Федеральное агентство по образованию
Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева

В. В. ЗОЛОТАРЕВ
Н.А. ФЕДОРОВА

АНАЛИЗ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рекомендовано в качестве учебного пособия
для студентов, обучающихся по специальностям
«Комплексное обеспечение информационной безопасности автоматизированных систем»
«Информационная безопасность телекоммуникационных систем»

Красноярск 2007

УДК 004.056
ББК 32.973.26-018.2
З 80

РЕЦЕНЗЕНТЫ:
канд. техн. наук, доцент каф. БИТ М. Н. Жукова
канд. техн. наук, доцент, проректор по информатизации Омского государственного технического университета М. Ю. Пляскин

Золотарев, В. В. , Федорова, Н.А.
З 80 Анализ защищенности автоматизированных систем: Учебное пособие / В. В. Золотарев, Н. А. Федорова; СибГАУ. – Красноярск, 2007. – 93 с.

Цель учебного пособия – ознакомить студентов с основными особенностями анализа защищенности автоматизированных систем, указать направления обучения и профессиональной деятельности. Издание содержит основы оценки защищенности по принятым в качестве российских международным стандартам ГОСТ Р ИСО/МЭК 15408-2002 и ГОСТ Р ИСО/МЭК 17799-2005. Кроме того, предлагается сравнительный анализ процедур оценки защищенности и сопоставление требований. Приведены справочные данные. Пособие содержит контрольные вопросы для самопроверки и примерные вопросы контрольного тестирования по указанному курсу.

Учебное пособие предназначено для студентов, обучающихся по специальностям 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 «Информационная безопасность телекоммуникационных систем» всех форм обучения.

УДК 004.056
ББК 32.973.26-018.2

Учебное издание

ЗОЛОТАРЕВ Вячеслав Владимирович
ФЁДОРОВА Наталия Александровна
АНАЛИЗ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Учебное пособие

Редактор
Компьютерная верстка

Подп. в печать _____. Формат 60×84/16. Бумага офисная.
Печать плоская. Усл. печ. л. 7,0. Уч.-изд. л. 7,3.
Тираж 50 экз. Заказ 410. С 70.

Санитарно-эпидемиологическое заключение
№ 24.04.953. П.000032.01.03. от 29.01.2003 г.
Редакционно-издательский отдел СибГАУ.
660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31.
Отпечатано в типографии «Город».
660014, г. Красноярск, ул. Юности, 24а.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Российское законодательство в области информационной безопасности (ИБ) на данный момент проходит некоторую промежуточную стадию своего формирования и является еще недостаточно зрелым.

Федеральные ведомства, регулирующие сферу ИБ (к их числу относятся, прежде всего, Федеральная служба безопасности, Федеральная служба по техническому и экспортному контролю и министерство обороны), в соответствии со стоящими перед ними задачами, до недавних пор были сосредоточены исключительно на вопросах обеспечения государственной безопасности. Применительно к ИБ речь шла главным образом о защите государственной тайны. Основным инструментом регулирования здесь традиционно являются лицензирование и сертификация.

Когда же речь идет о защите конфиденциальной информации, а также критичных информационных ресурсов, принадлежащих не государству, а частным лицам, то собственник информации обычно сам определяет требуемую степень ее защиты. Такой подход, с некоторыми оговорками, и применяется во многих странах.

Наше государство обратило внимание на вопросы, не связанные с защитой государственной тайны, относительно недавно. Первый в России руководящий документ Гостехкомиссии России, устанавливающий требования по защите конфиденциальной информации, СТР-К (Специальные требования и рекомендации по защите конфиденциальной информации) увидел свет в 1999 году. В качестве основных мер по защите информации он определяет сертификацию и аттестацию.

Для коммерческих организаций, в отличие от государственных, требования СТР-К носят рекомендательный характер, однако, это послабление компенсируется вышедшим в 2006 году Постановлением Правительства РФ № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»". Согласно этому документу лицензированию подлежат все виды хозяйствующих субъектов и все виды деятельности по защите конфиденциальной информации, а в качестве обязательных лицензионных условий - использование сертифицированных СЗИ и аттестованных АС [1].

Таким образом, всё чаще коммерческие организации выступают инициатором проведения процедуры аттестации объектов информатизации. На сложившуюся ситуацию, в первую очередь, оказало значительное влияние принятие в России международных стандартов оценки безопасности информационных технологий - ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», а также ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

Аттестация, проведенная согласно вышеупомянутому международному стандарту, для конкретной организации будет иметь немалые выгоды. Это и повышение инвестиционной привлекательности для компании, прошедшей аттестацию, и снижение тарифов страхования (страховые компании оценивают риски клиентов, автоматизированные системы которых прошли аттестацию, ниже, чем остальных).

Активное развитие информационных технологий, расширяющаяся сфера их применения в деятельности организации всех форм собственности, расширение со-

става угроз информационной безопасности, изменения в законодательной базе требуют постоянного развития нормативных и методических основ безопасности информационных систем.

В пособии рассмотрен подход к проблеме анализа защищенности автоматизированных систем, не содержащих информацию, составляющую государственную тайну Российской Федерации. При описании рассмотренных положений используются элементы отечественной нормативной базы анализа защищенности.

Данное учебное пособие предназначено для оказания помощи студентам в изучении курса «Аттестация автоматизированных систем», подготовке к лабораторным работам, занятиям и итоговому контролю.

Задачей курса «Аттестация автоматизированных систем» является подготовка студентов к проведению анализа защищенности автоматизированных информационных систем. Знания и практические навыки, полученные из курса, могут использоваться студентами при подготовке к занятиям по предметам специализации, а также в профессиональной деятельности.

В пособии описываются и сравниваются процедуры анализа защищенности автоматизированных систем по трем группам нормативных документов: ГОСТ Р ИСО/МЭК 15408-2002, ГОСТ Р ИСО/МЭК 17799-2005, РД ГТК России. В работе не рассматриваются конкретные средства анализа защищенности и некоторые вопросы предметной области, составляющие государственную тайну Российской Федерации.

Учебное пособие подготовлено в соответствии с рабочей программой курса, для каждой темы курсивом выделены основные положения, которые рекомендуется изучить. В конце каждого параграфа пособия даны задания для самостоятельной работы. В конце учебного пособия приведен словарь основных понятий и терминов, применяемых в предметной области, перечень сокращений, список литературы для дополнительного изучения. Пособие не является курсом лекций, поэтому более полную информацию можно получить, используя рекомендованную литературу и лекционный материал. Кроме того, издание не содержит сведений, относящихся к закрытым методикам оценки защищенности автоматизированных систем по РД ГТК России.

Учебное пособие соответствует Государственному образовательному стандарту подготовки специалистов по специальности 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» всех форм обучения.

Благодарности

За участие в подготовке издания и подборе материала авторы благодарят Ширкову Елену Андреевну и Ткаченко Константина Петровича.

1. АНАЛИЗ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

1.1 Общие сведения

Понятие защищенности. Методика анализа защищенности. Исходные данные по обследуемой автоматизированной системе. Объекты анализа защищенности. Методы тестирования системы защиты.

Понятие защищенности

Под защищенностью АС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.

Существует большое количество не поддающихся точной оценке возможных путей осуществления угроз безопасности в отношении ресурсов АС. «В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является первым фактором, определяющим защищенность АС. Вторым фактором является прочность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода, либо преодоления. Третьим фактором является величина ущерба, наносимого владельцу АС в случае успешного осуществления угроз безопасности» [2, с. 7].

Кроме того, для понимания изложенных ниже сведений необходимы следующие определения [5]:

Эффективность защиты информации - степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации - мера или характеристика для оценки эффективности защиты информации.

Нормы эффективности защиты информации - значения показателей эффективности защиты информации, установленные нормативными документами.

Мероприятие по контролю эффективности защиты информации - совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.

Категорирование защищаемой информации [объекта защиты] - установление градаций важности защиты защищаемой информации [объекта защиты].

Метод [способ] контроля эффективности защиты информации - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

Контроль состояния защиты информации - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

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

Контроль организации защиты информации - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Организационный контроль эффективности защиты информации - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности защиты информации - контроль эффективности защиты информации, проводимой с использованием средств контроля.

Методика анализа защищенности

В настоящее время не существует открытых стандартизированных методик анализа защищенности АС. Поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности автоматизированной системы предложить все-таки возможно. Эффективность данной методики многократно проверена на практике.

Типовая методика включает использование следующих методов:

- изучение исходных данных по АС;
- оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;
- анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
- ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;
- сканирование внешних сетевых адресов ЛВС из сети Интернет;
- сканирование ресурсов ЛВС изнутри;
- анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных агентов. [3]

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную, либо с использованием специализированных программных средств. [4]

Исходные данные по обследуемой автоматизированной системе

В соответствии с требованиями Положения по аттестации объектов информатизации по требованиям безопасности информации Гостехкомиссии (см. Приложение 1), включающих в себя предварительное обследование и анализ защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

- полное и точное наименование объекта информатизации и его назначение;
- характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия);
- организационная структура объекта информатизации;
- перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует);
- особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны;
- структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией;
- общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации;
- наличие и характер взаимодействия с другими объектами информатизации;
- состав и структура системы защиты информации на аттестуемом объекте информатизации;
- перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию;
- сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ;
- наличие на объекте информатизации службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных);
- наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители);
- наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Перечисленных исходных данных явно недостаточно для выполнения работ по анализу защищенности АС, и приведенный в Положении список нуждается в расширении и конкретизации. Последний пункт приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти «другие» данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС. Их список включает следующие виды документов:

Дополнительная документация.

- нормативно-распорядительная документация по проведению регламентных работ;
- нормативно-распорядительная документация по обеспечению политики безопасности;
- должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности;
- процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам;
- топология корпоративной сети с указанием IP-адресов и структурная схема;
- данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса;
- размещение информационных ресурсов в корпоративной сети;
- схема организационной структуры пользователей;
- схема организационной структуры обслуживающих подразделений;
- схемы размещения линий передачи данных;
- схемы и характеристики систем электропитания и заземления объектов АС;
- данные по используемым системам сетевого управления и мониторинга.

Проектная документация.

- функциональные схемы;
- описание автоматизированных функций;
- описание основных технических решений.

Эксплуатационная документация:

- руководства для пользователей и администраторов используемых программных и технических средств защиты информации (в случае необходимости).

Объекты анализа защищенности

В качестве объектов анализа защищенности могут выступать:

- автоматизированные системы;
- средства вычислительной техники;
- выделенные помещения;
- средства защиты информации.

Если автоматизированная система рассматривается как объект защиты, то необходимо соблюдение некоторых требований. Итак, АС должна:

- находиться на строго ограниченной контролируемой территории;

- выполнять четко определенные функции, заранее оговоренные документацией;
- управляться подразделением организации, несущим ответственность за ее функционирование.

Объектами защиты в широком смысле слова могут являться комплексы и отдельные средства автоматизации, телекоммуникационные и информационные системы. Кроме того, защищаться может организационно-управленческий процесс.

Для проведения анализа защищенности также характерно разделение на собственно автоматизированные системы и выделенные помещения. В первом случае оценивается значение технических каналов утечки информации (электромагнитных), во втором - нетехнических (акустических и виброакустических).

Наконец, в качестве объекта оценки могут выступать и непосредственно средства защиты информации.

Методы тестирования системы защиты

Тестирование системы защиты АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного программного обеспечения, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня. [3]

Кроме того, необходимо учитывать еще несколько подходов к тестированию систем защиты информации, которые могут быть использованы при проведении анализа защищенности автоматизированных систем:

- экспертно-документальный;
- пробного запуска;

- «взлома», или тестирования на устойчивость систем защиты информации в условиях внешних воздействий.

В результате оценки защищенности информации получают:

- структурированные данные о состоянии информационной безопасности в системе управления предприятием;
- детализированный перечень требований руководящих документов по защищенности информации для данного класса систем;
- рекомендации по формированию политики информационной безопасности, созданию или модернизации подсистемы защиты информации, управлению рисками и минимизации возможных потерь.

Рассмотренные направления являются на сегодняшний день одними из наиболее актуальных. Это вполне очевидно, так как использование в совокупности всех трех направлений позволяет поддерживать на достаточно высоком уровне безопасность информационных ресурсов организации. Это обусловлено тем, что направления взаимно дополняют друг друга и создают комплексность и непрерывность обеспечения информационной безопасности организации.

Контрольные задания и вопросы

1. Дайте определение защищенности автоматизированной системы.
2. Назовите основные и дополнительные исходные данные по обследуемой системе.
3. Какие требования предъявляются к автоматизированной системе как к объекту защиты?
4. Охарактеризуйте основные методы тестирования автоматизированных систем.

2. ОСНОВЫ ИСПОЛЬЗОВАНИЯ ГОСТ ИСО/МЭК 15408-2002

2.1 Использование международного опыта в развитии нормативной базы оценки безопасности информационных технологий

Общие сведения. Этапы создания Общих критериев. Использование международного стандарта ISO/IEC 15408-99 в России

Общие сведения

В российской практике сертификации принято оценивать по требованиям безопасности информации либо средства вычислительной техники (СВТ), либо автоматизированные системы (АС). До 2002 года на территории РФ единственными нормативными документами, позволяющими оценить защищенность средств вычислительной техники и автоматизированных систем, являлись руководящие документы ФСТЭК России [5-10].

Качественно новым этапом в развитии нормативной базы оценки безопасности ИТ послужило появление ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», который содержит полный аутентичный текст Международного стандарта ISO/IEC 15408:1999 «Information Technology. Security techniques. Evaluation criteria for IT security», так называемые «Общие критерии».

Этапы создания Общих критериев

Общие критерии представляют собой результат усилий международного сообщества по разработке критериев оценки безопасности информационных технологий.

Так в начале 1980-х годов в США были разработаны Критерии оценки доверенных компьютерных систем - «Оранжевая книга» (TCSEC). В следующем десятилетии уже сразу несколько стран принялись разрабатывать критерии оценки. Данные критерии базировались на концепции TCSEC, но были более гибкими и адаптируемыми по отношению к развитию ИТ. [11, с. 14]

В 1991 Европейской комиссией были выпущены европейские Критерии оценки безопасности информационных технологий (ITSEC), явившиеся результатом совместных усилий специалистов Франции, Германии, Нидерландов и Великобритании.

В начале 1993 года как комбинация подходов TCSEC и ITSEC в Канаде были выпущены Канадские критерии оценки доверенных компьютерных продуктов (CTCPEC), в США - рабочая версия Федеральных критериев безопасности информационных технологий (FC). [11, с. 15]

В 1990 под эгидой Международной организации по стандартизации (ISO) началась разработка международных стандартизированных критериев оценки. Новые критерии должны были учесть потребность во взаимном признании результатов оценки безопасности на глобальном рынке ИТ.

В разработке ОК участвовали Национальный институт стандартов и техноло-

гий и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство информационной безопасности коммуникаций (Голландия), Органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция). [11, с. 15]

Разработка версии 1.0 "Общих критериев" была завершена в январе 1996 года и одобрена Международной организацией по стандартизации в апреле того же года. Был проведен ряд экспериментальных оценок на основе версии 1.0 ОК, а также организовано широкое обсуждение документа.

В мае 1998 года была опубликована версия 2.0 ОК, и на ее основе в июне 1999 года принят международный стандарт ISO/IEC 15408-99. Официальный текст стандарта издан 01 декабря 1999 года. Изменения, внесенные в стандарт на завершающей стадии его принятия, учтены в версии 2.1 ОК, идентичной стандарту по содержанию. [22]

Таким образом, подведя итог вышесказанному, можно выделить следующие основные этапы в развитии мировых концепций и критериев оценки безопасности информационных технологий:

- в TCSEC («Оранжевая книга») использована жесткая классификационная структура требований безопасности, что характерно и для комплекта РД ГТК РФ по защите информации от несанкционированного доступа;
- BITSEC («Европейские критерии») выделены требований доверия и проведено их группирование по уровням доверия;
- в проекте Федеральных критериев США использована концепция профиля защиты как совокупности требований безопасности для типов продуктов и систем информационных технологий.

В итоге, Общие критерии обобщили содержание и опыт использования «Оранжевой книги», развили оценочные уровни доверия Европейских критериев, воплотили в реальные структуры концепцию типовых профилей защиты Федеральных критериев США.

Признание Общих критериев со стороны ИСО способствует их быстрому распространению в мире в качестве стандарта по сертификации и оценке безопасности изделий (продуктов и систем) ИТ. [12]

Использование международного стандарта ISO/IEC 15408-99 в России

В октябре 2000 года на заседании Коллегии Гостехкомиссии России был рассмотрен вопрос о развитии нормативно-методической базы сертификации средств защиты информации от несанкционированного доступа (НСД) на основе международного стандарта ISO/IEC 15408-99.

В последующие два года в России в этом направлении была проведена интенсивная и значительная по объему работа.

В течение года в соответствии с решением Межведомственной комиссии (МВК) Совета безопасности РФ по информационной безопасности №2.2 от 24.04.2001 г., широкий круг специалистов всесторонне изучал вопрос использования

в России международных стандартов в области безопасности информационных технологий и Общих критериев, в частности, с позиции возможных позитивных и негативных последствий развития российских стандартов на базе международных аналогов. [24]

Одновременно с этим на основе аутентичного перевода Общих критериев продолжалась разработка российского стандарта, других нормативных и методических документов в этой сфере, шло активное изучение международного опыта, в том числе Международного соглашения по признанию сертификатов, полученных на основе оценок по Общим критериям.

В апреле 2002 года Госстандарт России принял ГОСТ Р ИСО/МЭК 15408-2002, разработанный по заказу Гостехкомиссии России Центром безопасности информации, ЦНИИ Минобороны РФ, Центром "Атомзащитаинформ" и ЦНИИАТОМИНФОРМ Минатома России, ВНИИстандартом при активном участии экспертов международной рабочей группы по Общим критериям. Дата введения ГОСТа в действие - 01 января 2004 года. [12]

МВК по информационной безопасности Совета Безопасности Российской Федерации, рассмотрев на своем заседании результаты анализа последствий применения Общих критериев в России, решением от №1.2 26.03.2002 г. поручил Гостехкомиссии России в целях получения практического опыта использования международных аналогов при совершенствовании отечественных стандартов в течение 2002–2003 годов провести апробацию нормативных документов в области защиты информации, разработанных в соответствии с методологией стандарта ИСО/МЭК 15408-99, в системе сертификации средств защиты информации по требованиям безопасности информации. [12]

Во исполнение этого решения в мае 2002 года на заседании Коллегии Гостехкомиссии России был рассмотрен и одобрен Руководящий документ (РД) Гостехкомиссии России "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий", соответствующий ГОСТ Р ИСО/МЭК 15408-2002, с целью практической апробации Общих критериев до ввода в действие стандарта. Упомянутый РД введен в действие приказом Гостехкомиссии России № 187 от 19.06.2002 г. [12]

В рамках плана мероприятий по внедрению ГОСТ Р ИСО/МЭК 15408 в 2002 году специалисты ЦБИ, Центра "Атомзащитаинформ" и ЦНИИАТОМИНФОРМ разработали комментарии к российскому стандарту, поясняющие назначение, основные концептуальные положения, методологию и терминологию Общих критериев, а также расхождения в терминологии стандарта с принятой в России терминологией и действующими нормативными документами.

В связи с этим большое значение имеет работа по гармонизации отечественных и международных стандартов, в частности терминологии в области безопасности информационных технологий, которая начинается в текущем году по отдельной программе.

Контрольные задания и вопросы

1. Охарактеризуйте нормативную базу оценки защищенности в России.

2. Назовите основные связи различных стандартов и нормативов в области оценки защищенности и кратко поясните их.
3. Каковы основные этапы развития «Общих критериев»?
4. Охарактеризуйте использование стандарта ISO 15408:1999 в России на текущий момент.

