу относятся РИД, которые невозможно использовать вне сети Интернет: сайт, интернет-вещание и мультимедийные продукты.

Ко второму типу относятся РИД, которые являются охраняемыми по закону независимо от сети Интернет: произведения литературы, науки, искусства, программы для ЭВМ, аудиовизуальные произведения, мультимедийные продукты и др.

В стандарте выделяются следующие основные субъекты отношений в регулируемой предметной области:

- ◆ авторы (физическими лица, творческим трудом которых создан охраняемый РИД);
- ◆ интернет- правообладатели (правообладатели объектов интеллектуальной собственности и информационных ресурсов, размещенных в сети Интернет);
- ◆ интернет-пользователи (лица, имеющие доступ к сети Интернет);
- ◆ информационные посредники (лица, оказывающие услуги по предоставлению доступа к сети Интернет и услуги, связанные с размещением информации в Сети, в том числе организаторы распространения информации в сети Интернет, как они определены в законе № 149-ФЗ).

Интернет-пользователь, использующий Сеть с нарушением законодательства, определяется как интернет-нарушитель.

В стандарте описаны общие правила, способы и процедуры использования и распространения охраняемых РИД и средств индивидуализации в сети Интернет, а также защиты прав на объекты интеллектуальной собственности.

Описаны также меры ответственности субъектов отношений в случае нарушения национального законодательства в рассматриваемой предметной области.

Иск по делу о защите прав на объекты интеллектуальной собственности, размещенные в сети Интернет, по выбору истца может быть подан по месту нахождения:

- ◆ доменного имени, под которым создан сайт, содержащий РИД;
- ◆ организации – администратора сайта;
- ◆ владельца сайта;
- ◆ информационных посредников владельца сайта;
- ◆ обладателя информационного ресурса, содержащего РИД;
- ◆ интернет-пользователя, нарушившего интеллектуальные права на объекты интеллектуальной собственности.

Контрольные вопросы и задания к главе 4

1. Какие версии международного стандарта «Общие критерии» действуют в Российской Федерации?
2. Какие названия имеют три части стандарта ИСО/МЭК 15408?
3. Дайте определение понятиям «профиль защиты» и «задание по безопасности».
4. Какова структура ФТБ?
5. Какова структура требований доверия?
6. Что такое оценочный уровень доверия?
7. Что такое составной пакет доверия?
8. Какова структура технического отчета об оценке?
9. Каковы требования к системе защиты информации для АСЗИ?
10. Что такое преднамеренное электромагнитное воздействие?
11. Какие национальные стандарты посвящены защите АС от преднамеренных электромагнитных воздействий?
12. Каковы этапы обеспечения безопасности АС?
13. Каковы этапы оценки безопасности АС?
14. В чем заключаются основные причины усложнения оценки АС по сравнению с оценкой ИТ-продуктов?
15. Для каких целей введены дополнительные компоненты требований безопасности для оценки АС (по сравнению с требованиями в ИСО/МЭК 15408)?
16. Какова структура описания ПЗ?
17. Какова структура описания ЗБ?
18. Что такое высоконадежная биометрическая аутентификация?
19. Какие механизмы используются для биометрической аутентификации?

Список литературы

1. Основы информационной безопасности: Учеб. пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М.: Горячая линия — Телеком, 2006. — 544 с.: ил.
2. Барабанов А. В., Марков А. С., Цирлов В. Л. Учебный пример Задания по безопасности: Методическое пособие / УЦ «Эшелон». — М., 2012. — 56 с.
3. Галатенко В. А. Стандарты информационной безопасности: Курс лекций. 2-е изд. / ИНТУИТ.РУ «Интернет-университет информационных технологий». — М., 2006. — 264 с.
4. Правовое обеспечение информационной безопасности: Учеб. пособие для студентов высших учебных заведений. 3-е изд., стер. / С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.; Под ред. С. Я. Казанцева. — М.: Изд. центр «Академия», 2008. — 240 с.
5. Обеспечение информационной безопасности бизнеса / Под ред. А. П. Курило. — М.: Альпина Паблишерз, 2011.
6. Основы управления информационной безопасностью: Учеб. пособие для вузов. 2-е изд., испр. / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — М.: Горячая линия — Телеком, 2016. — 244 с.: ил. (Сер. «Вопросы управления информационной безопасностью». Вып. 1.)
7. Котухов М. М. Основные положения и нормативно-правовое обеспечение информационной безопасности автоматизированных систем: Учеб. пособие / ИПКИР. — М., 2006. — 67 с.
8. Котухов М. М. Лицензирование и сертификация в области защиты информации: Учеб. пособие / ИПКИР. — М., 2006. — 40 с.
9. Коробейников А. Г., Троников И. Б., Жаринов И. О. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: Монография / Под ред. П. П. Парамонова. — СПб.: Студия «НП-Принт», 2012. — 115 с.: ил.
10. Малюк А. А. Информационная безопасность: концептуальные и методические основы защиты информации: Учеб. пособие для вузов. — М.: Горячая линия — Телеком, 2004. — 280 с.: ил.

11. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах: Учеб. пособие для вузов. 2-е изд. — М.: Горячая линия — Телеком, 2004. — 147 с.: ил.
12. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / Под ред. А. С. Маркова. — М.: Радио и связь, 2012. — 192 с.
13. Моисеев А. И., Жмуров Д. Б. Информационная безопасность распределенных информационных систем: Учебник. — Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2013. — 180 с.
14. Наумов В. Б. Право и Интернет: Очерки теории и практики. — М.: Книжный дом «Университет», 2002. — 432 с.: ил.
15. Родичев Ю. А. Компьютерные сети: архитектура, технологии, защита. — Самара: Универс-групп, 2005. — 468 с.
16. Родичев Ю. А., Бусарова Е. Ю. Информационная система нормативно-правового обеспечения защиты информации: Электронное учеб.-метод. пособие / Самар. гос. ун-т. — Самара, 2008.
17. Родичев Ю. А. Правовая модель отношений субъектов информационного обмена // Вест. Самар. гос. ун-та. Гуманит. сер. — 2007. — № 5 (55). — С. 115–122.
18. Родичев Ю. А. Правовые аспекты информационного обмена в сети Интернет // Вест. Самар. гос. ун-та. Сер. Физ.-мат. науки. — 2007. — № 2(15). — С. 200–204.
19. Родичев Ю. А. Компьютерные сети. Нормативно-правовые аспекты информационной безопасности: Учеб. пособие для вузов. Ч. 1. — Самара: Универс-групп, 2007. — 344 с.
20. Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Учеб. пособие. — СПб.: Питер, 2008. — 272 с.
21. Родичев Ю. А. Правовая защита персональных данных: Учеб. пособие для вузов. — Самара: Вест. Самар. гос. ун-та, 2010. — 448 с.
22. Родичев Ю. А., Бусарова Е. Ю. Информационно-справочная система «Правовая защита персональных данных»: Электрон. учеб.-метод. пособие / Вест. Самар. гос. ун-та. — Самара, 2009.
23. Родичев Ю. А., Родичев А. Ю. Системная модель защиты информации информационных систем распределенного типа // Вест. Самар. гос. ун-та. — 2003. — № 2. — С. 15–20.
24. Родичев Ю. А. Правовая модель отношений субъектов информационного обмена // Вест. Самар. гос. ун-та. Гуманит. сер. — 2007. — № 5/1. — С. 115–122.