2.2 Структура, назначение и особенности ГОСТ Р ИСО/МЭК 15408-2002

Общие сведения. Определенные в ГОСТ Р ИСО/МЭК 15408-2002 средства построения наборов требований безопасности. Основные конструкции требований безопасности.

Общие сведения

ГОСТ Р ИСО/МЭК 15408-2002 имеет достаточно обобщенный характер. По сути, он не содержит определенных требований к конкретным системам защиты информации, а представляет собой набор определений и правил, в рамках которых можно описывать различные системы защиты. Таким образом, стандарт предоставляет возможность формировать максимально обоснованные требования безопасности к изделиям информационных технологий с учетом реальных угроз безопасности на основе единого методического подхода.

Данный стандарт используется как при задании требований к продуктам и системам ИТ, так и при оценке их безопасности на всех этапах жизненного цикла. Он также полезен и как руководство при разработке продуктов информационных технологий, причем не только специализированных средств защиты, но и любого ПО или аппаратных средств с функциями безопасности.

Основные принципы стандарта состоят в том, что должны быть четко сформулированы угрозы безопасности и угрозы блокирования политики безопасности организации, а предложенные меры безопасности должны быть безусловно достаточными, исходя из их предназначения. [14, с.6]

Под безопасностью информационной технологии в контексте ГОСТ Р ИСО/МЭК 15408-2002 понимается состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений. [15, с.18]

Доверие к безопасности ИТ обеспечивается, как реализацией в них необходимых функциональных возможностей, так и осуществление комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, проведением независимых оценок их безопасности и контролем её уровня при эксплуатации. [15, с.17]

Согласно ОК, основными целями обеспечения безопасности информационных технологий являются:

- предотвращение несанкционированного раскрытия информации (обеспечение конфиденциальности);

- предотвращение несанкционированной модификации и/или уничтожения информационно-программных ресурсов (обеспечение целостности);
- обеспечение своевременного санкционированного получения информации (обеспечение доступности).

Рассматриваемый стандарт не меняет сложившейся в России методологии защиты, однако по уровню систематизации, полноте и степени детализации требований, универсальности и гибкости значительно превосходит действующие в настоящее время нормативно – методические документы.

Также существует ряд отличительных особенностей данного международного стандарта от ныне действующих на территории Российской Федерации:

- прежде всего, ОК – это определенная методология и система формирования требований и оценки безопасности ИТ с наиболее полной на сегодняшний день совокупности требований безопасности ИТ;
- в ОК проведено четкое разделение требований безопасности на функциональные требования и требования доверия к безопасности. Функциональные требования относятся к функциям безопасности (идентификации, аутентификации, управлению доступом, аудиту). Требования доверия – к достижению уверенности в корректности реализации и эффективности функций безопасности путем оценки технологии разработки, тестирования, анализа уязвимостей, эксплуатационной документации, поставки, сопровождения продуктов и систем ИТ;
- общие критерии включают шкалу доверия к безопасности (оценочные уровни доверия - ОУД), которая может использоваться для получения степени уверенности в безопасности продуктов и систем ИТ;
- систематизация и классификация требований по иерархии «класс» - «семейство» - «компонент» - «элемент» с уникальными идентификаторами на каждом уровне иерархии обеспечивают удобство их использования;
- компоненты требований в семействах и классах ранжированы по степени полноты и строгости, а требования доверия сгруппированы в пакеты требований;
- гибкость в подходе к формированию требований безопасности для различных типов продуктов и систем ИТ и условий их применения обеспечивается возможностью целенаправленного формирования необходимых наборов требований в виде определенных в ОК стандартизированных структур (пакетов требований, профилей защиты, заданий по безопасности);
- общие критерии обладают открытостью и расширяемостью, то есть позволяют уточнять существующие и вводить дополнительные требования.

Таким образом, ОК представляют собой базовый стандарт, содержащий методологию задания требований и оценки безопасности ИТ, а также систематизированный каталог требований безопасности. В качестве функциональных стандартов, в которых формулируются требования к безопасности определенных типов продуктов и систем ИТ, предусматривается использование профилей защиты, создаваемых по методологии ОК и на основе каталога требований.

Некоторые аспекты безопасности информационных технологий находятся вне

рамок Общих критериев:

- стандарт не содержит критериев оценки безопасности, касающихся административных мер, непосредственно не относящихся к мерам безопасности ИТ. Административные меры безопасности в среде эксплуатации ОО рассматриваются в качестве предположений о безопасном использовании;
- оценка физических аспектов безопасности, таких, как контроль электромагнитного излучения не рассматривается;
- в ОК не рассматривается ни методология оценки, ни нормативная и правовая база, на основе которой критерии могут применяться органами оценки;
- процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. Аттестация продукта или системы ИТ является административным актом, посредством которого компетентный орган допускает их использование в конкретных условиях эксплуатации;
- критерии для оценки специфических качеств криптографических алгоритмов в ОК не входят. [13]

Определенные в ГОСТ Р ИСО/МЭК 15408-2002 средства построения наборов требований безопасности

Как уже отмечалось выше, данный стандарт содержит детальный и структурированный набор требований и правил к механизмам безопасности, мерам и средствам обеспечения их реализации.

В соответствии с концепцией ОК, требования к безопасности объекта оценки разделяются на две категории: функциональные требования и требования гарантированности.

Функциональные требования предъявляются к функциям ОО, предназначенным для поддержания безопасности ИТ, и определяют предусмотренный безопасный режим функционирования ОО. Данные требования сгруппированы и приведены в виде систематизированного каталога во второй части ГОСТ Р ИСО/МЭК 15408. Примерами функциональных требований являются требования к идентификации, аутентификации, аудиту безопасности, управлению доступом. Функциональные требования, сформированные для конкретного ОО, определяют в целом функции безопасности ОО, подлежащие реализации и оценке в этом ОО. [16, с.64]

Гарантированность - основа уверенности в том, что продукт или система ИТ выполняют цели безопасности. [14, с.7] Таким образом, требования гарантированности определяют меры и средства, которые должны быть использованы в процессе создания ИТ с целью приобретения необходимой уверенности в правильности реализации механизмов безопасности и в их эффективности.

Требования гарантированности, по сравнению с функциональными, представляются более проработанными, поскольку для них определены семь оценочных уровней доверия (ОУД). ОУД составлены из компонентов требований гарантированности и образуют возрастающую шкалу требований доверия к безопасности. Оценка гарантированности получается на основе изучения назначения, структуры и

функционирования объекта оценки. Рассмотрим основные оценочные уровни доверия по источнику [16].

Оценочный уровень доверия 1 (ОУД 1), предусматривающий функциональное тестирование, применим, когда требуется некоторая уверенность, что объект оценки работает безукоризненно, а угрозы безопасности не считаются серьёзными. Его можно достичь при помощи разработчика и с минимальными затратами посредством анализа функциональной спецификации, спецификации интерфейсов, эксплуатационной документации в сочетании с независимым тестированием.

Оценочный уровень доверия 2 (ОУД 2) предусматривает структурное тестирование и доступ к части проектной документации и результатам тестирования разработчиком. ОУД 2 применим, когда разработчикам или пользователям требуется независимо получаемый умеренный уровень доверия при отсутствии доступа к полной документации по разработке.

В дополнение к ОУД 1 предписывается анализ проекта верхнего уровня. Анализ должен быть поддержан независимым тестированием функций безопасности, актом разработчика об испытаниях, основанных на функциональной спецификации, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска явных уязвимостей. Требуется наличие списка конфигурации ОО с уникальной идентификацией элементов конфигурации и свидетельства безопасных процедур поставки.

Оценочный уровень доверия 3 (ОУД 3), предусматривающий систематическое тестирование и проверку, позволяет достичь максимально возможного доверия при использовании обычных методов разработки. Он применим в тех случаях, когда разработчикам или пользователям требуется умеренный уровень доверия на основе всестороннего исследования объекта оценки и процесса его разработки.

По сравнению с ОУД 2, в ОУД 3 добавлено требование, которое предписывает разработчику создавать акт об испытаниях с учетом особенностей не только функциональной спецификации, но и проекта верхнего уровня. Кроме того, требуется контроль среды разработки и управление конфигурацией объекта оценки.

Оценочный уровень доверия 4 (ОУД 4) предусматривает систематическое проектирование, тестирование и просмотр. Он позволяет достичь доверия, максимально возможного при следовании общепринятой практике коммерческой разработки. Это самый высокий уровень, на который экономически целесообразно ориентироваться для существующих типов продуктов.

ОУД 4 характеризуется анализом функциональной спецификации, полной спецификации интерфейсов, эксплуатационной документации, проектов верхнего и нижнего уровней, а также подмножества реализации, применением неформальной модели политики безопасности ОО. Среди других дополнительных требований – независимый анализ уязвимостей, демонстрирующий устойчивость к попыткам проникновения нарушителей с низким потенциалом нападения, и автоматизация управления конфигурацией.

Отличительными особенностями оценочного уровня доверия 5 (ОУД 5) являются полуформальное проектирование и тестирование. С помощью ОУД 5 достигается доверие, максимально возможное при следовании строгой практике коммерческой разработки, поддержанной умеренным применением специализированных ме-

тодов обеспечения безопасности. ОУД 5 востребован, когда нужен высокий уровень доверия и строгий подход к разработке, не влекущий излишних затрат.

Для достижения ОУД 5 требуется формальная модель политики безопасности ОО и полуформальное представление функциональной спецификации и проекта верхнего уровня, полуформальная демонстрация соответствия между ними, а также модульная структура проекта ОО. Акт об испытаниях должен быть основан ещё и на проекте нижнего уровня. Необходима устойчивость к попыткам проникновения нарушителей с умеренным потенциалом нападения.

Оценочный уровень доверия 6 (ОУД 6) характеризуется полуформальной верификацией объекта. Он позволяет получить высокое доверие путем применения специальных методов проектирования в строго контролируемой среде разработки при производстве высококачественных изделий ИТ и при защите ценных активов от значительных рисков.

Особенностями ОУД 6 являются следующие факторы: структурированное представление реализации, полуформальное представление проекта нижнего уровня, иерархическая структура проекта ОО, устойчивость к попыткам проникновения нарушителей с высоким потенциалом нападения, использование структурированного процесса разработки, полная автоматизация управления конфигурацией ОО.

Оценочный уровень доверия 7 (ОУД 7), предусматривающий формальную верификацию проекта, применим к разработке изделий ИТ для использования в ситуациях чрезвычайно высокого риска или там, где высокая ценность активов оправдывает повышенные затраты.

Таким образом, на седьмом оценочном уровне доверия дополнительно требуются:

- формальное представление функциональной спецификации и проекта верхнего уровня и формальная демонстрация соответствия между ними;
- модульная, иерархическая структура проекта ОО;
- полное независимое подтверждение результатов тестирования разработчиком. [16, с. 77-78]

На основе анализа вышеизложенного можно сделать вывод, что для большинства областей применения достаточно третьего уровня доверия. Так как ОУД 3 достижим при разумных затратах на разработку, его можно считать типовым.

Также, по мнению автора, при конфигурировании повышенной защищенности наиболее разумно применять четвертый оценочный уровень.

Функциональные требования и требования гарантированности представлены в едином стиле согласно иерархии «класс» – «семейство» – «компонент» – «элемент». [13]

Термин «класс» используется для наиболее общей группировки требований безопасности. Члены класса называются семействами. В семейства группируются наборы требований, которые обеспечивают выполнение определенной части целей безопасности и могут отличаться по степени жесткости. Члены семейства называются компонентами. Компоненты описывают минимальный набор требований безопасности и построены из элементов, где элемент – самый нижний, неделимый уровень требований безопасности.

Основные конструкции требований безопасности

В качестве основных конструкций требований безопасности в Общих критериях определены профили защиты и задания по безопасности.

Профиль защиты (ПЗ) определяет проблему безопасности, которую нужно решить. В терминах ГОСТ Р ИСО/МЭК 15408 проблема безопасности определяется так называемой средой безопасности:

- угрозами, которым нужно противостоять;
- правилами политики безопасности организации, которым нужно следовать;
- предположениями безопасности – которые необходимо реализовать в среде функционирования изделия ИТ. [17, с.40]

Для решения проблемы безопасности в ПЗ формулируются цели безопасности, которые необходимо достичь, и требования безопасности, которые должны быть удовлетворены.

Разработка ПЗ сопровождается аргументированным обоснованием соответствия требований целям безопасности, целей безопасности – аспектам среды безопасности.

Профиль защиты в общем случае инвариантен к средствам реализации его требований. То есть технические решения, удовлетворяющие конкретному ПЗ, могут быть разными. Этим и интересен профиль защиты, как инструмент регламентации требований на уровне государства, ведомства, сообщества пользователей, отдельной организации. [16, с. 65] Профиль защиты отвечает на вопрос: «Что надо сделать», но не говорит (не навязывает), как это сделать.

Исходя из этого, логично сделать следующий вывод - профиль защиты представляет собой функционально полный, прошедший апробацию стандартизированный набор требований, предназначенный для многократного использования.

Задание по безопасности (ЗБ) разрабатывается по конкретному существующему изделию ИТ и в этом плане является близким по направленности (но не по форме представления) к техническим условиям. Структура задания по безопасности близка к структуре профиля защиты. Но так как здесь рассматривается уже конкретное изделие ИТ, то в ЗБ появляется краткая спецификация реализованных функций безопасности и мер доверия. [17, с.40]

Таким образом, ЗБ является тем документом, на соответствие которому проводится оценка. Если в ЗБ помещено утверждение о соответствии некоторому ПЗ, то результатом оценки будет соответствие профилю защиты, который государство или некоторое сообщество выдвинуло в качестве своих требований. [17, с. 41]

Иначе говоря, задание по безопасности – это полная комбинация требований, являющихся необходимыми для создания и оценки конкретной системы или продукта ИТ. Ввиду этого, работы по анализу требований, реализуемые на основе стандарта ОК, позволяют грамотно задать требования к безопасности ИТ [18, с. 30]. Результаты работ могут также использоваться для сравнительного анализа различных систем и продуктов ИТ.

Общие критерии заложили современную методологическую базу формирования требований безопасности (основанную на принципах гибкости, обоснованности,

достаточности, технической реализуемости и экономической эффективности требований) и современную методологическую базу оценки безопасности ИТ.

Однако, как следует из ограничений, приведенных в ГОСТ Р ИСО/МЭК 15408, его область эффективного применения связана в основанном с оценкой безопасности изделий ИТ и не охватывает ряд аспектов (оценку рисков, управление персоналом, физическую защиту, эксплуатационные требования, организационные и административные аспекты), необходимых при оценке безопасности АС.

Несмотря на некоторые ограничения в применении, сама методология формирования требований безопасности в виде профилей защиты и заданий по безопасности, описанная в ГОСТ Р ИСО/МЭК 15408, является чрезвычайно прогрессивной и её, несомненно, было бы целесообразно распространить на АС, что предполагается в настоящий момент реализовать в отечественной системе оценки ИТ. [16, с.67]

Требования к безопасности конкретных продуктов и систем ИТ устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, а также с учетом условий их применения.

Контрольные задания и вопросы

1. Поясните понятия профиля защиты и задания по безопасности.
2. Каковы основные цели безопасности согласно «Общим критериям»? Коротко поясните.
3. Поясните понятие «оценочный уровень доверия» в контексте «Общих критериев».
4. Охарактеризуйте достаточный уровень доверия для коммерческих систем.

2.3 Основные документы, выпускаемые в поддержку ГОСТ Р ИСО/МЭК 15408-2002

Общие сведения. Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». Руководящий документ «Общая методология оценки безопасности информационных технологий». Руководящий документ «Руководство по разработке профилей защиты и заданий по безопасности». Руководящий документ «Руководство по формированию семейств ПЗ». Руководящий документ «Руководство по регистрации ПЗ и ЗБ».

Общие сведения

На основе методологии ГОСТ Р ИСО/МЭК 15408-2002 (во исполнение решений Совета Безопасности Российской Федерации от 26.03.2002г. №1.2 и Коллегии Гостехкомиссии России от 30.05.2002г. №9.2) с 2002г. была начата разработка и апробация нового поколения нормативных документов в системе сертификации ФСТЭК. [19]

Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»

В качестве основы для разработки нормативных документов по оценке безопасности информационных технологий был принят Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (введен в действие с 01 августа 2002г. приказом председателя Гостехкомиссии России от 19.06.2002г. №187).

Основной целью данного РД является повышение доверия к безопасности продуктов и систем информационных технологий. Положения руководящего документа направлены на создание продуктов и систем информационных технологий с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политике безопасности с учетом условий применения, что должно обеспечить оптимизацию продуктов и систем ИТ по критерию «эффективность - стоимость». [20, с. 4]

Таким образом, данный руководящий документ по содержанию соответствует ГОСТ Р ИСО/МЭК 15408-2002 и «предназначен для практического использования в деятельности заказчиков, разработчиков, пользователей изделий ИТ, органов по оценке соответствия с обеспечением возможности оперативного внесения в него текущих изменений, вызванных необходимостью учета опыта его практического применения и совершенствования критериев оценки безопасности ИТ» [20, с. 15].

Руководящий документ «Общая методология оценки безопасности информационных технологий»

Основным сопутствующим документом, выпускаемым в поддержку Общих критериев, является Общая методологии оценки (ОМО) безопасности информационных технологий.

Общая методология оценки безопасности информационных технологий – документ, дополняющий ОК подробным объяснением основных принципов и способ проведения оценки на основе ОК. ОМО описывает тот минимум операций, который должен выполняться оценщиком при оценке по ОК с использованием критериев и свидетельств оценки, указанных в ОК.

Потенциальными пользователями ОМО являются прежде всего оценщики, применяющие ОК, и эксперты органов сертификации, подтверждающие действия оценщика, а также – заявители оценки, разработчики, авторы ПЗ/ЗБ. [21, с.57]

Руководящий документ «Руководство по разработке профилей защиты и заданий по безопасности»

Настоящий РД представляет собой методический документ по разработке профилей защиты (ПЗ) и заданий по безопасности (ЗБ) продуктов и систем информационных технологий в соответствии с РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».

Руководство содержит:

- определение назначения, состава и структуры профилей защиты и заданий по безопасности;
- общие положения и рекомендации по представлению материалов разделов профилей защиты и заданий по безопасности;
- рекомендации по представлению материалов профилей защиты и заданий по безопасности для составных изделий информационных технологий;
- рекомендации по формированию функциональных пакетов требований и пакетов требований доверия к безопасности изделий информационных технологий;
- примеры описания угроз, политик безопасности организаций, целей и требований безопасности. [22, с.41]

Руководящий документ «Руководство по формированию семейств ПЗ»

Данный документ устанавливает порядок формирования семейств профилей защиты и регламентирует:

- назначение, состав и структуру семейств профилей защиты;
- состав классов защищенности IT-изделий и соответствующих им базовых пакетов требований доверия и уровней стойкости функций безопасности;
- порядок разработки профилей защиты на основе семейств профилей защиты;
- порядок включения профилей защиты в семейство и порядок модификации семейств профилей защиты. [22, с.42]

Руководящий документ «Руководство по регистрации ПЗ и ЗБ»

Данный РД определяет процедуры, которые необходимо применять органу регистрации при сопровождении профилей защиты и пакетов для оценки безопасности информационных технологий.

В Руководстве по регистрации профилей защиты изложены:

- функции органа регистрации ПЗ и пакетов требований к безопасности изделий информационных технологий;
- порядок рассмотрения заявок на регистрацию ПЗ или пакетов требований;
- критерии отклонения заявок на регистрацию;
- порядок публикации реестра ПЗ и пакетов требований;
- процедура апелляции в отношении действий, осуществляемых органом регистрации ПЗ и пакетов требований. [22, с.42].

Контрольные задания и вопросы

1. Перечислите основные руководящие документы, выпущенные в поддержку «Общих критериев».
2. Коротко охарактеризуйте каждый из перечисленных документов.

3. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОЦЕДУР ОЦЕНКИ ПО РД ГТК РОССИИ И ГОСТ Р ИСО/МЭК 15408-2002

3.1 Сравнительный анализ концептуальных положений ОК и российской нормативной документации по безопасности информационных технологий

Общие сведения. Анализ отличий методик проведения оценки безопасности информационных технологий

Общие сведения

В Российской Федерации действует ряд законодательных правовых актов в области обеспечения информационной безопасности (ФЗ РФ от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации»; ФЗ РФ от 29.07.2004г. N 98-ФЗ «О коммерческой тайне» и другие), а также руководящие документы ФСТЭК России (ГТК РФ) по защите от несанкционированного доступа к информации, который в совокупности определяют основные концептуальные положения и терминологию в этой области, а также методологию разработки и оценки безопасности информационных технологий.

Согласно РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа», «…из общей проблемы безопасности информации выделяются те направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности технических средств, ошибки программного обеспечения или стихийные бедствия могут привести к утечке, модификации или уничтожению информации» [10]. Отсюда следует, что защита информации направлена на обеспечение конфиденциальности информации и её целостности. Об обеспечении доступности информации в данном документе не говорится.

Указанная проблема возникла в связи с тем, что ныне действующий комплект руководящих документов ФСТЭК (ГТК) России создавался в начале 90-х годов. В то время, как принятый в 2006 году ФЗ РФ №149-ФЗ «Об информации, информационных технологиях и защите информации» определяет защиту информации как принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Вместе с тем, в ОК эти три цели отнесены к основным аспектам обеспечения безопасности информационных технологий. Поэтому можно говорить об определенной общности российских концептуальных положений по защите информации с исходными посылками ОК.

Как ОК, так и рассматриваемый пакет РД в качестве источника несанкционированных действий рассматривают, прежде всего, человека, взаимодействующего с системой ИТ. В то же время в сравниваемых документах учитываются и события, не

связанные с действиями человека, например, сбои электрооборудования или ошибки, возникающие в линиях связи. Это также свидетельствует о возможности использования подходов Общих критериев в российской практике разработки и оценки информационных технологий. [23, с. 16]

Анализ отличий методик проведения оценки безопасности информационных технологий

РД [5-7] содержат критерии оценки некоторых видов продуктов и систем ИТ. В качестве объектов оценки в РД рассматриваются как средства вычислительной техники, так и автоматизированные системы. Все объекты классифицируются, причем каждому классу соответствует определенная совокупность требований (показателей защищенности) безопасности информации. [23, с. 16]

В РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» классификация проводится исходя из условий применения АС.

Для классификации АС выбраны три критерия, имеющие по два значения:

- режим работы АС (однопользовательский или многопользовательский);
- права пользователей на доступ к обрабатываемой к АС информации (равные или различные права);
- количество уровней конфиденциальности информации, обрабатываемой в АС (один или несколько уровней конфиденциальности информации).

Для каждой комбинации значений этих критериев подразумевались определенные виды угроз информации и режимы работы с информацией ограниченно доступа, исходя из которых формировались совокупности функциональных требований. При этом заказчик АС легко определял класс защищенности АС, а разработчик ориентировался на разработку СВТ (или ИТ) определенного класса защищенности. Явно ни в одном РД [5-7] угрозы информации для указанных видов продуктов или систем не приведены. [23, с. 16]

Такой упрощенный подход привел к тому, что все многообразие АС было сведено к девяти классам, то есть было необходимо предъявить к АС только одну из девяти совокупности требований по безопасности информации. Возможно, это было оправдано на момент выпуска РД (1992 год), когда использовались, в основном, мэйнфреймы и терминальные сети на их базе. [23, с. 16]

Однако в настоящее время, при большом многообразии конфигураций вычислительных систем, относить их к одному из девяти классов систем без учета их особенностей весьма затруднительно. Общие критерии снимают эту проблему. По методологии ОК, профиль защиты, назначение которого по нашей терминологии соответствует классу защищенности. [23, с. 17] Может быть разработан для любого вида или продукта систем ИТ с учетом как всех особенностей данного вида продукта или системы, так и условий их применения.

В ОК используется понятие «система ИТ». Следует отметить, что используемое в российской нормативной документации понятие «автоматизированная система» и «система ИТ» из ОК – понятия не совпадающие. В соответствии с ГОСТ

34.003-90, автоматизированная система определяется как система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационные технологии выполнения установленных функций. Понятие «система ИТ» определяется как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации. То есть, в отличие от АС понятие «система ИТ» как объект оценки не включает человека, а ограничивается только программно-аппаратными средствами с соответствующими руководствами.

В РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» наряду с требованиями к программно – аппаратным средствам АС содержатся требования организационного порядка, а также требования по физической защите.

По методологии ОК в ПЗ должно содержаться описание условий, в которых будет применяться объект оценки. Данные условия описываются в разделе ПЗ «Среда безопасности». В этот раздел включается описание предположений, угроз, политики безопасности организации, валяющих на формирование функциональных требований к объекту оценки и требований доверия.

Например, в качестве предположения в ПЗ может быть указано, что доступ посторонних в помещение, где расположены рабочие станции сети, маловероятен (ограничен, исключен). Это означает, что продукт или система ИТ должны функционировать в помещении, в котором в той или иной степени реализована физическая защита и действует политика безопасности организации, ограничивающая доступ. [23, с. 17]

Другим примером, касающимся политики безопасности организации, является правило, согласно которому печать документов разрешается только в соответствии с правилами делопроизводства. Это означает, что указанный ПЗ подойдет потребителю продукта или системы, соответствующих данному ПЗ, только в том случае, если у него обеспечена соответствующая физическая защита и реализован порядок делопроизводства.

При переходе к формированию требований безопасности к определенному типу продукта или системы ИТ по методологии ОК соответствующие нормативные документы должны быть изложены в формате профилей защиты. В отличие от РД [5-7], формат ПЗ предполагает наличие в нем подробного описания продукта или системы ИТ, их окружения, угроз безопасности и/или политики безопасности, требований безопасности, а также обоснования как целей, так и требований.

ОК предписывают, что «цели безопасности должны отражать изложенное намерение противостоять всем установленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации». При этом при постановке целей безопасности используется описание либо угроз, либо политики безопасности организации, либо и того, и другого. [23, с. 18]

Таким образом, принимая возможность постановки целей безопасности, исходя из угроз и /или политики безопасности, авторы ОК ориентируются на то, что чем подробнее и яснее будет описана среда, тем яснее будет постановка целей. То же касается предположений.

Профиль защиты по сравнению с набором требований конкретного класса защищенности РД содержит не только перечень требований к продукту или системе ИТ, но и логическое обоснование того, что именно эти требования необходимы.

Другой особенностью является обязательное включение в профиль защиты не только функциональных требований, но и требований доверия к безопасности. Частично, правда, в других формулировках подобные требования содержатся в РД [5, 6]. Однако в ОК перечень этих требований полнее, более систематизирован и детализирован.

В соответствии с российским подходом сертификации продуктов и систем ИТ по требованиям безопасности информации проводится, в основном, на соответствие требованиям РД. Однако в связи с ограниченными возможностями набора действующих РЛ (к некоторым видам продуктов и систем ИТ не сформулированы требования безопасности и не оформлены в виде РД), сертификация выполняется иногда на соответствие требованиям, приведенным разработчиком (изготовителем) в технических условиях (ТУ) на продукт или систему ИТ.

По методологии ОК оценка продуктов и систем ИТ не проводится на соответствие ПЗ в принципе, а только на соответствие ЗБ. Это связано с тем, что оценка осуществляется с целью проверки соответствия ОО тем требованиям, о реализации которых разработчик объявил в ЗБ. При этом в ЗБ может быть заявлено о соответствии одному или нескольким ПЗ. В российской же практике сертификация ОО по ТУ используется только в том случае, когда нет соответствующего РД. [23, с. 19]

Сходство в подходе к сертификации по требованиям безопасности информации в российской практике и к оценке продуктов и систем ИТ по ОК состоит в том, что для оценки используются четко заданные наборы требований (классы РД у нас, ЗБ в ОК). Именно потому, что ПЗ не является точно заданным набором требований в окончательном виде (так как допускается уточнение и конкретизацию требований) и не проводится оценка на соответствие требованиям ПЗ.

Российская практика разработки СВТ и АС состоит в том, что, что СВТ и АС разрабатываются на основе технических заданий (ТЗ). Как правило, такие ТЗ включают раздел, касающийся безопасности информации. Указанный раздел должен содержать требования по безопасности информации. Требования либо формулируются в произвольной форме, либо содержится требование соответствия определенному классу защищенности из РД ГТК. В первом случае, если совокупность требований не соответствует какому-либо классу защищенности, для последующей разработки должны быть разработаны ТУ, и в дальнейшем СВТ будет оцениваться на соответствие требования ТУ. В противном случае, СВТ или АС оцениваются на соответствие требованиям РД.

При переходе к ОК по форме и содержанию РД будут заменены ПЗ, тогда ТЗ может содержать требование соответствия определенному ПЗ с уточнениями и дополнениями при необходимости. При этом раздел требований по безопасности в ТУ должен будет излагаться в формате ЗБ в составе ТУ или в виде отдельного документа. [23, с. 19]

Необходимо отметить и тот факт, что по сравнению с РД, в ОК значительно больше внимания уделено процедурам поставки (важно, чтобы при выполнении процедуры поставки программный продукт был защищен от подмены или модифи-

кации) и поддержке продукции.

Также, в ОК акцентируется внимание на следующий факт - программный продукт, который не поддерживается должным образом разработчиком, не может считаться "доверенным", не может претендовать на высокий уровень ОУД, а значит, не может применяться для защиты ценной информации.

На сегодняшний день в Российской Федерации имеется определенный опыт проведения оценки по требованиям безопасности информации объектов информатизации. В частности, к таким видам оценки относятся процессы аттестации и сертификации объектов информатизации. При этом технология контроля (оценки) защищенности информации, принятая в Российской Федерации, основанная на базе Руководящих документов ФСТЭК (ГТК) России 1992-1993 годов, существенно отличается от технологий, применяемых в настоящее время в международной практике.

В связи с этим, ниже будут представлены основные положения оценки информационных технологий по требованиям безопасности как на основании РД ФСТЭК (ГТК) России, так и согласно концепции Общих Критериев.

Контрольные задания и вопросы

1. Поясните проблему доступности в контексте ОК и РД ГТК.
2. Назовите основные признаки классификации автоматизированных систем по РД ГТК.
3. Поясните различия между профилем защиты и набором требований к СЗИ.
4. Охарактеризуйте различия между понятиями «система ИТ» и «автоматизированная система».

3.2 Методологии оценки безопасности информационных технологий

Методология оценки безопасности информационных технологий по Общим критериям. Методы оценки безопасности объектов информатизации на соответствие требованиям РД ГТК России. Выводы по сравнению нормативных основ анализа защищенности.

Методология оценки безопасности информационных технологий по Общим критериям

Основным сопутствующим документом, выпускаемым в поддержку Общих критериев, является «Общая методология оценки безопасности информационных технологий» (ОМО).

Причиной создания ОМО явилась унификация на международном уровне способов и приемов проведения оценки в соответствии с Общими критериями в целях взаимного признания оценок и, таким образом, устранения накладных расходов, связанных с дублированием оценок продуктов информационных технологий (ИТ) и профилей защиты (ПЗ).

Разработчики ОМО при её создании руководствовались следующими принципами:

- объективность: результаты оценки основываются на фактических свидетельствах и не зависят от личного мнения оценщика;
- беспристрастность: результаты оценки являются непредубежденными, когда требуется субъективное суждение;
- воспроизводимость: действия оценщика, выполняемые с использованием одной и той же совокупности поставок для оценки, всегда приводят к одним и тем же результатам;
- корректность: действия оценщика обеспечивают точную техническую оценку;
- достаточность: каждый вид деятельности по оценке осуществляется до уровня, необходимого для удовлетворения всех заданных требований доверия;
- приемлемость: каждое действие оценщика способствует повышению доверия, по меньшей мере, пропорционально затраченным усилиям. [23, с. 33]

Эти принципы нашли отражение при описании представленных в методологии видов деятельности по оценке.

Соотношение структур Общих критериев и Общей методологии оценки безопасности информационных технологий

Между структурой ОК (класс – семейство – компонент - элемент) и структурой ОМО (вид деятельности – подвид деятельности – действие – шаг оценивания) была установлена прямая взаимосвязь. Причем, семейства доверия прямо не рассматриваются в ОМО, поскольку при проведении оценки всегда используется только один компонент доверия из применяемого семейства.

Рисунок 1 иллюстрирует соответствие между такими конструкциями ОК, как классы, компоненты и элементы действий оценщика, и рассматриваемыми в ОМО видами деятельности, подвидами деятельности и действиями. Вместе с тем, некоторые шаги оценивания ОМО могут прямо следовать из требований ОК, содержащихся в элементах действий разработчика, содержания и представления свидетельств.

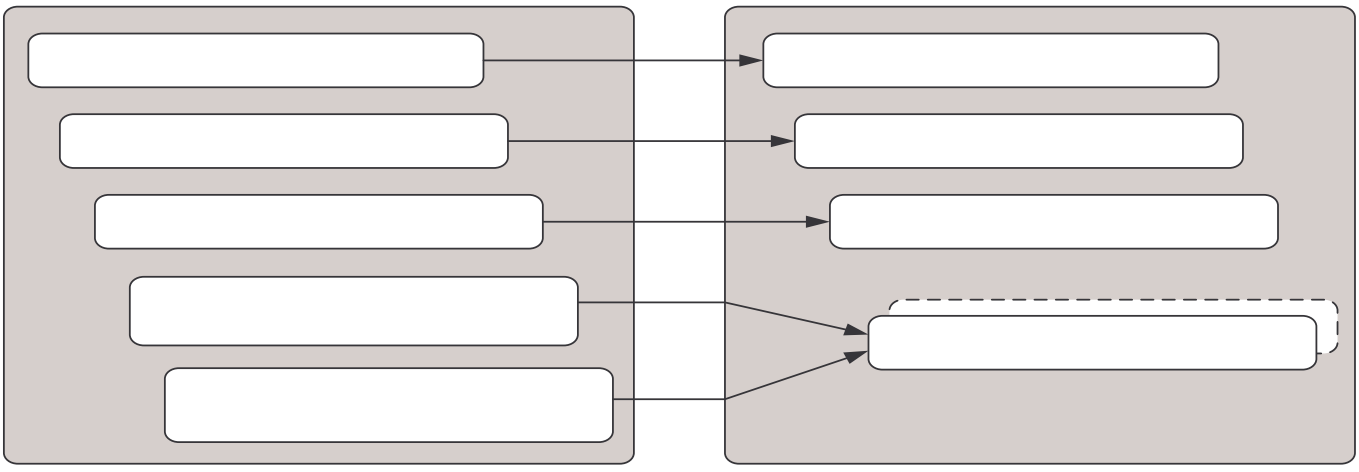

Рисунок 1 – Соотношение структур ОК и ОМО

Как видно из рисунка 1, с элементом действий оценщика из части 3 ОК связан термин "Действие". Эти действия или сформулированы в явном виде как действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов доверия из части 3 ОК. [21, с. 55]

Термин "Шаг оценивания" описывает неразделимый фрагмент работы по оценке. Каждое действие в ОМО включает один или несколько шагов оценивания, которые сгруппированы по элементам содержания и представления или действий разработчика соответствующего компонента из части 3 ОК. Шаги оценивания представлены в ОМО в том же порядке, что и элементы ОК, из которых они следуют. Шаги оценивания содержат обязательные действия, которые оценщик должен выполнить, чтобы прийти к заключению.

Текст, сопровождающий шаги оценивания, содержит дальнейшие разъяснения использования формулировок ОК при оценке. Хотя сопроводительный текст не предписывает обязательные меры, он дает представление о том, что ожидается от оценщика при удовлетворении обязательных аспектов шагов оценивания. [21, с. 57-58]

Общая модель оценки

Согласно ОМО, процесс оценки состоит из выполнения оценщиком задачи получения исходных данных для оценки, подвидов деятельности по оценке и задачи оформления результатов оценки. Рисунок 2 дает общее представление о взаимосвязи этих задач и подвидов деятельности по оценке.

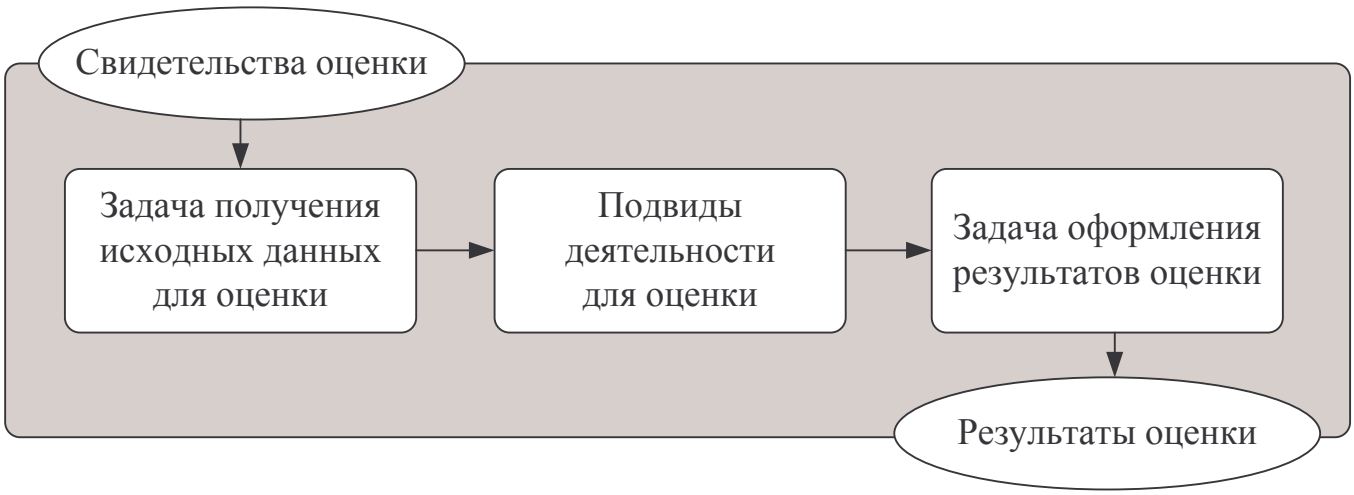

Рисунок 2 – Общая модель оценки

На основании вышеуказанной иллюстрации – общей модели оценки, выделяют три стадии проведения оценки:

- подготовка к оценке;
- проведение работ по оценке;
- завершение процесса оценки.

Стадия «Подготовка к оценке» включает начальный контакт между заявителем и оценщиком, консультации с целью определения готовности к оценке и непосредственно подготовку к самой оценке. Консультации должны подтвердить, что заявитель и разработчик должным образом подготовились к проведению оценки, и

включают, как минимум, предварительный анализ ЗБ и других представляемых для оценки материалов.

При принятии решения о возможности выполнения оценки утверждается список материалов, которые должны быть представлены для оценки, план – график их представления и план проведения оценки.

Этапами технологического цикла подготовки к оценке, согласно ОК являются:

- определение объекта оценки (ОО);
- описание таких аспектов среды ОО, как:
  - предположение безопасности (выделяет объект оценки из общего контекста, задают границы рассмотрения. Истинность данных предположений принимается без доказательства, а из множества возможных отбирается только то, что заведомо необходимо для обеспечения безопасности ОО);
  - угрозы безопасности ОО, наличие которых в рассматриваемой среде установлено или предполагается. Угрозы характеризуются несколькими параметрами: источник, метод воздействия, опасные с точки зрения злонамеренного использования уязвимости, ресурсы (активы), потенциально подверженные повреждению.