25. Родичев Ю. А. Правовые аспекты информационного обмена в сети Интернет // Вест. Самар. гос. ун-та. Сер. Физ.-мат. науки. – 2007. – № 2 (15). – С. 200–204.
26. Родичев Ю. А. Правовые аспекты информатизации в современном законодательстве: Матер. межвуз. науч.-метод. конф. – Самара: Вест. Самар. гос. ун-та, 2008. – С. 15–21.
27. Родичев Ю. А. Нормативно-правовые и организационные аспекты защиты персональных данных: Матер. регион. конф. «Безопасность общества и бизнеса: актуальные проблемы». – Тольятти, 2010. – С. 165–172.
28. Родичев Ю. А. Электронный учебно-методический комплекс «Экономико-правовые аспекты рынка программного обеспечения» // Хроники объединенного фонда электронных ресурсов «Наука и образование». – 2015. – № 3 (70). – С. 8; http://Ofernio.ru/rto_files_ofernio/20825.doc.
29. Родичев Ю. А. Электронный учебно-методический комплекс «Нормативная база, российские и международные стандарты по информационной безопасности» // Хроники объединенного фонда электронных ресурсов «Наука и образование». – 2015. – № 3 (70). – С. 9; http://Ofernio.ru/rto_files_ofernio/20828.doc.
30. Романов О. А., Бабин С. А., Жданов С. Г. Организационное обеспечение информационной безопасности: Учебник для студ. высш. учеб. заведений. – М.: Изд. центр «Академия», 2008. – 192 с.
31. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.
32. Организационно-правовое обеспечение информационной безопасности: Учеб. пособие для студ. высш. учеб. заведений /А. А. Стрельцов и др. / Под ред. А. А. Стрельцова. – М.: Изд. центр «Академия», 2008. – 256 с.
33. Титоренко Г. А. Методы и средства построения систем информационной безопасности. Их структура. 2-е изд., доп. – М.: ЮНИТИ-ДАНА, 2003. – 205 с.
34. Тихонов В. А., Райх В. В. Информационная безопасность: концептуальные, организационные и технические аспекты: Учеб. пособие. – М.: Гелиос АРВ, 2006. – 528 с.: ил.
35. Шамраев А. В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. – М.: Статут; Интертех; БЦД-пресс, 2003. – 1013 с.
36. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 г. (утв. распоряжением Правительства Российской Федерации от 01.11.2013 г. № 2036-р). «Собрание законодательства РФ», 18.11.2013, № 46, ст. 5954.

37. Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». «Собрание законодательства РФ», 30.12.2002, № 52 (ч.1), ст. 5140.
38. Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.
39. Федеральный закон Российской Федерации от 07.07.2003 г. № 126-ФЗ «О связи». «Собрание законодательства РФ», 14.07.2003, № 28, ст. 2895.
40. Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных». «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3451.
41. Стратегия национальной безопасности Российской Федерации до 2020 г. (утв. Указом Президента Российской Федерации от 12.05.2009 г. № 537).
42. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 31.12.2015 г. № 683).
43. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Указом Президента Российской Федерации от 03.02.2012 г. № 803).
44. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. (утв. Президентом Российской Федерации от 24.07.2013 г. № Пр-1753).
45. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г.
46. Концепция развития национальной системы стандартизации РФ на период до 2020 г. (одобрена распоряжением Правительства РФ от 24.09.2012 г. № 1762-р).
47. О федеральном информационном фонде технических регламентов и стандартов и единой информационной системе по техническому регулированию (утв. Постановлением Правительства Российской Федерации от 15.08.2003 г. № 500).
48. О порядке разработки и утверждения сводов правил (утв. Постановлением Правительства Российской Федерации от 19.11.2008 г. № 858).
49. Постановление Госстандарта РФ от 30.01.2004 г. № 4 «О национальных стандартах Российской Федерации».

50. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
51. Постановление Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом “О персональных данных” и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
52. Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
53. Конвенция об обеспечении международной информационной безопасности (концепция). <http://www.scrf.gov.ru/documents/6/112.html>.
54. Правила поведения в области обеспечения международной информационной безопасности. <http://www.mid.ru>.

Список документов ФСТЭК

1. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утв. решением председателя Гостехкомиссии России от 30.03.1992 г.).
2. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. (Гостехкомиссия России, 1992 г.)
3. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утв. решением председателя Гостехкомиссии от 30.03.1992 г.).
4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. решением председателя Гостехкомиссии России от 30.03.1992 г.).
5. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утв. решением председателя Гостехкомиссии России от 30.03.1992 г.).
6. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. приказом председателя Гостехкомиссии России от 25.11.1994 г.).
7. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. приказом председателя Гостехкомиссии России от 27.10.1995 г. № 199).
8. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утв. решением председателя Гостехкомиссии России от 25.07.1997 г.).

9. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утв. решением председателя Гостехкомиссии России от 25.07.1997 г.).
10. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. решением председателя Гостехкомиссии России от 04.06.1999 г. № 114).
11. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. (Гостехкомиссия России, 2003 г.)
12. Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. (Гостехкомиссия России, 2003 г.)
13. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. (Гостехкомиссия России, 2003 г.)
14. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. (Гостехкомиссия России, 2003 г.)
15. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (введен в действие приказом Гостехкомиссии России от 19.06.2002 г. № 187).
16. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. 2002 г.
17. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. 2002 г.
18. Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (зарегистрировано в Минюсте России 30.06.2014 г. № 32919).
19. Требования к системам обнаружения вторжений (утв. приказом ФСТЭК России от 06.12.2011 г. № 638).

20. Требования к средствам антивирусной защиты (утв. приказом ФСТЭК России от 20.03.2012 г. № 28).
21. Требования к средствам контроля съемных машинных носителей (утв. приказом ФСТЭК России от 28.07.2014 г. № 87).
22. Требования к средствам доверенной загрузки (утв. приказом ФСТЭК России от 27.09.2013 г. № 119).
23. Профиль защиты средств антивирусной защиты. Пакет методических документов (утв. ФСТЭК России от 04.06.2012 г.).
24. Профиль защиты систем обнаружения вторжений. Пакет методических документов (утв. ФСТЭК России от 03.02.2012 г. и от 06.03.2012 г.).
25. Профиль защиты средств контроля подключения съемных машинных носителей информации. Пакет методических документов (утв. ФСТЭК России от 01.12.2014 г.).
26. Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации. Пакет методических документов (утв. ФСТЭК России от 01.12.2014 г.).
27. Профиль защиты средства доверенной загрузки. Пакет методических документов (утв. ФСТЭК России от 30.12.2013 г.).
28. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
29. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом ФСТЭК от 18.02.2013 г. № 21).
30. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014 г.).
31. Приказ ФСБ и ФСТЭК № 416/489 от 31.08.2010 г. «О защите информации, содержащейся в информационных системах общего пользования».
32. Методический документ ФСТЭК «Базовая модель угроз безопасности ПД при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 15.02.2008 г.).
33. Методический документ ФСТЭК «Методика определения актуальных угроз безопасности ПД при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14.02.2008 г.).
34. Проект методического документа ФСТЭК «Методика определения угроз безопасности информации в информационных системах». 2015 г.

Список национальных стандартов

1. ГОСТ Р ИСО/МЭК 15408-1–2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
2. ГОСТ Р ИСО/МЭК 15408-2–2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».
3. ГОСТ Р ИСО/МЭК 15408-3–2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».
4. ГОСТ Р ИСО /МЭК 27033-1–2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
5. ГОСТ Р ИСО /МЭК 27033-3–2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления».
6. ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
7. ГОСТ Р ИСО/МЭК 27001–2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности». Требования».
8. ГОСТ Р ИСО/МЭК 27002–2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
9. ГОСТ Р ИСО/МЭК 27003–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента

- информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
10. ГОСТ Р ИСО/МЭК 27004–2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
 11. ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
 12. ГОСТ Р ИСО/МЭК 27006–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
 13. ГОСТ Р ИСО/МЭК 27007–2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности».
 14. ГОСТ Р ИСО/МЭК 27011–2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».
 15. Р 50.1.053–2005 «Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации».
 16. Р 50.1.056–2005 «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения».
 17. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».
 18. ГОСТ Р 53114–2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».
 19. ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
 20. ГОСТ Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
 21. ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
 22. ГОСТ Р 56093–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования».

23. ГОСТ Р 56103–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения».
24. ГОСТ Р 56115–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования».
25. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».
26. ГОСТ Р 52069.0–2013 «Защита информации. Система стандартов. Основные положения».
27. ГОСТ Р 56045–2014 «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью».
28. ГОСТ Р ИСО/МЭК 13335-1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
29. ГОСТ Р ИСО/МЭК ТО 13335-5–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».
30. ГОСТ Р ИСО/МЭК 18045–2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
31. ГОСТ Р ИСО/МЭК ТО 19791–2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
32. ГОСТ ИСО/МЭК 17000–2012 «Оценка соответствия. Словарь и общие принципы».
33. ГОСТ Р ИСО/МЭК ТО 15446–2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».
34. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
35. ГОСТ Р ИСО/МЭК 27034-1–2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия».