При анализе рисков принимаются во внимание вероятность активизации угрозы и ее успешного осуществления, а также размер возможного ущерба. По результатам анализа из множества допустимых угроз отбираются только те, ущерб от которых нуждается в уменьшении;

- положения политики безопасности, предназначенные для применения к объекту оценки. Для системы ИТ такие положения могут быть описаны точно, для продукта - в общих чертах;
- формулировка целей безопасности для ОО, направленные на обеспечение противостояния угрозам и выполнение политики безопасности;
- обоснованное определение требований безопасности, предъявляемых к объекту и среде – функциональных и требований доверия;

После того как сформулированы функциональные требования, требования доверия и требования к среде, возможна оценка безопасности изделия ИТ. [24, с. 52]

Стадия «Проведение работ по оценке». Процесс проведения оценки – это структурированный формальный процесс, в ходе которого оценщику необходимо выполнить ряд действий, определенных в ОК и представленных ниже. Подробности выполнения действий по оценке продукта ИТ на ОУД 1 – ОУД 4 приведены в ОМО. В результате оценщиком формируется отчеты о недостатках представленных к оценке материалов, подготавливается Технический отчет об оценке (ТОО).

При проведении оценки изделия ИТ главными являются следующие вопросы: «Отвечают ли функции безопасности ОО функциональным требованиям?», «Корректна ли реализация функций безопасности?».

Задача оценки в общем случае разбивается на следующие подзадачи:

- оценка задания по безопасности;
- оценка управления конфигурацией ОО;
- оценка документации по передаче ОО потребителю и эксплуатационной документации; оценка документации разработчиков; оценка руководств;

- оценка поддержки жизненного цикла ОО;
- оценка тестов; тестирование;
- оценка анализа уязвимостей.

Стадия «Завершение процесса оценки» предполагает процесс передачи испытательной лабораторией органу по сертификации выходных материалов оценки – ТОО. Технический отчет об оценке содержит информацию ограниченного доступа и, следовательно не является общедоступным документом. Орган по сертификации использует информацию ТОО для подготовки к публикации отчета по сертификации. [24, с. 53-54]

Субъекты, участвующие в процессе оценки

Общая модель оценки предусматривает наличие следующих четырех ролей: заявитель, разработчик, оценщик и орган оценки.

Заявитель инициирует оценку, то есть является заказчиком оценки и отвечает за обеспечение оценщика свидетельствами оценки.

Разработчик предъявляет объект оценки (ОО) и отвечает за представление свидетельств, требуемых для оценки (например, проектной документации), от имени заявителя.

Оценщик принимает свидетельства оценки от разработчика от имени заявителя или непосредственно от заявителя, выполняет подвиды деятельности по оценке и представляет результаты оценки органу оценки.

Орган оценки организует и поддерживает систему оценки, контролирует процесс оценки и выпускает отчеты о сертификации, а также выдает сертификаты, основываясь на результатах, представленных оценщиками.

Для предотвращения негативного влияния на оценку предусматривается определенное разделение ролей. То есть роли, описанные выше, должны выполняться разными организациями. Исключение — возможность выполнения роли разработчика и роли заявителя одной и той же организацией. [25]

В ходе проведения оценки оценщик может получить доступ к коммерческой информации заявителя и разработчика (например, информации о конструкции ОО или специализированных инструментальных средствах), а также к информации, являющейся в соответствии с действующим законодательством информацией ограниченного доступа. В этих случаях от оценщика потребуется поддержание конфиденциальности предоставленных ему свидетельств оценки.

В настоящее время общеупотребительным подходом к построению критериев оценки безопасности ИТ является использование совокупности определенным образом упорядоченных качественных требований к функциональным механизмам обеспечения безопасности, их эффективности и доверия к реализации.

Качественные критерии применимы для оценки большей части механизмов обеспечения безопасности ИТ, а также оценки выполнения требований доверия к безопасности изделий ИТ. Несмотря на это, ОМО предусматривает возможность проведения, там где это применимо, количественных оценок с использованием соответствующих качественных показателей.

Чтобы корректно использовать количественный показатель, он должен иметь объективную интерпретацию, однозначную зависимость от отдельных аспектов безопасности. Поэтому количественные критерии целесообразно использовать для оценки таких механизмов безопасности, как парольная защита, контрольное суммирование. [21]

Так как, несмотря на то, что ОМО предусматривает возможность выполнения количественных оценок, но результирующая оценка безопасности ИТ имеет качественное выражение, направление количественной оценки ОМО рассмотрено не было.

Правила формирования заключения по результатам оценки

При выполнении работы по оценке оценщик делает заключения относительно выполнения требований ОК. Наименьшая структурная единица ОК, по которой делается заключение — элемент действий оценщика. Заключение по выполняемому элементу действий оценщика из ОК делается в результате выполнения соответствующего действия из ОМО и составляющих его шагов оценивания. [26]

В ОМО различаются три взаимоисключающих вида заключения:

- условиями положительного заключения являются завершение оценщиком элемента действий оценщика из ОК и определение, что при оценке требования к ПЗ, ЗБ или ОО выполнены. Для элемента условием положительного заключения является успешное завершение всех шагов оценивания, составляющих соответствующее действие из ОМО;
- условиями отрицательного заключения являются завершение оценщиком элемента действий оценщика из ОК и определение, что при оценке требования к ПЗ, ЗБ или ОО не выполнены;
- все заключения являются неокончательными до выдачи положительного или отрицательного заключения. [26]

Общее заключение положительно только тогда, когда все составляющие заключения положительны.

В результате оценки ОО должна быть установлена степень доверия тому, что ОО соответствует требованиям, а именно:

- отвечают ли специфицированные функции безопасности ОО функциональным требованиям и, следовательно, эффективны ли они для достижения целей безопасности ОО;
- правильно ли реализованы специфицированные функции безопасности ОО.

Оформление результатов оценки

Основные выходные результаты оценки оформляются в виде сообщений о проблемах (если это необходимо при выполнении оценки) и технического отчета об оценке (ТОО) [17, с. 40]. Для сообщения о проблеме (СП) и ТОО ОМО определяет лишь содержание минимально необходимой информации и не препятствует включению в эти сообщения (отчеты) дополнительной информации, которая может требоваться в рамках конкретной системы оценки.

Сообщение о проблемах (СП) предоставляют оценщику механизм для запроса разъяснений (например, от органа оценки о применении требований) или для определения проблемы по одному из аспектов оценки (например, запрос на корректировку ЗБ, направляемый заявителю оценки).

Таким образом, СП может использоваться оценщиком как один из способов выражения потребности в разъяснении, либо для отражения результата оценки при отрицательном заключении (окончательном или неокончательном).

Оформляя СП, оценщик должен привести в нем следующую информацию:

- идентификатор оцениваемого ПЗ или ОО;
- ссылку на задачу/подвид деятельности по оценке, при выполнении которой/которого была выявлена проблема;
- суть проблемы;
- оценку серьезности проблемы (например, приводит к отрицательному заключению, задерживает выполнение оценки или требует решения до завершения оценки);
- идентификационную информацию организации, ответственной за решение проблемы;
- рекомендуемые сроки решения проблемы;
- влияние на оценку отрицательного результата решения проблемы. [21, с. 60]

Результаты оценки отражаются в ТОО, в котором оценщик представляет техническое обоснование сделанных им заключений. Минимальные требования к содержанию ТОО определены в ОМО.

При изложении информации в ТОО необходимо исходить из того, что тот, кто будет знакомиться с данным документом, имеет представление об общих концепциях информационной безопасности, ОК, ОМО и подходах к оценке безопасности ИТ.

Основная цель ТОО — помочь органу оценки провести независимую экспертизу и подтвердить результаты оценки.

В ОМО предусмотрены две разновидности ТОО:

- ТОО по результатам оценки ПЗ;
- ТОО по результатам оценки ОО.

Принимая во внимание тот факт, что данные два типа ТОО имеют схожую структуру, а также так как далее пойдет речь об оценке продуктов и систем ИТ, то ниже буде рассмотрен только ТОО по результатом оценки ОО.

Технический отчет об оценке ОО (продукта или системы ИТ)

Содержание ТОО, отражающего результаты оценки ОО, имеет следующую структуру:

Введение – в данном разделе оценщик должен привести следующую информацию:

- идентификационная информация системы оценки, требуемая для однозначной идентификации системы, в рамках которой проводилась оценка ОО;
- название, дата составления и номер версии ТОО;
- информация управления конфигурацией ОО (наименование и номер версии)

для того, чтобы орган оценки мог определить, что именно подвергалось оценке;

- название, дата составления и номер версии ЗБ для того, чтобы орган оценки мог определить, на соответствие чему проводилась оценка, и подтвердить правильность заключений, сделанных оценщиком;
- ссылка на ПЗ (если ЗБ содержит утверждение о соответствии ОО требованиям одного или нескольких ПЗ);
- идентификационная информация разработчика ОО;
- идентификационная информация заявителя оценки ОО;
- идентификационная информация оценщика.

Описание архитектуры ОО (оценщик должен привести высокоуровневое описание ОО и его главных компонентов, основанное на свидетельстве оценки, указанном в семействе доверия ОК "Проект верхнего уровня" (ADV_HLD), если компонент доверия из этого семейства был включен в ЗБ, и по нему выполнялась оценка);

Оценка – оценщик должен привести следующую информацию:

- ссылки на критерии, методологию, технологии и инструментальные средства оценки, использованные при оценке ОО;
- сведения о каких-либо ограничениях, имевших место в процессе оценки ОО или при обработке результатов этой оценки, а также о предположениях, сделанных в процессе оценки, которые повлияли на ее результаты.

Кроме того, оценщик может включить в ТОО информацию о каких-либо правовых или законодательных аспектах оценки ОО, организации работ по оценке, информацию, связанную с обеспечением конфиденциальности материалов оценки, а также другую информацию.

Результаты оценки – для каждого вида деятельности по оценке ОО оценщик должен привести следующую информацию:

- название рассматриваемого вида деятельности;
- заключение по каждому из компонентов доверия, определяющих рассматриваемый вид деятельности, как результат выполнения соответствующих действий ОМО и составляющих их шагов оценивания;
- обоснование каждого сделанного заключения, показывающее в какой мере свидетельства оценки удовлетворяют или не удовлетворяют требованиям. Обоснование должно содержать описание выполненной работы, методов и процедур, применявшихся при получении результатов.

Выводы и рекомендации – оценщик должен изложить выводы по результатам оценки ОО об удовлетворении ОО требованиям ЗБ.

Результат оценки ОО в целом должен формулироваться как "соответствие/несоответствие". При положительном результате оценки должна быть указана степень, с которой можно доверять тому, что ОО соответствуют требованиям ОК. Должно поясняться соотношение с функциональными требованиями из части 2 ОК, требованиями доверия из части 3 ОК или же непосредственно с ПЗ, как это указано ниже [20]:

- соответствие части 2 ОК — ОО соответствует части 2 ОК, если функциональные требования основаны только на функциональных компонентах из

части 2 ОК;

- расширение части 2 ОК— ОО соответствует расширению части 2 ОК, если функциональные требования включают функциональные компоненты, не содержащиеся в части 2 ОК;
- соответствие части 3 ОК — ОО соответствует части 3 ОК, если требования доверия представлены в виде ОУД из части 3 ОК или пакета требований доверия, включающего только компоненты доверия из части 3 ОК;
- усиление части 3 ОК — ОО соответствует усилению части 3 ОК, если требования доверия представлены в виде ОУД или пакета требований доверия и включают другие компоненты доверия из части 3 ОК;
- расширение части 3 ОК — ОО соответствует расширению части 3 ОК, если требования доверия представлены в виде ОУД, дополненного требованиями доверия не из части 3 ОК, или пакета требований доверия, который включает требования доверия, не содержащиеся в части 3 ОК, или полностью состоит из них.
- соответствие ПЗ — ОО соответствует ПЗ только в том случае, если он соответствует всем частям этого ПЗ.

Перечень свидетельств оценки – оценщик должен привести следующую информацию относительно каждого свидетельства оценки: идентификатор составителя (например, разработчик, заявитель), название, уникальная ссылка (например, дату составления и номер версии).

Перечень сокращений / глоссарий терминов.

Сообщение о проблемах – оценщик должен привести полный перечень СП, выпущенных в процессе оценки, а также их текущий статус. Для каждого СП в перечне следует привести идентификатор СП, а также его название или аннотацию) [21, с. 61].

Итак, в результате оценщик представляет органу оценки ТОО, а также все СП, выпущенные в процессе оценки. Договорными отношениями может быть предусмотрено предоставление ТОО заявителю или разработчику. Но если ТОО включает чувствительную для оценщика информацию (информацию о "ноу-хау" и, в первую очередь, о приемах и методах оценки), то такую информацию оценщик вправе изъять до передачи ТОО заявителю или разработчику.

Соотнесение процессов аттестации и сертификации в контексте ОК

Достаточность мер безопасности для ряда организаций, согласно действующему законодательству должна быть подтверждена органом по аттестации. Орган по аттестации определяет требования по сертификации используемых продуктов ИТ как средства подтверждения выполнения требований безопасности и адекватного противостояния угрозам.

Во многих случаях при аттестации систем ИТ возникает необходимость оценки объема работ оценщика (организации, проводящей аттестационные испытания). Необходимость эта вызвана стремлением эффективно использовать имеющиеся ресурсы. По результатам аттестационных испытаний, оценщик может рекомендовать

органу по аттестации вынести положительное решение по аттестации системы ИТ, при этом право окончательного решения принадлежит органу по аттестации.

В тех случаях, когда сертификация ИТ является необходимым условием аттестации, отчет о сертификации должен использоваться в качестве отправной точки процесса аттестации [22, с.43].

Методы оценки безопасности объектов информатизации на соответствие требованиям РД ГТК России

Система аттестации АС является составной частью единой системы сертификации средств защиты информации (СЗИ) и аттестации объектов информатизации по требованиям безопасности информации, организация функционирования которой осуществляется ФСТЭК России.

В соответствии с принятой в нашей стране концепцией защиты информации от несанкционированного доступа (НСД), существует два относительно самостоятельных направления решения этой проблемы: направление, связанное со средствами вычислительной техники (СВТ), и направление, связанное с АС. Отличие между этими направлениями заключается в том, что при рассмотрении вопросов защиты СВТ ограничиваются только программно-техническими аспектами функционирования системы, в то время как защита АС предполагает рассмотрение организационных мер защиты, вопросов физического доступа, защиты информации от утечки по техническим каналам.

Ниже будут рассмотрены отдельно два направления оценки объектов информатизации – процесс сертификации СЗИ и процесс аттестации информационных систем. Необходимо отметить следующее - в связи с тем, что в данном подразделе дипломной работы проводится сравнение методов оценки согласно ГОСТ Р ИСО/МЭК 15408-2002 и РД ГТК (ФСТЭК) России, а такое направление деятельности, как оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) отсутствует, то в текущем разделе данное направление также опущено.

Сертификация средств защиты информации

Под сертификацией средств защиты информации по требованиям безопасности информации понимается комплекс организационно – технических мероприятий, в результате которых посредствам специального документа – сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных уполномоченными федеральными органами исполнительной власти в пределах их компетенции [27].

Цель сертификации – сделать защищенность информационных систем очевидной и сравнимой так, чтобы, с одной стороны, предоставить пользователям детализированную информацию и помощь при выборе системы, а с другой стороны – дать заинтересованным изготовителя подтверждение качества их продукции [28, с. 777].

Организационную структуру системы сертификации образуют:

- ФСТЭК России (федеральный орган исполнительной власти, уполномоченный проводить работу по обязательной сертификации);
- органы по сертификации средств защиты информации - органы, проводящие сертификацию определенной продукции;
- испытательные лаборатории - лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;
- заявители - изготовители, продавцы или потребители продукции. [27]

Система сертификации средств защиты информации по требованиям безопасности информации, кроме того, включает подсистему аттестации объектов информатизации и подсистему подготовки и аттестации экспертов.

Органы по сертификации средств защиты информации и испытательные лаборатории проходят аккредитацию на право проведения работ по сертификации, в ходе которой ФСТЭК России определяет возможности выполнения этими органами и лабораториями работ по сертификации средств защиты информации.

Аккредитация проводится только при наличии у указанных органов и лабораторий лицензии на проведение мероприятий и (или) оказание услуг в области защиты государственной тайны в части технической защиты информации по сертификации и сертификационным испытаниям.

ФСТЭК России в пределах своей компетенции осуществляет следующие функции:

- создает систему сертификации средств защиты информации по требованиям безопасности информации и устанавливает правила проведения сертификации средств защиты информации;
- аккредитует органы по сертификации средств защиты информации и испытательные лаборатории;
- осуществляет выбор способа подтверждения соответствия средств защиты информации требованиям нормативных документов;
- выдает сертификаты и лицензии на применение знака соответствия;
- ведет государственный реестр участников сертификации и сертифицированных средств защиты информации;
- осуществляет государственные контроль и надзор за соблюдением участниками сертификации правил сертификации;
- рассматривает апелляции по вопросам сертификации;
- утверждает нормативные документы, на соответствие требованиям которых проводится сертификация;
- приостанавливает или отменяет действие выданных сертификатов.

Органы по сертификации средств защиты информации осуществляет следующие функции:

- сертифицируют средства защиты информации, выдают сертификаты и лицензии на применение знака соответствия с представлением копий в ФСТЭК России и ведут их учет;
- формируют фонд нормативных документов, необходимых для сертификации;
- осуществляют инспекционный контроль за сертифицированными средствами

защиты информации. [27]

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации средств защиты информации и изготовителям.

Изготовители и продавцы СЗИ должны иметь лицензию на проведение работ, связанных с созданием средств защиты, предназначенных для защиты сведений, составляющих государственную тайну и защиты конфиденциальной информации, а также лицензию на их реализацию.

Правовой базой деятельности Системы сертификации средств защиты информации по требованиям безопасности информации являются:

- ФЗ РФ "Об информации, информационных технологиях и о защите информации";
- ФЗ РФ " О техническом регулировании";
- Постановление Правительства Российской Федерации от 26 июня 1995 года № 608 "О сертификации средств защиты информации";
- порядок проведения сертификации продукции в Российской Федерации, утвержденный постановлением Госстандарта России от 21 сентября 1994 года № 15.

К основным стандартам и руководящим документам (РД) по вопросам обеспечения безопасности информации, в соответствии с требованиями которых осуществляется сертификация продукции и аттестация объектов информатизации по требованиям безопасности в области защиты информации от несанкционированного доступа, относятся:

- ГОСТ Р 50922-96. Защита информации. Основные термины и определения;
- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
- ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;
- РД ГТК (ФСТЭК) России, представленные в библиографическом списке п. 14 – п. 19.

При сертификации продукции подтверждаются следующие требования по защите информации:

- защита от несанкционированного доступа, в том числе от компьютерных вирусов;
- защита посредством криптографических преобразований;
- защита от утечки за счет побочных электромагнитных излучений и наводок;
- защита от воздействия на продукцию специальных устройств (в том числе программных закладок), встроенных в конфигурацию СЗИ.

Причем сертификации могут подтверждаться как отдельные характеристики, так и весь комплекс характеристик продукции, связанных с обеспечением безопасности информации. [28, с.783 - 784]

Так, например, руководящий документ ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показа-

тели защищенности от несанкционированного доступа к информации» устанавливает классификацию средств вычислительной техники по уровню защищенности то несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

В соответствии с данным руководящим документом возможные показатели защищенности исчерпываются семью классами. По классу защищенности можно судить о номенклатуре используемых механизмов защиты – наиболее защищенным является первый класс.

Выбор класса защиты зависит от секретности обрабатываемой информации, условий эксплуатации и расположения объектов системы. В частности, для защиты конфиденциальной информации рекомендуется применять средства защиты 5 и 6 класса.

На рисунке 3 показана зависимость секретности информации от класса защищенности СВТ.

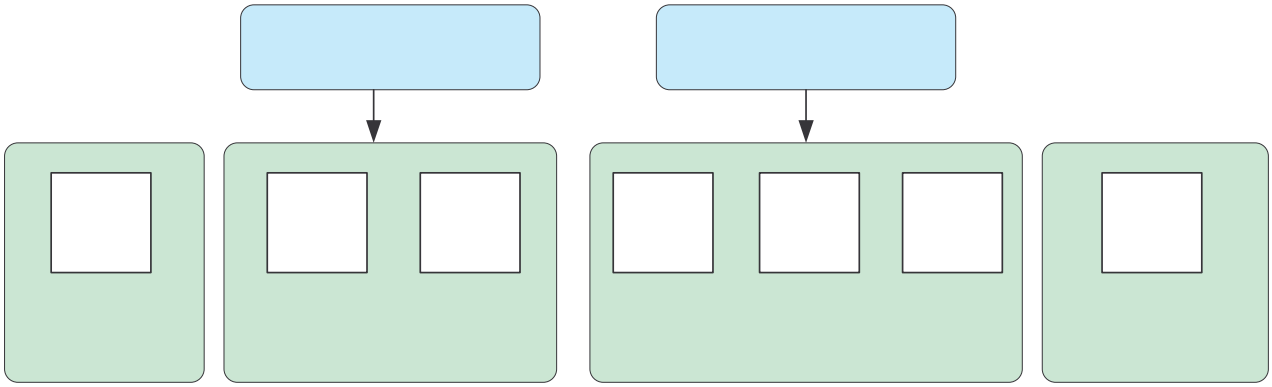

Рисунок 3 – Показатели защищенности СВТ

Защищенность СВТ есть потенциальная защищенность, то есть способность их предотвращать или существенно затруднять НСД к информации в дальнейшем при использовании СВТ в составе АС. [30]

Другим важным руководящим документом ФСТЭК России является «Защита от несанкционированного доступа к информации. Часть I. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Данный РД устанавливает классификацию программного обеспечения средств защиты информации по уровню контроля отсутствия в нем недекларированных возможностей (НДВ).

На рисунке 4 показано рекомендуемое соответствие степени конфиденциальности информации и уровня контроля отсутствия НДВ СВТ.

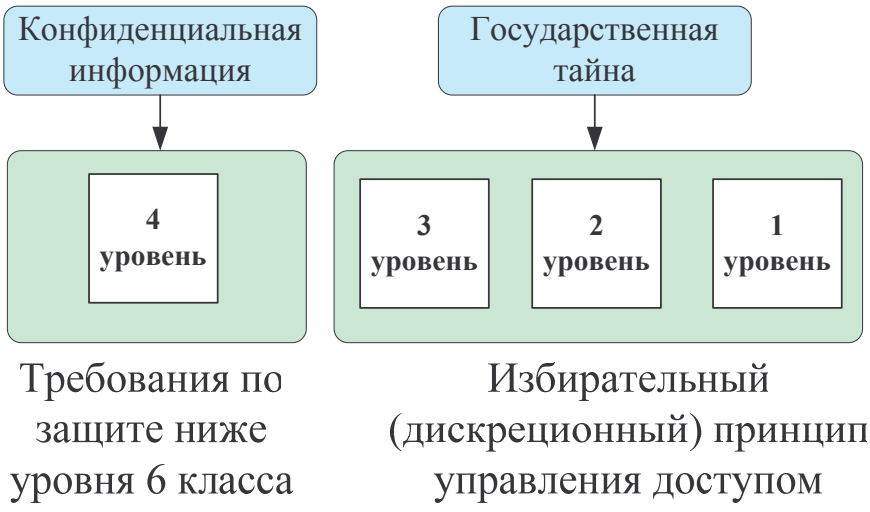

Рисунок 4 – Классификация СВТ по уровню контроля НДВ

Также следует отметить руководящий документ ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Данный РД устанавливает классификацию МЭ по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

На рисунке 5 показано соответствие степени конфиденциальности информации и классов защищенности МЭ от НСД.

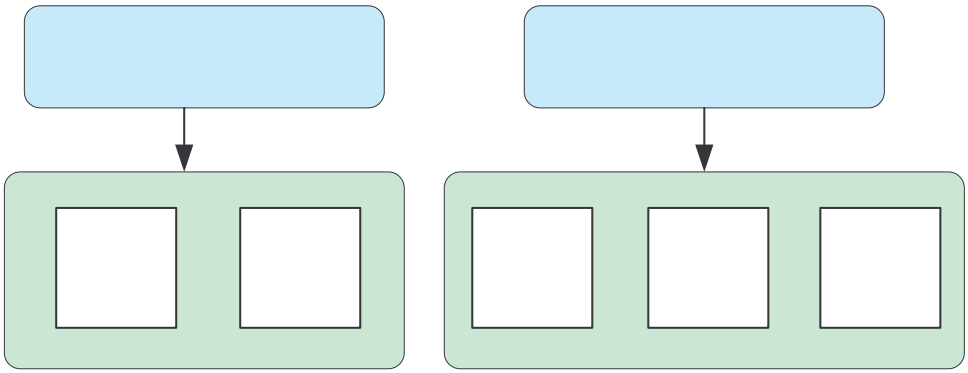

Рисунок 5 – Классификация МЭ по уровню защищенности от НСД

Аттестация объектов информатизации по требованиям безопасности

В Российской Федерации сложилась и достаточно эффективно действует система оценки соответствия АС требованиям безопасности информации. Основы деятельности этой системы определяются относящимися к сфере информации и информационной безопасности федеральными законами, указами Президента РФ, руководящими и методическими документами федеральных органов исполнительной власти.

Аттестация по требованиям безопасности информации предшествует началу обработки в АС подлежащей защите информации определяется необходимостью подтверждения эффективности комплекса используемых в АС и на конкретном объекте информатизации мер и средств защиты информации.

Обязательной аттестации в настоящее время подлежат АС, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектам, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер и может осуществляться по инициативе заказчика или владельца АС.

Аттестация предусматривает комплексную проверку АС в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

При аттестации АС подтверждается её соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействия на АС (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на неё за счет спе-

циальных устройств, встроенных в АС.

Подтверждение соответствия АС требованиям по безопасности информации оформляется документом «Аттестат соответствия АС требованиям безопасности информации» (далее – Аттестат соответствия). Наличие на объекте информатизации действующего Аттестата соответствия дает право обработки информации с определенным уровнем конфиденциальности и в указанный в данном документе период времени. [29]

Организационная структура оценки соответствия автоматизированных систем требованиям безопасности информации включает следующих участников:

- ФСТЭК России (федеральный орган исполнительной власти, уполномоченный организовывать работу по оценке соответствия АС требованиям безопасности информации);
- органы оценки соответствия АС требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики АС, оцениваемых по требованиям безопасности информации). [31]

В настоящее время аттестация информационных систем производится в соответствии с Руководящем документе ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Данный РД вводит в рассмотрение 9 классов защищенности АС, объединенных в три группы.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

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

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Данная группа также содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А. [5]

Основные признаки группировки в различные классы связаны с:

- наличием в АС информации различного уровня конфиденциальности;
- уровнем полномочий субъектов доступа АС на доступ к конфиденциальной информации (одинаковый или разный);
- режимом обработки данных в АС (коллективный или индивидуальный).

Для каждого класса сформулирован определенный набор требований для следующих подсистем: управление доступом, регистрация и учет, криптографической, обеспечения целостности.

Соответствие классов защищенности АС различным уровням обрабатываемой в АС информации приведено на рисунке 6.

При проведении аттестационных испытаний применяются следующие методы проверок и испытаний:

- экспертно – документальный метод предусматривает проверку соответствия объектов информатизации требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации требованиям режима обеспечения конфиденциальности, требованиям к размещению, монтажу и эксплуатации технических средств защиты;
- проверка комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного запуска средств защиты информации от НСД и наблюдение за их выполнением, а также попытки «взлома» системы защиты информации;
- инструментальный метод предусматривает оценку уровней защищенности от утечки информации по каналам ПЭМИН. [29]

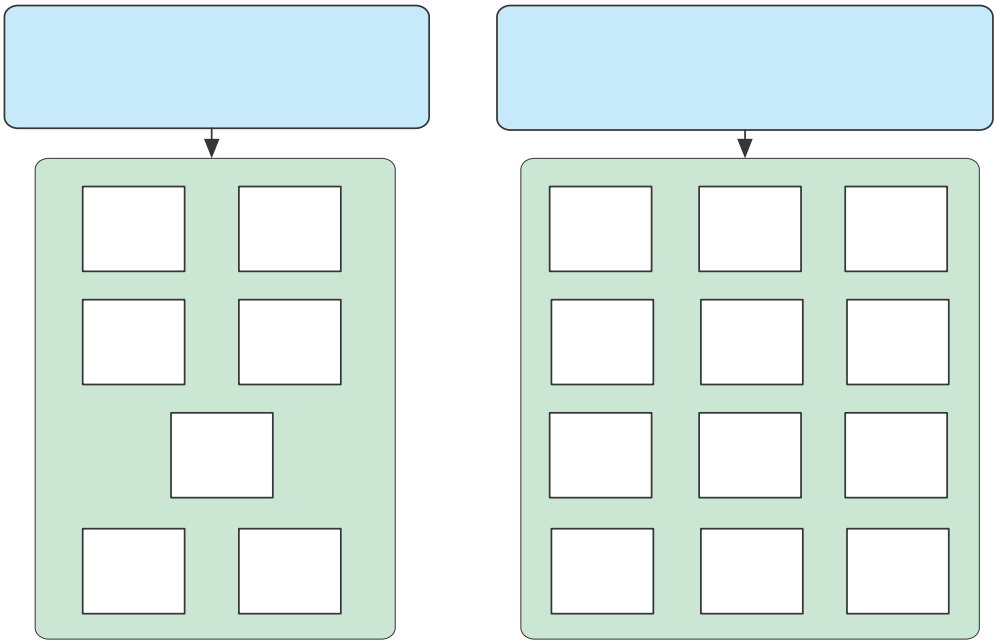

Рисунок 6 – Классы защищенности АС и категории информации ограниченного доступа

Проверка на соответствие организационно – техническим и режимным требованиям по защите информации включает в себя следующие этапы:

Проверка достаточности представленных документов, регламентирующих организацию и порядок проведения работ по защите сведений, составляющих государственную тайну на объектах, и соответствия их содержания требованиям безопасности и режима секретности проводимых работ.

Проверка соответствия состава и структуры программно – технических средств объектов информатизации.

Проверка правильности классификации АС проводится в соответствии с Руководящим документом Государственной Технической Комиссии (ФСТЭК) России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» на основании следующих определяющих признаков:

- степени секретности обрабатываемой в АС информации;
- уровни полномочий по доступу к секретной информации различных пользователей АС;
- режим обработки данных в АС – многопользовательский или однопользовательский.

Проверка правильности категорирования всех объектов вычислительной техники, входящих в состав объекта информатизации, проводится на основании следующих исходных данных:

- максимальной степени секретности информации, обрабатываемой на объектах информатизации;
- условий расположения объектов.

Проверка уровня подготовки кадров и распределения ответственности персонала производится на основе следующих показателей:

- экспертной оценки знания инструкций по обеспечению режима секретности и по безопасности информации пользователями;
- наличия разрешительной системы доступа персонала, определяющей полномочия доступа к охраняемой информации и процедуры их оформления, системы распределения ответственности персонала за выполнение режимных требований, требований по безопасности информации, оформленной приказами и распоряжениями руководителя организации.

Путем опроса персонала проверяется доведение до конкретных исполнителей руководящих документов, инструкций по обеспечению режима секретности, технологических инструкций, а также уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях.

Проверка наличия сертификатов соответствия на средства защиты информации, экспертиза протоколов по специальным исследованиям СВТ, предписаний на эксплуатацию СВТ.

Проверка выполнения режимных требований к помещениям, в которых проводится обработка информации.

Производится проверка выполнения требований по условиям размещения СВТ в рабочих помещениях, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

Проверка ведения учета, хранения и обращения секретных носителей информации.

Выводы по сравнению нормативных основ анализа защищенности

На основании изложенного были сделаны следующие выводы. Сложившаяся к началу 2000 года нормативная база оценки соответствия информационных систем требованиям безопасности информации имеет ряд недостатков, основными из которых являются:

- статичность и недостаточная корректность требований, слабый учет особен-

ностей АС и имеющихся угроз безопасности информации, недостаточная проработанность процедурных и методических аспектов оценки соответствия АС;

- преобладание технических мер по отношению к организационным и технологическим мерам обеспечения безопасности информационной системы;
- недостаточность развития критериальной базы оценки организационных и технологических мер обеспечения безопасности информации в информационной системе.

Всё это отрицательно сказывается на достоверности и повторяемости результатов оценки соответствия АС требованиям безопасности информации.

В качестве направлений совершенствования нормативной и методической базы системы оценки соответствия АС могут быть предложены следующие:

- развитие критериальной базы в направлении охвата всей совокупности организационных, технологических и технических мер обеспечения информационной безопасности;
- четкая структуризация и дифференциация требований в зависимости от категории АС, уровня ценности защищаемых активов, состава угроз и условий среды функционирования;
- совершенствование организационных и процедурных основ оценки соответствия АС в направлении четкой регламентации видов работ, выполняемых на различных этапах жизненного цикла, формализации состава и структуры разрабатываемых документов, порядка их актуализации с учетом динамики изменения АС и среды функционирования;
- развитие методов и форм проведения оценки соответствия АС в направлении выполнения работ, обеспечивающих объективность, достоверность и повторяемость результатов.

В связи с вышеизложенным, были сформированы основные принципы, на которых должна основываться оценка соответствия АС. К данным принципам относятся следующие:

- требования безопасности информации должны включать организационные, технические и эксплуатационные требования, устанавливаемые на основе анализа риска, определяемого исходя из ценности защищаемых активов и идентифицированных для АС угроз и уязвимостей;
- требования безопасности должны быть разработаны на основе стандартизованной структурированной базы точно определенных требований безопасности и представляться в установленной форме;
- методология формирования требований безопасности для различных уровней объектов (АС, изделий ИТ) должна быть тесно взаимосвязана в целях обеспечения их взаимного учета;
- оценка соответствия АС должна осуществляться в соответствии с четко определенными критериями и общей методологией, которые должны позволять проводить доказательную оценку выполнения установленных требований, обеспечивать объективность и повторяемость результатов, а также обеспечивать возможность учета результатов сертификации применяемых в АС изделий ИТ;

- процессы оценки соответствия должны состоять из четко определенных, взаимоувязанных этапов и работ, выполнение которых приводит к принятию обоснованного решения о соответствии (несоответствии) АС установленным для нее требованиям;
- поддержание безопасности АС должно обеспечиваться постоянным мониторингом и периодической переоценкой безопасности АС.

Критерии оценки соответствия АС требованиям безопасности информации должны представлять собой систематизированную совокупность требований безопасности информации и методологии оценки удовлетворения АС требованиям на основании результатов исследования материалов разработчика АС, документов эксплуатирующей организации и фактического материала, получаемого в ходе работ по непосредственной оценке соответствия АС.

Требования безопасности должны содержать две категории требований:

- функциональные требования безопасности АС;
- требования доверия к безопасности АС.

Первая группа требований, как уже отмечалось выше, предъявляются к тем функциональным возможностям мер и средств обеспечения безопасности АС, которые предназначены для обеспечения безопасности АС и определяют желательный безопасный режим функционирования АС.

Функциональные требования должны включать в себя следующие группы требовании:

- организационные требования безопасности АС;
- эксплуатационные требования безопасности АС;
- требования безопасности информационных технологий АС.

Требования доверия к безопасности АС предъявляются к действиям разработчика АС, документам (свидетельствам), представляемым для оценки, действиям по оценке соответствия АС и действиям эксплуатирующей организации.

Требования доверия к безопасности АС включают:

- требовании доверия к мерам и средствам обеспечения безопасности при разработке АС;
- требовании доверия к мерам и средствам обеспечения безопасности при эксплуатации АС;
- требовании доверия к безопасности информационных технологий АС.

Оценка соответствия АС требованиям безопасности информации должна проводиться на основе единой методологии оценки, предусматривающей конкретные виды действия оценщика по оценке соответствия АС требованиям безопасности информации.

Контрольные задания и вопросы

1. Поясните основные положения методологии оценки по ОК.
2. Поясните различия между защитой гостайны и коммерческой информации на примере межсетевых экранов, многопользовательских автоматизированных систем, однопользовательских автоматизированных систем.

3.3 Сопоставление требований стандартов

Сопоставление требований. Краткое обоснования сопоставления.

Сопоставление требований. Краткое обоснование сопоставления

Требования к средствам вычислительной техники и требования к объектам оценки могут быть сопоставлены для перехода к требованиям одного стандарта требованиям другого.

При обосновании сопоставления требований применяется следующее правило: обоснование требования, описанного однажды, не повторяется вновь, за исключением особых дополнений, связанных с логикой построения сопоставления.

1) Дискреционный принцип контроля доступа:
   1.1) осуществление контроля доступа наименованных субъектов к наименованным объектам:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО)
- ADV_FSP.2 (Полностью определенные внешние интерфейсы)
- AGD_ADM.1 (Руководство администратора)
- FDP_ACF.1 (Управление доступом, основанное на атрибутах безопасности)
- FDP_ACC.2 (Полное управление доступом).

Исходя из анализа общих элементов политики безопасности, целей безопасности (см. Приложение 4), предположений безопасности (Приложение 5), а также определения неформальной политики безопасности, был сделан вывод о том, что в принципе весь список требований, объединенных показателем защищенности – дискреционный принцип контроля доступа, можно закрыть требованием гарантированности ADV_SPM.1: Неформальная модель политики безопасности ОО с последующими уточнениями.

Таким образом, введение требования ADV_SPM.1: Неформальная модель политики безопасности ОО основано на следующем: неформальная модель ПБ – описание политик безопасности, осуществляемых услугами или функциями безопасности, доступными через внешний интерфейс. Например, политика управления доступом описывает защищаемые ресурсы и условия, которые должны быть обеспечены для предоставления доступа. Политика идентификации и аутентификации описывает, как идентифицируются пользователи, как аутентифицируется заявленная идентификационная информация, а также правила, влияющие на то, каким образом аутентифицируется идентификационная информация. Политика аудита описывает подвергаемые аудиту события ОО, идентифицируя, как те события, что выбираются администратором, так и те, которые всегда подвергаются аудиту.

Далее, требование ADV_FSP.2 было введено, так как считаю необходимым в данном случае наличие функциональной спецификации, которая должна содержать описание назначения и методов использования всех внешних интерфейсов КСБ, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

Также, процесс контроля доступа должен подвергаться администрированию и аудиту. В связи с этим было введено требование AGD_ADM.1: Руководство администратора. Руководство администратора должно содержать описание функций безопасности ОО, относящиеся к администрированию, а также описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

Управление доступом, основанное на атрибутах безопасности (FDP_ACF.1) позволяет КСБ осуществить доступ, основанный на атрибутах и именованных группах атрибутов безопасности. Применение функций разграничения доступа основывается на следующих атрибутах безопасности: идентификаторы субъектов доступа, идентификаторы объектов доступа, адреса субъектов доступа, адреса объектов доступа, права доступа субъектов. [16, с.91]

Полное управление доступом (FDP_ACC.2) содержит требование, чтобы каждая идентифицированная ПСБ управления доступом охватила все операции субъектов на объектах, управляемых этой ПСБ.

1.2) Явное задание санкционированных типов доступа для каждой пары субъект – объект:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО).
- AGD_ADM.1 (Руководство администратора).

1.3) Возможность санкционированного изменения правил разграничения доступа:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО).

1.4) Возможность санкционированного изменения списка пользователей СВТ:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО).

1.5) Возможность санкционированного изменения списка защищаемых объектов СВТ:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО).