36. ГОСТ Р 52447–2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества».
37. ГОСТ Р 52448–2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения».
38. ГОСТ Р 53110–2008 «Система обеспечения информационной безопасности. Сети связи общего пользования. Общие положения».
39. ГОСТ Р 52633.0–2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
40. ГОСТ Р 52633.1–2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».
41. ГОСТ Р 52633.2–2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».
42. ГОСТ Р 52633.3–2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
43. ГОСТ Р 52633.4–2011 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия – код доступа».
44. ГОСТ Р 52633.5–2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия – код доступа».
45. ГОСТ Р 52633.6–2012 «Защита информации. Техника защиты информации требования к индикации близости предъявленных биометрических данных образу “Свой”».
46. ГОСТ Р 53113.1–2008. «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».
47. ГОСТ Р 53113.2–2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».

48. ГОСТ Р 53115–2008 «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства».
49. ГОСТ Р 53131–2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».
50. ГОСТ Р 1.0–2012 «Стандартизация в Российской Федерации. Основные положения».
51. ГОСТ Р 1.2–2014 «Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления и отмены».
52. ГОСТ Р 1.12–2004 «Стандартизация в Российской Федерации. Термины и определения».
53. ГОСТ Р 1.4–2004 «Стандарты организаций. Общие положения».
54. ГОСТ Р 1.5–2012 «Стандарты национальные. Правила построения, изложения, оформления и обозначения».
55. ГОСТ 1.1–2002 «Межгосударственная система стандартизации. Термины и определения».
56. ГОСТ Р 56545–2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».
57. ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».
58. ГОСТ Р 56824–2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет».

Список стандартов Банка России

1. Стандарт Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
2. Стандарт Банка России СТО БР ИББС-1.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности».
3. Стандарт Банка России СТО БР ИББС-1.2–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014».
4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.0–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».
5. Рекомендации в области стандартизации Банка России РС БР ИББС-2.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».
6. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2–2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».
7. Рекомендации в области стандартизации Банка России РС БР ИББС-2.5–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности».

8. Рекомендации в области стандартизации Банка России РС БР ИББС-2.6–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».
9. Рекомендации в области стандартизации Банка России РС БР ИББС-2.7–2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности».
10. Рекомендации в области стандартизации Банка России РС БР ИББС-2.8–2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации».

Ю. А. Родичев

**Нормативная база и стандарты
в области информационной безопасности.
Учебное пособие**

Серия «Учебник для вузов»

Заведующая редакцией
Ведущий редактор
Литературный редактор
Художественный редактор
Корректоры
Верстка

*Ю. Сергиенко
Н. Риманчан
Н. Рошина
С. Заматтеская
С. Беляева, В. Сайко
Л. Соловьева*

Изготовлено в России. Издатель: ООО «Прогресс книга».
Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург,
Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 11.2020. Наименование: книжная продукция. Срок годности: не ограничен.
Импортер в Беларусь: ООО «ПИТЕР М», РБ, 220020, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс 208 80 01.
Налоговая льгота — общероссийский классификатор продукции ОК 034-2014,
58.11.11 — Учебники печатные общеобразовательного назначения.
Подписано в печать 13.111.20. Формат 70x100/16. Бумага писчая. Усл. п. л. 20,640. Доп. тираж. Заказ 0000.

Ю. А. Родичев

**Нормативная база и стандарты
в области информационной безопасности.
Учебное пособие**

Серия «Учебник для вузов»

Заведующая редакцией
Ведущий редактор
Литературный редактор
Художественный редактор
Корректоры
Верстка

*Ю. Сергиенко
Н. Риманчан
Н. Рошина
С. Заматтеская
С. Беляева, В. Сайко
Л. Соловьева*

Изготовлено в России. Издатель: ООО «Прогресс книга».
Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург,
Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 11.2020. Наименование: книжная продукция. Срок годности: не ограничен.
Импортер в Беларусь: ООО «ПИТЕР М», РБ, 220020, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс 208 80 01.
Налоговая льгота — общероссийский классификатор продукции ОК 034-2014,
58.11.11 — Учебники печатные общеобразовательного назначения.
Подписано в печать 13.111.20. Формат 70x100/16. Бумага писчая. Усл. п. л. 20,640. Доп. тираж. Заказ 0000.