1.6) Предоставление права реализовывать санкционированное изменение правил разграничения доступа только выделенным субъектам:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- FMT_MOF.1 (Управление режимом применения сервисов безопасности).

Управление – важнейший аспект информационной безопасности. Управление режимом применения сервисов безопасности (FMT_MOF.1) допускает роли уполномоченных пользователей к управлению режимом применения сервисов КСБ, использующих правила или условия, которые могут быть управляемы. Только администратору позволяется определять режим функционирования, отключения, подключения, модифицировать режимы идентификации и аутентификации, управлять права доступа, протоколирования и аудита.

1.7) Предоставление права реализовывать санкционированное изменение списка пользователей СВТ только выделенным субъектам:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- FMT_MOF.1 (Управление режимом применения сервисов безопасности).

2) Очистка памяти

2.1) Предотвращение доступа субъекта к остаточной информации при первоначальном назначении или при перераспределении внешней памяти:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- AGD_ADM.1 (Руководство администратора);
- FDP_RIP.2 (Полная защита остаточной информации).

Проект верхнего уровня (ADV_HLD.2: Безопасность в проекте верхнего уровня) должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, необходимые КСБ, с представлением сервисов, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

Непосредственно требование по защите остаточной информации определено с помощью требования FDP_RIP.2: Полная защита остаточной информации, согласно которому для всех объектов должна обеспечиваться полная защита остаточной информации, то есть недоступность предыдущего состояния при освобождении ресурса.

3) Идентификация и аутентификация:

3.1) Идентификация пользователя при запросе на доступ

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- FIA_UID.2 (Идентификация до любых действий пользователя).

Кроме вышеуказанных требований гарантированности, считаю, что для корректной реализации процедуры регистрации действий пользователей, процессы идентификации и аутентификации пользователей должны проводиться до совершения каких-либо действий. На основание чего и было введено функциональное требование FIA_UID.2: Идентификация до любых действий пользователя, говорящее о том, что каждый пользователь должен быть успешно идентифицирован и аутентифицирован до разрешения любого действия, выполняемого сервисом безопасности от его имени.

3.2) Осуществление аутентификации - проверка подлинности идентификации:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня).

3.3) Запрет доступа к защищаемым ресурсам при неуспешной аутентификации:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- FIA_AFL.1 (Обработка отказов аутентификации).

FIA_AFL.1: Обработка отказов аутентификации содержит требование, чтобы КСБ был способен завершить процесс открытия сеанса после определенного числа

неуспешных попыток аутентификации пользователя. При достижении определенного администратором числа неуспешных попыток аутентификации, необходимо отказать субъекту в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности.

4) Гарантии проектирования:

4.1) Построение модели защиты на начальном этапе проектирования СВТ

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ALC_DVS.1 (Идентификация мер безопасности).

Идентификация мер безопасности (ALC_DVS.1) необходима для определения достаточности применения мер и средств контроля безопасности для обеспечения конфиденциальности и целостности проекта и реализации ОО. Это необходимо для того, чтобы безопасная эксплуатация ОО не была скомпрометирована.

4.2) Модель защиты должна включать ПРД к объектам и непротиворечивые правила изменения ПРД

- ADV_SPM.1 (Неформальная модель политики безопасности ОО).

5) Регистрация:

В данной категории показателей защищенности, как и в п.1, доминирующим требованием является наличие неформальной политики безопасности, а именно политика аудита. Помимо того, что в неформальной политике безопасности должны быть указаны все события, подвергаемые регистрации (аудиту), а в руководстве администратора должны быть прописаны все параметры безопасности, контролируемых администратором, считаю необходимым дополнить данные требования гарантированности функциональными требованиями.

5.1) Регистрация использования идентификационного и аутентификационного механизма:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- FAU_GEN.1 (Генерация данных аудита);
- FAU_SEL.1 (Избирательный аудит).

Обязательному протоколированию подлежат запуск и завершение регистрационных функций, а также все события для базового уровня аудита. В каждой регистрационной записи должны присутствовать дата и время события, идентификатор субъекта и результат (успех или неудача) события (FAU_GEN.1: Генерация данных аудита).

Избирательность регистрации событий должна основываться хотя бы на минимально необходимом наборе атрибутов, состоящем из идентификатора объекта, идентификатора субъекта, адреса узла сети, типа события, даты и времени события.

5.2) Регистрация запроса на доступ к защищаемому ресурсу:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- FAU_GEN.1 (Генерация данных аудита);
- FAU_SEL.1 (Избирательный аудит).

5.3) Регистрация создания и уничтожения объекта:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);

- AGD_ADM.1 (Руководство администратора);
- FAU_GEN.1 (Генерация данных аудита);
- FAU_SEL.1 (Избирательный аудит).

5.4) Регистрация действий по изменению ПРД:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- FAU_GEN.1 (Генерация данных аудита).

5.5) Регистрация даты и время осуществления регистрируемого события:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- FAU_GEN.1 (Генерация данных аудита).

5.6) Регистрация субъекта, осуществившего регистрируемое действие:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- FAU_GEN.2 (Ассоциация идентификатора пользователя).

Требование FAU_GEN.2: Ассоциация идентификатора пользователя предполагает, что КСБ должен быть способен сопоставить каждое подлежащее аудиту событие с идентификатором пользователя, который был инициатором этого события.

5.7) Наличие в КСЗ средства выборочного ознакомления с регистрируемой информацией:

- FAU_SAR.3 (Выборочный просмотр аудита).

Функциональное требование FAU_SAR.3 предполагает, что средства просмотра аудита должны отбирать данные аудита на основе критериев просмотра. Причем, доступ ко всей регистрируемой информации имеет только администратор.

6) Целостность комплекса средств защиты (КСЗ):

6.1) Наличие средства периодического контроля за целостностью программной и информационной части КСЗ:

- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- FPT_TST.1 (Тестирование КСБ);
- FCS_COP.1 (Криптографические операции).

Контроль за целостностью программной и информационной части КСЗ, на мой взгляд, можно достичь путем выполнения требований FPT_TST.1: Тестирование КСБ и FCS_COP.1: Криптографические операции.

Для демонстрации правильности работы функций безопасности в процессе нормального функционирования и/или по запросу администратора при запуске периодически должен выполняться пакет программ самотестирования, а администратор верифицирует целостность данных и выполняемого кода функций безопасности (FPT_TST.1).

Целостность информационной части КСЗ должна контролироваться согласно требованиям стандартов и других нормативных документов (FCS_COP.1).

7) Тестирование

7.1) Тестирование перехвата явных и скрытых запросов:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.1 (Описательный проект верхнего уровня);

- AGD_ADM.1 (Руководство администратора);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой КСБ (ADV_HLD.1).

Разработчик должен протестировать КСБ и задокументировать результаты. Тестовая документация должна состоять из планов и описаний процедур тестирования, ожидаемых и фактических результатов тестирования (ATE_FUN.1).

Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде (AVA_VLA.2).

7.2) Тестирование правильного распознавания санкционированных запросов на доступ:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.1 (Описательный проект верхнего уровня);
- AGD_ADM.1 (Руководство администратора);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.3) Тестирование правильного распознавания несанкционированных запросов на доступ:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.1 (Описательный проект верхнего уровня);
- AGD_ADM.1 (Руководство администратора);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.4) Тестирование средств защиты механизма разграничения доступа:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.5) Тестирование санкционированного изменения правил разграничения доступа:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.1 (Описательный проект верхнего уровня);
- AGD_ADM.1 (Руководство администратора);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.6) Тестирование успешного осуществления идентификации и аутентификации:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.1 (Описательный проект верхнего уровня);

- AGD_ADM.1 (Руководство администратора);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.7) Тестирование средств защиты механизмов идентификации и аутентификации:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.8) Тестирование процесса очистки памяти в соответствии с требованием по очистке памяти:

- ATE_IND.2 (Выборочное независимое тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

Цель Выборочного тестирования (ATE_IND.2) – сделать заключение о соответствии спецификациям режим функционирования ОО, и повышение уверенности в результатах тестирования разработчиком путем выполнения выборки тестов разработчика

7.9) Тестирование регистрации событий, установленных для данного класса СВТ:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.10) Тестирование средств защиты регистрационной информации:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

7.11) Тестирование возможности санкционированного ознакомления с регистрационной информацией:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора);
- ATE_FUN.1 (Функциональное тестирование);
- AVA_VLA.2 (Независимый анализ уязвимостей).

8) Руководство пользователя:

8.1) Описание способов использования КСЗ и его интерфейса с пользователем:

- AGD_USR.1 (Руководство пользователя).

Руководство пользователя должно содержать описание сервисов и интерфейсов безопасности, доступных пользователям, а также инструкции и указания по безопасному использованию ОО

9) Руководство по комплексу средств защиты (КСЗ):

9.1) Описание контролируемых функций:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО);
- AGD_ADM.1 (Руководство администратора).

9.2) Руководство по генерации КСЗ:

- ADO_IGS.1 (Процедуры установки, генерации и запуска).

Требование гарантированности ADO_IGS.1: Процедуры установки, генерации и запуска обязывает разработчика задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

10) Тестовая документация:

10.1) Наличие описания производимых тестов и результатов тестирования в соответствии с требованиями тестирования:

- ATE_FUN.1 (Функциональное тестирование);
- ATE_COV.1 (Подтверждение покрытия).

Оценка покрытия показывает соответствие между тестами, идентифицированными в тестовой документации, и функциональной спецификации (ATE_COV.1).

11) Конструкторская (проектная) документация

11.1) Общее описание принципов работы СВТ

- ADV_HLD.1 (Описательный проект верхнего уровня);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня).

11.2) Общая схема комплекса средств защиты

- ADV_FSP.1 (Неформальная функциональная спецификация);
- ADV_LLD.1 (Описательный проект нижнего уровня);
- ADV_HLD.1 (Описательный проект верхнего уровня).

Общую схему комплекса средств защиты можно получить путем анализа неформальной функциональной спецификации, которая должна содержать неформальное описание КСБ и его внешних интерфейсов (ADV_FSP.1), проекта нижнего уровня, определяющего взаимосвязи между модулями в терминах, предоставляемых функциональных возможностей безопасности и зависимостей от других модулей (ADV_LLD.1) и проекта верхнего уровня.

11.3) Описание интерфейсов комплекса средств защиты с пользователем:

- AGD_USR.1 (Руководство пользователя).

11.4) Описание интерфейсов частей КСЗ между собой:

- ADV_LLD.1 (Описательный проект нижнего уровня);
- ADV_FSP.2 (Полностью определенные внешние интерфейсы);
- ADV_HLD.2 (Безопасность в проекте верхнего уровня).

11.5) Описание механизмов идентификации и аутентификации:

- ADV_FSP.1 (Неформальная функциональная спецификация).

11.6) Описание модели защиты:

- ADV_SPM.1 (Неформальная модель политики безопасности ОО)
- ADV_HLD.2 (Безопасность в проекте верхнего уровня).

11.7) Описание механизмов контроля целостности КСЗ:

- ADV_FSP.1 (Неформальная функциональная спецификация).

11.8) Описание механизмов очистки памяти

- ADV_FSP.1 (Неформальная функциональная спецификация).

Контрольные задания и вопросы

1. Поясните возможность существования аналогов в требованиях РД ГТК и ОК.
2. Назовите аналоги требований к тестовой документации, схеме комплекса средств защиты, тестированию, идентификации и аутентификации.
3. Найдите аналоги требований РД для 6-го класса СВТ в ОК.
4. Найдите аналоги требований РД для 5-го класса СВТ в ОК.
5. Поясните и обоснуйте причины выбора среди требований РД 5 и 6 класса СВТ.

4. АНАЛИЗ ОСТАТОЧНЫХ ИНФОРМАЦИОННЫХ РИСКОВ

4.1 Аудит безопасности

Общие сведения. Методика анализа рисков ГОСТ Р ИСО/МЭК 17799-2005. Процесс аудита информационной безопасности

Общие сведения

После установки систем защиты информации может возникнуть вопрос о достаточности принятых мер. В таком случае может применяться анализ остаточных информационных рисков по стандарту ГОСТ Р ИСО/МЭК 17799-2005, принятого в качестве российского на основе международного.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому вопрос, "как оценить уровень безопасности корпоративной информационной системы", - обязательно влечет за собой следующие: в соответствии с какими критериями производить оценку эффективности защиты, как оценивать и переоценивать информационные риски предприятия? Вследствие этого, в дополнение к требованиям, рекомендациям и руководящим документам Гостехкомисии России и ФСБ приходится адаптировать к нашим условиям и применять методики международных стандартов (ISO 17799, 9001, 15408, BSI и пр.). А также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности инвестиций в обеспечение безопасности и защиту информации.

Аудит безопасности в российских условиях имеет ряд специфических особенностей. В настоящее время существует три основных практических подхода к анализу и оценке текущего состояния информационной безопасности предприятия:

- на основе анализа требований к корпоративной системе информационной безопасности;
- на основе инструментальных проверок состояния информационной безопасности предприятия;
- на основе анализа информационных рисков предприятия. [32]

Первый подход обычно используется при определении так называемого базового уровня информационной безопасности предприятия, когда достаточно выработать и проверить их соблюдение на практике некоторых общих требований обеспечения информационной безопасности предприятия. Сегодня существует два основных способа определения названных требований: основанные на жестких априорных (действующие РД Гостехкомиссии) и на гибких адаптивных (международный стандарт ISO/IEC 15408:1999) требованиях. Более перспективным считается второй способ, что и подтверждается практикой выполнения подобных работ.

Второй подход, так называемый "активный аудит" используется, в основном, для выявления возможных уязвимостей технического уровня обеспечения информационной безопасности предприятия (пример методики "активного" аудита, автором

которой является Pete Herzog). Данный подход является, безусловно, необходимым, но явно не достаточным для проверки соответствия текущего уровня информационной безопасности предприятия поставленным целям. Дело в том, что в этом подходе уделяется мало внимания собственно корректности и адекватности организации обработки данных на предприятии, и особенно организационно-режимным средствам и мероприятиям, которые являются преимущественными по отношению к другим мерам и средствам защиты. В результате, например, при неправильном определении степени конфиденциальности защищаемой информации может оказаться неэффективным следование рекомендациям, полученным в ходе выполнения работ по активному аудиту сети предприятия. Другими словами, практика работ отчетливо показывает, что любая проверка эффективности системы защиты предприятия должна начинаться с проверки технологии обработки данных на предприятии, и контроля организационно-режимных мер и средств защиты. Цель этих мероприятий - выявление наиболее критичных зон обработки данных, нарушений действующих на данном предприятии инструкций по обеспечению режима, а также определение степени соответствия данных инструкций возложенным на них задачам.

Третий подход, основывающийся, как правило, на основе международного стандарта ISO 17799, используется для проведения полного анализа защищенности корпоративной сети и управления информационной безопасностью предприятия на основе специальных методов и инструментальных средств, построенных с использованием структурных методик системного анализа и проектирования (SSADM - Structured Systems Analysis and Design), например COBRA, CRAMM.

Методика анализа рисков ISO 17799

В последнее время в разных странах появилось новое поколение стандартов информационной безопасности компьютерных информационных систем, посвященных практическим вопросам обеспечения и аудита информационной безопасности. Это прежде всего международные и национальные стандарты оценки и управления информационной безопасностью ISO 15408, ISO 17799 (BS 7799), BSI; стандарты аудита информационных систем и информационной безопасности COBIT, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им.

В соответствие с этими стандартами обеспечение информационной безопасности в любой компании предполагает следующее. Во-первых, определение целей обеспечения информационной безопасности компьютерных систем. Во-вторых, создание эффективной системы управления информационной безопасностью. В третьих, расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям. В четвертых, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния. В пятых, использование методик (с обоснованной системой метрик и мер обеспечения информационной безопасности) проведения аудита информационной безопасности, позволяющих объективно оценить текущее состояние дел. [33]

Рассмотрим методику анализа рисков, предложенную Международным стандартом ISO/IEC 17799:2000 (BS 7799-1) "Управление информационной безопасно-

стью - Информационные технологии. - Information technology- Information security management".

Данный стандарт был разработан на основе первой части Британского стандарта BS 7799-1:1995 "Практические рекомендации по управлению информационной безопасностью - Information security management - Part 1: Code of practice for information security management" и относится к новому поколению стандартов информационной безопасности компьютерных информационных систем. Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности корпоративных информационных систем;
- управление доступом;
- требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании. [34]

Вторая часть стандарта BS 7799-2:2000 "Спецификации систем управления информационной безопасностью - Information security management - Part 2: Specification for information security management systems", определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Давайте рассмотрим основные положения методики проведения аудита и рекомендованные ее средства и методы оценки рисков Guide to BS 7799 risk assessment and risk management. - DISC, PD 3002, 1998, Guide to BS 7799 auditing. - DISC, PD 3004, 1998. Существенно, что эти рекомендации вполне применимы к отечественным условиям и могут быть использованы при разработке соответствующих методик. Особенно полезными представляются простейшие методы оценки и управления рисками, не требующие использования сложного и дорогостоящего программного обеспечения.

Каждая компания, решившая провести аудит информационной безопасности, в соответствии с требованиями стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) должна провести подготовительные мероприятия, подготовить документацию и систему управления информационной безопасностью.

Подготовительные мероприятия включают в себя подготовку нормативно-методической документации компании по организации информационной безопасности и проведение внутренней проверки соответствия системы обеспечения информационной безопасности компании требованиям стандарта ISO 17799.

Процесс аудита информационной безопасности

Процесс аудита информационной безопасности компании начинается с подготовки детальных и подробных планов проведения аудита. Планы должны быть представлены соответствующим лицам компании до начала процедуры аудита безопасности. При этом важно, чтобы аудиторы были ознакомлены с тем, каким законодательно-правовым нормам и требованиям отраслевых и ведомственных стандартов следует проверяемая организация или компания. Далее начинается проверка нормативно-методической документации компании, которая может проводиться как внутри компании, так и за ее пределами. Состав проверяемой документации может включать:

- концепцию и политику безопасности;
- описание рамок защищаемой системы (карту корпоративной системы, в том числе описание состава и структуры используемого в компании прикладного и системного программного обеспечения);
- должностные инструкции корпоративных пользователей;
- положения о департаменте информационной безопасности;
- описания методик оценки и управления информационными рисками;
- оценки состояния информационной безопасности компании, правил и норм эксплуатации программно-технических средств обеспечения информационной безопасности и пр.

Если компания уже проходила процедуру аудита, то также представляется отчет о предыдущей проверке и данные о всех выявленных ранее несоответствиях. Кроме того, должна быть подготовлена так называемая Ведомость соответствия - документ, в котором оценивается соответствие поставленных целей и средств управления информационной безопасностью требованиям стандарта.

Сущность аудита безопасности на соответствие системы управления информационной безопасностью компании требованиям стандарта заключается в проверке выполнения каждого положения стандарта ISO 17799. По каждому такому положению проверяющие должны ответить на два вопроса: выполняется ли данное требование, и если нет, то каковы причины невыполнения? На основе ответов составляется Ведомость соответствия, основная цель которой - аргументированное обоснование имеющихся отклонений информационной безопасности от требований стандарта ISO 17799. По завершению аудита безопасности выявленные несоответствия при необходимости могут быть устранены. Другими словами, в ходе выполнения аудита всей компании в целом, аудитор, выполняющий данную работу, должен собрать доказательства того, что компания отвечает всем требованиям стандарта ISO 17799. Это делается на основе анализа документов, бесед с экспертами, а при необходимо-

сти и проведения соответствующих организационных проверок режима безопасности и инструментальных проверок компонентов корпоративной системы.

В общем плане возможны два варианта аудита информационной безопасности: аудит компании в целом и аудит только информационной системы (в этом случае могут быть использованы также рекомендации международного стандарта ISO 15408). В первом случае компания должна подготовить для проверки:

- документы, подтверждающие внедрение в организации выработанной политики информационной безопасности и, в частности, наличие документированного подхода к оцениванию и управлению рисками в рамках всей компании;
- описание организационной инфраструктуры информационной безопасности на местах - распределение обязанностей сотрудников по обеспечению безопасности;
- обоснование выбора средств защиты для рассматриваемой системы;
- документацию на процессы обслуживания и администрирования информационной системы;
- документацию с описанием подходов к оцениванию и управлению рисками;
- документацию по подготовке периодических проверок по оцениванию и управлению рисками;
- описание процедуры принятия уровня остаточного риска, с документированным выводом о реализации необходимых средств обеспечения информационной безопасности, степени их тестирования и корректности использования;
- документацию по системе управления информационной безопасностью и реестр средств управления безопасностью в документе "Ведомость соответствия";
- результаты оценивания рисков по информационной системе;
- описание контрмер для противодействия выявленным рискам. [35]

Все перечисленные проверки выполняются с использованием принятых в компании подходов к оценке и управлению рисками.

В случае аудита только информационной системы компания должна подготовить для проверки:

- описание политики информационной безопасности, документацию по системе управления информационной безопасностью и документ "Ведомость соответствия", отражающий реальное состояние оцениваемой системы;
- документацию по проведенному оцениванию рисков;
- документацию по средствам управления информационной безопасностью;
- доказательства эффективности принятых контрмер и результаты их тестирования. [35]

Кроме того, при аудите только информационной системы аудитор должен подтвердить документированность вопросов, рассматриваемых в ходе проведения периодических проверок системы управления информационной безопасностью, а также корректность оценки рисков, выполненных посторонними или рекомендуемыми стандартом методами. Он должен заверить достоверность результатов оценки, подтвердить, что результаты оценивания рисков достоверны, приемлемы и документированы должным образом. Познакомившись со средствами обеспечения ин-

формационной безопасности, аудитор должен подтвердить, что необходимые средства обеспечения информационной безопасности были установлены корректно, прошли тестирование и правильно используются, а сотрудники знакомы с политикой информационной безопасности и система управления информационной безопасностью должным образом документирована и подготовлен документ "Ведомость соответствия". В заключении проводящий аудит сотрудник должен стандартным образом оформить заключение.

В процессе аудита подсистемы информационной безопасности компании на соответствие стандарту ISO/IEC 17799:2000 (BS 7799-1:2000) аудиторы должны проанализировать наиболее важные аспекты информационной безопасности с учетом объема подлежащей защите проверяемой информации, ее специфики и ценности для проверяемой компании. Поскольку подобная деятельность аудитора в настоящее время с большим трудом поддается формальному описанию, требует значительных знаний системного анализа и опыта аналогичной практической работы, опыт и компетентность аудитора являются существенными факторами качественно проведенного аудита безопасности корпоративной системы. [32]

В результате проведения аудита создается список замечаний, выявленных несоответствий требованиям стандарта и рекомендаций по их исправлению. При этом аудиторы должны гарантировать выполнения всех требований процедуры аудита. Поскольку и аудиторам, и проверяемой компании необходимо знать, насколько серьезны обнаруженные недостатки и каковы способы их исправления, то в стандарте определяются и используются две категории несоответствия.

Существенное несоответствие: не выполняется одно или несколько базовых требований стандарта ISO 17799 или установлено использование неадекватных мер по обеспечению конфиденциальности, целостности или доступности критически важной информации компании, приводящих к недопустимому информационному риску.

Несущественное несоответствие: не выполняются некоторые второстепенные требования, что несколько повышает информационные риски компании или снижает эффективность мер обеспечения информационной безопасности компании.

Каждое выявленное несоответствие обязательно должно иметь ссылку на соответствующее требование стандарта ISO 17799. При выявлении в процессе проверки значительного числа несущественных несоответствий аудитор обязан исследовать возможность возникновения существенного несоответствия. После выявления несоответствий аудитор и представители компании обязаны наметить пути их устранения. По результатам проверки аудитор может сформулировать в отчетных документах замечание, если он допускает возможность усовершенствования подсистемы информационной безопасности компьютерной информационной системы. Реакция компании на замечания аудитора может быть различной, поскольку компании сами в добровольном порядке определяют свои действия по их устранению. Замечания фиксируются и при последующих проверках. Аудиторы обязаны выяснить действия компании по их устранению. [34]

Контрольные задания и вопросы

1. Кратко опишите стандарт ГОСТ Р ИСО/МЭК 17799-2005 (ISO 17799:2000).
2. Назовите основные требования, предъявляемые стандартом ГОСТ Р ИСО/МЭК 17799-2005 к системе обеспечения информационной безопасности.
3. Поясните понятие «анализ остаточных информационных рисков». Как оно связано с анализом защищенности автоматизированных систем?
4. Опишите процесс аудита информационной безопасности.

ЗАДАНИЯ ДЛЯ САМОПОДГОТОВКИ

Задачи

1. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля доступа на базе СЗИ «Secret Net 5.0», предназначенную для защиты коммерческой тайны в однопользовательском режиме.
2. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля доступа на базе СЗИ «Secret Net 2000», предназначенную для защиты коммерческой тайны в компьютерной сети с разграничением прав доступа.
3. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля доступа на базе СЗИ «Страж 2.5», предназначенную для защиты коммерческой тайны в однопользовательском режиме.
4. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля информационных потоков на базе СЗИ «Застава», предназначенную для защиты государственной тайны в компьютерной сети в многопользовательском режиме.
5. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля информационных потоков на базе СЗИ «VipNET», предназначенную для защиты коммерческой тайны в компьютерной сети с разграничением прав доступа.
6. Проведите процедуру базового анализа остаточных информационных рисков согласно ГОСТ Р ИСО/МЭК 17799-2005 для системы защиты информации компьютерной сети
7. Проведите процедуру базового анализа остаточных информационных рисков согласно ГОСТ Р ИСО/МЭК 17799-2005 для системы защиты информации электронного документооборота
8. Проведите процедуру базового анализа остаточных информационных рисков согласно ГОСТ Р ИСО/МЭК 17799-2005 для системы защиты информации электронного архива

ЗАКЛЮЧЕНИЕ

Анализ защищенности автоматизированных систем – необходимый элемент комплексного обеспечения информационной безопасности. При использовании в организации информации, составляющей коммерческую тайну, такой метод повышения стойкости защиты становится экономически оправданным. Разные виды конфиденциальной информации, в том числе и государственная тайна Российской Федерации, также требуют применения процедур анализа защищенности автоматизированных систем.

Именно поэтому изучение основ анализа защищенности и нормативно-правовой базы в предметной области в курсе «Аттестация автоматизированных систем» является частью общей программы подготовки специалистов по специальностям 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 «Информационная безопасность телекоммуникационных систем».

В пособии раскрыты основные понятия, методы и нормативно-правовые основы анализа защищенности автоматизированных систем, за исключением составляющих государственную тайну Российской Федерации, порядок решения различных задач в предметной области.

В процессе работы над пособием были по возможности учтены последние изменения в законодательстве, но, принимая во внимание его постоянное совершенствование, планируется издание соответствующих дополнений.

В самостоятельные разделы пособия выделены основы анализа защищенности как процесса оценки автоматизированных систем, проанализированы требования и рекомендации руководящих документов, стандартов и законодательства, приведен справочный материал по вопросам аттестации автоматизированных систем, аккредитации и функционирования испытательных лабораторий.

Настоящее учебное пособие призвано помочь будущим специалистам понять основы своей профессии, подготовить их к профессиональной работе в службах обеспечения информационной безопасности государственных предприятий и коммерческих организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Положение о лицензировании деятельности по технической защите конфиденциальной информации от 15 августа 2006 г. N504. [Электронный ресурс]. - Режим доступа: http://www.infosecurity.ru/gazeta/content/060901/article01.shtml
2. ГОСТ Р 50922-96. Защита информации. Основные термины и определения [Текст]. – Введ. 10.07.96. М.: Издательство стандартов, 1996. – 12 с.
3. Астахов А. Анализ защищенности корпоративных автоматизированных систем [Текст] // Jet Info Информационный бюллетень. – 2002. – № 7. – 23 с.
4. Трубачев А. П. Оценка безопасности информационных технологий [Текст] / Трубачев А. П., Долинин М. Ю., Кобзарь М. Т., Сидак А. А., Сороковиков В. И. / под общ. ред. Галатенко В. А. – М.: Издательство СИП РИА, 2001. – 356 с.
5. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: утв. решением ГТК при Президенте Российской Федерации от 30 марта 1992. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_docs/doc_3_3_004.htm.
6. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: утв. решением ГТК при Президенте Российской Федерации от 30 марта 1992. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_docs/doc_3_3_003.htm.
7. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: утв. решением ГТК при Президенте Российской Федерации от 25 июля 1997. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_docs/doc_3_3_006.htm.
8. Руководящий документ. Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов: утв. решением Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_docs/doc_3_3_007.htm.
9. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия НДВ: утв. решением Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_docs/doc_3_3_010.htm.
10. Руководящий документ. Концепция защиты средства вычислительной техники и автоматизированные системы от несанкционированного доступа к информации: утв. решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992. [Электронный ресурс]. - Режим доступа: http//www.fstec.ru/_docs/doc_3_3_001.htm.

11. Общие критерии оценки безопасности информационных технологий [Текст]: учебное пособие / под ред. М.Т. Кобзаря, А.А. Сидака. – М: ЦБИ, 2004. – 81 с.
12. Галатенко В.А. Стандарты информационной безопасности [Текст]. М.: ИТУИТ.РУ «Интернет – университет Информационных технологий», 2004. – 328 с.
13. Савельев М. Станут ли общими общие критерии. [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/?ID=602972.
14. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности [Текст]. – Введ. 01.01.2004. М.: Издательство стандартов, 2004. – 176 с.
15. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 «Введение и общая модель [Текст]. – Введ. 01.01.2004. М.: Издательство стандартов, 2004. – 47 с.
16. Трубачев А.П. Формирование требований безопасности автоматизированных систем [Текст] // Защита информации. INSIDE. – 2006. - №7. – С. 64 – 67.
17. Кобзарь М.Т. Общие критерии – основа новой нормативной базы оценки безопасности информационных технологий [Текст] // Защита информации. INSIDE. – 2006. - №3. – С. 38 – 43.
18. Петренко С.А. Развитие нормативной базы по технической защите конфиденциальной информации [Текст] // Защита информации. INSIDE. – 2005. - №4. – С. 28 – 40.
19. Скородумов Б. Стандарты информационной безопасности. [Электронный ресурс]. - Режим доступа: http://www.bre.ru/security/10808.html.
20. Руководящий документ. Безопасность информационных технологий - Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель: утв. приказом ГТК при Президенте Российской Федерации от 19 июня 2002. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_razd/_ispo.htm.
21. Кобзарь М.Т. Методология оценки безопасности информационных технологий по Общим критериям [Текст] // Защита информации. INSIDE. – 2005. - №4. – С. 54 – 63.
22. Калайда И.А. Развитие нормативной базы в области безопасности информационных технологий. Ближайшая перспектива [Текст] // Защита информации. INSIDE. – 2005. - №4. – С. 41 – 45.
23. Долинин М.Ю. Комментарии к Российскому стандарту ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий»/Долинин М.Ю., Кобзарь М.Т., Сидак А.А. и др. М.: ФГУП «ЦНИИАТОМИНФОРМ», 2003. – 38 с.
24. Сидак А.А. Особенности сертификации продуктов и ИТ – систем на основе Общих критериев [Текст] // Защита информации. INSIDE. – 2006. - №7. – С. 51 – 54.

25. Сидак А.А. Стандартизация безопасности ИТ. [Электронный ресурс]. – Режим доступа: http://www.iitrust.ru/articles/st_bezop.htm.
26. Руководящий документ. Безопасность информационных технологий – Общая модель оценки безопасности информационных технологий. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_razd/_info.htm.
27. Положение о сертификации средств защиты информации по требованиям безопасности информации: утв. приказом председателя ГТК при Президенте РФ от 27 октября 1995. [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/_docs/doc_2_2_011.htm.
28. Домарев В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – К.: ООО «ТИД «ДС», 2004. – 992с.
29. Астахов А. Общее описание процедуры аттестации автоматизированных систем по требованиям информационной безопасности. [Электронный ресурс]. – Режим доступа: http://www.jetinfo.ru/2000/11/1/article1.11.2000.html.
30. Панасенко Е. Законодательство и регулирование отрасли информационной безопасности. [Электронный ресурс]. – Режим доступа: http://www.directum-journal.ru/print.aspx?ContentID=1743433.
31. Положение по аттестации объектов информатизации по требованиям безопасности информации Гостехкоммисии РФ: утв. решением ГТК при Президенте РФ от 25 ноября 1994. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_docs/doc_2_2_012.htm.
32. Симонов С.В. Методология анализа рисков в информационных системах. [Текст]. // Конфидент. Защита информации. - №1. – 2001. – С. 72-76
33. Мишель М. Управление информационными рисками // Финансовый директор – 2003. - № 9 (сентябрь). [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/20718.html
34. Симонов С.В. Технологии и инструментарий для управления рисками. [Текст]. // Jet Info. - №1. – 2003
35. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты. [Текст]. // Конфидент. Защита информации. - №2. – 2001. – С.48-53

СПИСОК ИСПОЛЬЗУЕМЫХ ТЕРМИНОВ

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Активы – информация или ресурсы, которые должны быть защищены средствами объекта оценки.

Атрибут безопасности – информация, связанная с субъектами, пользователями и/или объектами, которая используется для реализации ПБО.

Аттестация объектов информатизации – комплекс организационно – технических мероприятий, в результате которых посредствам специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям государственных стандартов или иных нормативно – технических документов по безопасности информации, утвержденных уполномоченными федеральными органами исполнительной власти.

Аутентификационные данные – данные, используемые для подтверждения подлинности пользователя.

Базовая стойкость сервиса безопасности (ССБ) – уровень стойкости сервиса безопасности ОО, на котором в соответствии с результатами анализа обеспечивается адекватная защита от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.

Внешний интерфейс – видимый для пользователя.

Высокая стойкость сервиса безопасности (ССБ) – уровень стойкости сервиса безопасности ОО, на котором в соответствии с результатами анализа обеспечивается адекватная защита от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

Гарантированность – основание для уверенности в том, что объект соответствует заданным целям безопасности.

Доверие – основание для уверенности в том, что объект оценки отвечает своим целям безопасности.

Задание по безопасности – совокупность требований безопасности и спецификаций, которую необходимо использовать в качестве основы для оценки конкретного ОО.

Знак соответствия – зарегистрированный в установленном порядке знак, которым по правилам, установленным в данной системе сертификации, подтверждается соответствие маркированной им продукции установленным требованиям.

Идентификатор – представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть полное или сокращенное имя этого пользователя или его псевдоним.

Изделие ИТ – обобщенный термин для продуктов и систем ИТ.

Интерфейс комплекса сервисов безопасности ОО – совокупность интерфейсов, как интерактивных (человеко-машинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО под контролем КСБ, или получение от КСБ какой-либо информации.

Информационная технология (ИТ) – приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации.

Итерация – более чем однократное использование компонента при различном выполнении операций.

Класс – совокупность семейств, объединенных общим назначением.

Комплекс сервисов безопасности ОО – совокупность всех аппаратных, программных и программно-аппаратных средств ОО, обеспечивающих адекватную реализацию ПБО.

Компонент – наименьшая совокупность элементов, которая может быть выбрана для включения в ПЗ, ЗБ или пакет.

Межсетевой экран (МЭ) – локальное (однокомпонентное) или функционально распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и / или выходящей из АС. Защита АС обеспечивается посредствам фильтрации информации, то есть её анализа по совокупности критериев и принятия решения о её распространении в (из) АС.

Модель политики безопасности ОО – структурированное представление политики безопасности, которая должна быть реализована ОО.

Недекларированные возможности (НДВ) – функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и целостности обрабатываемой информации.

Неформальный (Informal) – выраженный на естественном языке.

Область действия КСБ – совокупность возможных взаимодействий с ОО или внутри него, которые подчинены правилам ПБО.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Объект оценки – подлежащие оценке продукт ИТ или система с руководствами администратора и пользователя.

Орган оценки – организация, которая посредством системы оценки осуществляет применение ОК для определенной сферы, устанавливает стандарты и контролирует качество оценок, проводимых в данной сфере другими организациями.

Оценка – установление соответствия ПЗ, ЗБ или ОО определенным критериям.

Пакет – неоднократно используемая совокупность функциональных компонентов или компонентов гарантированности (например, УГО), объединенных для достижения определенных целей безопасности.

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

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение активов внутри ОО.

Предположения – условия, которые должны быть обеспечены в среде, чтобы ИТ или АС в целом могли рассматриваться как безопасные.

Продукт ИТ – совокупность программных , программно – аппаратных и (или) аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ и АС.

Профиль защиты – не зависящая от реализации (не связанная с реализацией) совокупность требований безопасности для некоторой категории ОО, отвечающей специфическим потребностям потребителя.

Расширение – добавление в ЗБ или ПЗ функциональных требований, не содержащихся в части 2, и/или требований гарантированности, не содержащихся в части 3 ОК.

Роль – заранее определенная совокупность правил, устанавливающих допустимые взаимодействия между пользователем и ОО.

Семейство – совокупность компонентов, объединенных одинаковыми целями безопасности, но отличающихся акцентами или строгостью.

Сервис безопасности – часть или части ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

Сертификат соответствия – документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Сертификация СЗИ по требованиям БИ - комплекс организационно – технических мероприятий, в результате которых посредствам специального документа – сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует требованиям государственных стандартов или иных нормативных документов по защите информации.

Система – конкретная реализация ИТ с определенными назначением и условиями эксплуатации.

Система оценки – организационно - правовая структура, в рамках которой осуществляется применение ОК в определенной сфере.

Средства защиты информации (СЗИ) – технические, криптографические, программные и другие средства, предназначенные для защиты сведений конфиденциального характера, а также средства контроля эффективности защиты информации.

Стойкость сервиса безопасности (ССБ) – характеристика сервиса безопасности ОО, выражающая минимально необходимые воздействия непосредственно на его механизмы безопасности, в результате которых нарушается выполнение этого сервиса.

Субъект – сущность, находящаяся в ОДК, которая инициирует выполнение операций.

Угроза – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба функционированию АС, защищаемых активам или отдельным лицам.

Уполномоченный пользователь – пользователь, которому в соответствии с ПБО разрешено выполнять определенные действия.

Уровень гарантированности оценки (УГО) – пакет компонентов гарантированности из части 3 ОК, соответствующий определенному положению на заданной ОК шкале гарантированности.

Усиление – добавление одного или нескольких компонентов гарантированности из части 3 в УГО или пакет гарантированности.

Уязвимость – недостаток актива или группы активов, автоматизированной системы или среды функционирования, который может использоваться одной или несколькими угрозами.

Формальный – выраженный на языке с ограниченным синтаксисом и заданной семантикой, основанной на строго определенных математических концепциях.

Функциональная спецификация – описание на верхнем уровне видимого пользователем интерфейса и режима функционирования КСБ, представляет собой отражение функциональных требований безопасности ОО.

Цель безопасности – сформулированное намерение противостоять идентифицированным угрозам и/или удовлетворять идентифицированной политике безопасности организации и предположениям.

Элемент – неделимое требование безопасности.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС	Автоматизированная система
ЗБ	Задание по безопасности
ИТ	Информационная технология
КСБ	Комплекс сервисов безопасности ОО
МЭ	Межсетевой экран
НДВ	Недекларированные возможности
ОК	Общие критерии (исторически сложившееся название, часто используемое для стандарта ГОСТ Р ИСО/МЭК 15408-2002 вместо его официального названия "Критерии оценки безопасности информационных технологий")
ОО	Объект оценки
ОМО	Общая методология оценки
ПБ	Политика безопасности
ПЗ	Профиль защиты
ПСБ	Политика сервиса безопасности
РД	Руководящий документ
СБ	Сервис безопасности
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СП	Сообщение о проблемах
ТОО	Технический отчет об оценке
УГО	Уровень гарантированности оценки
ФСТЭК	Федеральная служба по техническому и экспортному контролю

ПРИЛОЖЕНИЯ

Приложение 1

Положение по аттестации объектов информатизации по требованиям безопасности информации (без приложений)

Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Государственной технической комиссии при Президенте РФ Ю.Яшиным " 25 " ноября 1994 г

Содержание:

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

1.2. Положение разработано в соответствии с законами Российской Федерации “О сертификации продукции и услуг” и "О государственной тайне", "Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", "Положением о государственном лицензировании деятельности в области защиты информации", "Положением о сертификации средств защиты информации по требованиям безопасности информации", "Системой сертификации ГОСТ Р".

1.3. Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации (далее - федеральный орган по сертификации и аттестации), которым является Гостехкомиссия России.

1.4. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что

объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

1.5. Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.
В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

1.6. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

1.7. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер средств защиты требуемому уровню безопасности информации.
1.8. Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

1.9. Органы по аттестации аккредитуются Гостехкомиссией России. Правила аккредитации определяются действующим в системе "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Гостехкомиссия России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти.

1.10. Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители. Оплата работ по обязательной аттестации производится в соответствии с договором по утвержденным расценкам, а при их отсутствии - по договорной цене в порядке, установленном Гостехкомиссией России по согласованию с Министерством финансов Российской Федерации.

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители за счет финансовых средств, выделенных на разработку (доработку) и введение в действие защищаемого объекта информатизации.

1.11. Органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

2. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СИСТЕМЫ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1. Организационную структуру системы аттестации объектов информатизации образуют:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - Гостехкомиссия России;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции, по требованиям безопасности информации;

- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

2.2. Федеральный орган по сертификации и аттестации осуществляет следующие функции:

- организует обязательную аттестацию объектов информатизации;
- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;
- рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;
- организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

2.3. Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации.

Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

2.4. Органы по аттестации:

- аттестуют объекты информатизации и выдают "Аттестаты соответствия";
- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;
- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";
- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;
- ведут информационную базу аттестованных этим органом объектов информатизации;
- осуществляют взаимодействие с Гостехкомиссией России и ежеквартально информируют его о своей деятельности в области аттестации.

2.5. Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с "Положением о сертификации средств защиты информации по требованиям безопасности информации".

2.6. Заявители:

- проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;
- привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;
- предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;
- привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;
- осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";
- извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");
- предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

3. ПОРЯДОК ПРОВЕДЕНИЯ АТТЕСТАЦИИ И КОНТРОЛЯ

3.1. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработка программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрация и выдача "Аттестата соответствия";

- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
- рассмотрение апелляций.

3.2. Подача и рассмотрение заявки на аттестацию.

3.2.1. Заявитель для получения "Аттестата соответствия" заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации по форме, приведенной в Приложении 1.

3.2.2. Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

3.3. Предварительное ознакомление с аттестуемым объектом. При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.

3.4. Испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте информатизации.

3.4.1. При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

3.4.2. Испытания отдельных несертифицированных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации проводятся до аттестационных испытаний объектов информатизации. В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения органов по сертификации средств защиты информации по требованиям безопасности информации и сертификаты.

3.5. Разработка программы и методики аттестационных испытаний.

3.5.1. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по

сертификации средств защиты информации по требованиям безопасности информации.

3.5.2. Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

3.5.3. Программа аттестационных испытаний согласовывается с заявителем.

3.6. Заключение договоров на аттестацию.

3.6.1. Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по аттестации с привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

3.6.2. Оплата работы членов аттестационной комиссии производится органом по аттестации в соответствии с заключенными трудовыми договорами (контрактами) за счет финансовых средств от заключаемых договоров на аттестацию объектов информатизации.

3.7. Проведение аттестационных испытаний объектов информатизации.

3.7.1. На этапе аттестационных испытаний объекта информатизации:

- осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
- определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
- проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
- проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
- проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
- оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатиза-

ции в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

3.7.2. Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи "Аттестата соответствия" и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

3.8. Оформление, регистрация и выдача "Аттестата соответствия".
3.8.1. "Аттестат соответствия" на объект информатизации, отвечающий требованиям по безопасности информации, выдается органом по аттестации по форме, приведенной в Приложении 2.

3.8.2. "Аттестат соответствия" оформляется и выдается заявителю после утверждения заключения по результатам аттестации.

3.8.3. Регистрация "Аттестатов соответствия" осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору.

Ведение сводных информационных баз аттестованных объектов информатизации осуществляется Гостехкомиссией России или по ее поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов.

3.8.4. "Аттестат соответствия" выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристик, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более, чем на 3 года.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

3.8.5. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости

проведения дополнительной проверки эффективности системы защиты объекта информатизации.

3.8.6. при несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче "Аттестата соответствия", при этом может быть предложен срок повторной аттестации при условии устранения недостатков.

При наличии замечаний непринципиального характера "Аттестат соответствия" может быть выдан после проверки устранения этих замечаний.

3.9. Рассмотрение апелляций.

В случае несогласия заявителя с отказом в выдаче "Аттестата соответствия" он имеет право обратиться в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

3.10. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации.

3.10.1. Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации проводится Гостехкомиссией России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации - периодически в соответствии с планами работы по контролю и надзору.

Гостехкомиссия России может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органам по аттестации.

3.10.2. Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

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

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

3.10.5. При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и надзор, может быть приостановлено или аннулировано действие "Аттестата соответствия", с оформлением этого решения в "Аттестате соответствия" и информированием органа, ведущего сводную информационную базу аттестованных объектов информатики, и Гостехкомиссии России. Решение об аннулировании действия "Аттестата соответствия" принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

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

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

4. ТРЕБОВАНИЯ К НОРМАТИВНЫМ И МЕТОДИЧЕСКИМ ДОКУМЕНТАМ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

4.1. Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России.

4.2. Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

4.3. В нормативную документацию включаются только те показатели, характеристики, требования, которые могут быть объективно проверены.

4.4. В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

4.5. Тексты нормативных и методических документов, используемых при аттестации объектов информатизации, должны быть сформулированы

ясно и четко, обеспечивая их точное и единообразное толкование. В них должно содержаться указание о возможности использования документа для аттестации определенных типов объектов информатизации по требованиям безопасности информации или направлений защиты информации.

4.6. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

Приложение 2

Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (приводится без приложений)

Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Государственной технической комиссии при Президенте РФ Ю.Яшиным " 25 " ноября 1994 г

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает основные принципы аккредитации юридических лиц - предприятий, организаций и учреждений (далее предприятий) в качестве испытательных лабораторий и органов по сертификации средств защиты информации в системе сертификации средств защиты информации по требованиям безопасности информации.

1.2. Положение разработано в соответствии с Законом Российской Федерации "О сертификации продукции и услуг", Постановлением Правительства Российской Федерации "О сертификации средств защиты информации", на основании "Системы сертификации ГОСТ Р" , "Правил по проведению сертификации в Российской Федерации", "Положения о сертификации средств защиты информации по требованиям безопасности информации", "Положения о государственном лицензировании деятельности в области защиты информации".

1.3. Аккредитация предприятия в качестве органа по сертификации средств защиты информации по требованиям безопасности информации (далее - орган по сертификации) является официальным признанием его технической компетентности и независимости от разработчиков, изготовителей (поставщиков) и заказчиков (потребителей) испытываемых средств защиты информации для организации и проведения испытаний в соответствии с требованиями стандартов или иных нормативных документов.

Аккредитация предприятия в качестве испытательной лаборатории может являться официальным признанием только ее технической компетентности в проведении испытаний. При этом, испытания для целей серти-

фикации допускается проводить лишь под контролем представителей органа по сертификации соответствующих средств защиты информации.

Аккредитация производится только при наличии у указанных органов и лабораторий лицензий на соответствующие виды деятельности.

1.4. При аккредитации предприятия ему выдается Аттестат аккредитации (Приложения 1, 2) с указанием области аккредитации. Срок действия Аттестата аккредитации не должен превышать пяти лет.

1.5. Требования аккредитации, установленные настоящим документом, являются общими для всех видов испытаний средств защиты информации.

При необходимости, они могут быть дополнены другими требованиями, исходя из специфики деятельности конкретного предприятия.

1.6. Аккредитацию предприятий осуществляет Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России).

2. ПОРЯДОК АККРЕДИТАЦИИ ПРЕДПРИЯТИЯ

2.1. Аккредитация предусматривает следующие этапы:

- рассмотрение документов, представленных предприятием;
- проверка предприятия комиссией, определяемой Гостехкомиссией России;
- принятие решения об аккредитации по результатам проверки;
- оформление, регистрация и выдача Аттестата аккредитации.

2.2. Предприятие, претендующее на аккредитацию, должно подать заявку на аккредитацию (Приложения 3, 4). Одновременно с заявкой направляется проект Положения об органе по сертификации или испытательной лаборатории с заявляемой областью аккредитации (Приложение 5). В случае аккредитации предприятия в качестве испытательной лаборатории средств защиты информации к заявке дополнительно прикладывается паспорт испытательной лаборатории (Приложение 6) и анкета - опросник (Приложение 7).

2.3. После рассмотрения представленных материалов создается комиссия по проверке предприятия. Состав комиссии формируется из специалистов территориальных органов Гостехкомиссии России, отраслевых, региональных центров по защите информации, других организаций и предприятий, компетентных в области защиты информации, и утверждается руководителем Гостехкомиссии России.

2.4. Проверка проводится на соответствие фактического состояния предприятия представленным документам и на его способность выполнять заявленные функции. По результатам проверки комиссия составляет акт (в случае испытательной лаборатории средств защиты информации форма акта приведена в Приложении 8), который подписывается членами комиссии и представляется для ознакомления руководителю аккредитуемого предприятия.

2.5. Решение об аккредитации предприятия принимается после рассмотрения всей полученной информации о состоянии этого предприятия и

его готовности к аккредитации. Аккредитованное предприятие вносится Гостехкомиссией России в государственный реестр системы и ему выдается Аттестат аккредитации.

2.6. За 6 месяцев до окончания срока действия Аттестата аккредитации предприятие, имеющее намерение продлить его действие, направляет заявку в соответствии с п.2.2 настоящего документа.

Порядок повторной аккредитации устанавливается в зависимости от результатов контроля и может проводиться по полной или сокращенной процедуре, устанавливаемой в каждом конкретном случае.

2.7. Аккредитация в дополнительной области.

2.7.1. Орган по сертификации, испытательная лаборатория, претендующие на расширение своей области аккредитации, направляют заявку на аккредитацию в дополнительной области (Приложения 3, 4).

К заявке прилагаются:

- сведения о дополнительной области аккредитации;
- дополнения к Паспорту (Приложение 5).

2.7.2. Аккредитация может проводиться по полной или сокращенной программе, устанавливаемой в каждом конкретном случае.

3. КОНТРОЛЬ И НАДЗОР ЗА ДЕЯТЕЛЬНОСТЬЮ АККРЕДИТОВАННЫХ ИСПЫТАТЕЛЬНЫХ ЛАБОРАТОРИЙ И ОРГАНОВ ПО СЕРТИФИКАЦИИ

3.1. Контроль может осуществляться путем:

- периодических проверок;
- предоставления предприятием регулярной информации о качестве проводимых им испытаний, о результатах периодических внутренних проверок системы обеспечения качества испытаний, о претензиях клиентов и т.д.;
- любых других действий контрольного характера, которые могут обеспечить уверенность в том, что предприятие в течение срока действия Аттестата аккредитации соответствует требованиям, предъявленным к нему при аккредитации.

3.2. Условия контроля для каждого предприятия определяются в соответствующем Положении об органе по сертификации (испытательной лаборатории) при принятии решения по его аккредитации.

3.3. Расходы на проведение всех видов работ по аккредитации предприятий в качестве испытательных лабораторий и органа по сертификации, по осуществлению контроля и надзора за их деятельностью оплачиваются заявителями в порядке, установленном Гостехкомиссией России по согласованию с Министерством финансов Российской Федерации.

4. АННУЛИРОВАНИЕ АККРЕДИТАЦИИ ПРЕДПРИЯТИЙ В КАЧЕСТВЕ ИСПЫТАТЕЛЬНЫХ ЛАБОРАТОРИЙ И ОРГАНОВ ПО СЕРТИФИКАЦИИ

4.1. Аккредитация предприятия может быть досрочно отменена в следующих случаях:

- несоответствие предприятия требованиям, предъявляемым к аккредитованным предприятиям;
- самостоятельное решение аккредитованного предприятия о досрочном прекращении действия аккредитации.

Предприятие может в течение 15 дней опротестовать решение по любым вопросам аккредитации в Госарбитраже России.

Приложение 2

Типовое положение об испытательной лаборатории

Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 25 ноября 1994 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Типовое положение устанавливает основные функции, права, обязанности, ответственность и другие аспекты деятельности испытательной лаборатории при проведении сертификационных испытаний средств защиты информации.

1.2 Типовое положение разработано в соответствии с законами Российской Федерации "О сертификации продукции и услуг" и "О государственной тайне", "Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", на основании "Системы сертификации ГОСТ Р" и "Правил по проведению сертификации в Российской Федерации".

1.3 Испытательные лаборатории являются составной частью организационной структуры системы сертификации средств защиты информации, деятельность которой организует Государственная технической комиссии при Президенте Российской Федерации (Гостехкомиссия России).

1.4 Испытательные лаборатории аккредитуются Гостехкомиссией России в соответствии с "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Испытательная лаборатория должна быть юридическим лицом или его отдельным структурным подразделением, располагать подготовленными специалистами, необходимой испытательной базой, руководящими и нормативными документами для проведения всего комплекса работ по сертификации средств защиты информации в своей области аккредитации и отвечать установленным требованиям.

Аккредитация производится только при наличии лицензии Гостехкомиссии России на соответствующие виды деятельности.

Аккредитация в качестве испытательной лаборатории предприятий, подведомственных федеральным органам исполнительной власти, осуществляется по представлению этих органов власти.

1.5 Испытательная лаборатория в своей деятельности руководствуется законодательством Российской Федерации, государственными стандартами,

нормативной и методической документацией по вопросам сертификации средств защиты информации, утвержденной Гостехкомиссией России.

1.6 Испытательная лаборатория осуществляет свою деятельность в соответствии с Положением, разработанным на основе настоящего Типового положения с учетом юридического статуса и конкретной области аккредитации.

1.7 Руководство деятельностью испытательной лаборатории осуществляет начальник (руководитель) испытательной лаборатории (инженер, образование высшее), который назначается по согласованию с органом по сертификации.

1.8 Испытательная лаборатория должна быть укомплектована специалистами по проведению испытаний, по автоматизации процессов испытаний и измерений, по метрологическому обеспечению испытаний, по ремонту испытательного оборудования и средств измерений, а также по технологии изготовления средств защиты информации и по внесению изменений в конструкторскую документацию.

1.9 Испытательная лаборатория должна располагать материально-технической и метрологической базой, достаточной для проведения сертификационных испытаний в пределах установленной области аккредитации.

1.10 Состав и квалификация персонала испытательной лаборатории, материально-техническая база, нормативная документация и другие сведения, подтверждающие соответствие испытательной лаборатории требованиям настоящего Типового положения, должны быть отражены в Паспорте испытательной лаборатории.

1.11 Форма перечня испытаний, проводимых испытательной лабораторией, и номенклатура закрепленных за испытательной лабораторией средств защиты информации, приведены в Приложении к настоящему Типовому положению.

1.12 Расходы испытательной лаборатории по проведению сертификационных испытаний оплачивают заявители.

Оплата работ по сертификации конкретных средств защиты информации производится в порядке, установленном Гостехкомиссией России по согласованию с Министерством Финансов Российской Федерации, на основании заключенных договоров.

2 ЗАДАЧИ И ФУНКЦИИ ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ

2.1 Основными задачами испытательной лаборатории являются:

- проведение сертификационных испытаний средств защиты информации на соответствие требованиям нормативных документов, утвержденных Гостехкомиссией России, и Государственных стандартов;
- проведение отдельных испытаний средств защиты информации по поручению Гостехкомиссии России и органов по сертификации;
- разработка и представление на согласование в орган по сертификации необходимых методик испытаний;

- проведение экспертизы нормативной документации в части контролируемых показателей, методов и средств испытаний.

2.2 Испытательная лаборатория осуществляет следующие функции:

- осуществляют испытания конкретных средств защиты информации, оформляют заключения и протоколы сертификационных испытаний;
- осуществляют отбор образцов средств защиты информации для проведения сертификационных испытаний;
- участвуют в предварительной проверке (аттестации) производства сертифицируемых средств защиты информации;
- анализирует причины несоответствия представленных на испытания средств защиты информации требованиям безопасности информации;
- разрабатывает и совершенствует методики и программы испытаний, методы и средства испытаний, нормативные и технологические документы по проведению испытаний;
- участвует в проведении проверок с целью контроля стабильности качества изготовления испытываемых средств защиты информации (по поручению Гостехкомиссии России и органов по сертификации);
- участвует в предварительной проверке условий производства видов сертифицируемых средств защиты информации, закрепленных за испытательной лабораторией;
- участвует в рассмотрении апелляций по вопросам сертификации средств защиты информации;
- оказывает методическую и консультационную помощь испытательным подразделениям предприятий, выпускающих закрепленные за испытательной лабораторией средства защиты информации;
- осуществляет сбор, хранение, систематизацию и представление органу по сертификации информации о средствах защиты информации (изделиях), проходивших испытания в испытательной лаборатории. Полученная информация должна использоваться строго конфиденциально (без нарушения прав собственности заявителя на изделие, включая его авторское право и право на защиту коммерческой тайны);
- анализирует зарубежный опыт по проведению закрепленных за испытательной лабораторией видов испытаний, по требования к средствам защиты и по методикам испытаний.

Испытательная лаборатория по результатам проведенных испытаний готовит и представляет органу по сертификации (копии - заявителю):

- протоколы испытаний с заключением о соответствии (или несоответствии) испытанных средств защиты информации установленным требованиям безопасности испытаний. Протоколы испытаний с заключением является основным обязательным документом при принятии решения о соответствии изделия предъявляемым требованиям по безопасности информации;
- акт экспертизы нормативной документации.

3 ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ

3.1 Испытательная лаборатория в пределах установленной области аккредитации имеет право:

- заключать договоры на проведение работ;
- разрабатывать форму протоколов испытаний, порядок их оформления и подписания, обеспечивающих объективную оценку и отражение результатов проведенных испытаний;
- при отрицательных результатах испытаний по инициативе заявителя проводить обследование предприятий-изготовителей средств защиты информации с целью выдачи рекомендаций по изменению технологии их изготовления, внесению изменений в техническую и конструкторскую документацию на средства защиты информации;
- по согласованию с заявителем и органом по сертификации передавать часть сертификационных испытаний на условиях субподряда другим испытательным лабораториям;
- пропагандировать работу испытательной лаборатории;
- по согласованию с заявителем оставлять у себя образцы сертифицируемых средств защиты информации.

3.2 Испытательная лаборатория обязана:

- выполнять функции, предусмотренные настоящим Типовым положением;
- обеспечивать полноту и объективность проведения испытаний, достоверность и точность их результатов;
- соблюдать порядок и сроки проведения испытаний, согласованные с заявителем, а также условия, обеспечивающие конфиденциальность их проведения;
- обеспечивать условия, предотвращающие распространение сертифицированного продукта с нарушениями порядка, установленного законодательством;
- обеспечивать сохранность государственных секретов согласно требованиям действующих нормативных документов;
- обеспечивать в необходимых случаях доступ представителям заявителя, контролирующих органов в помещения или на испытательные участки (площадки) для наблюдения за проводимыми испытаниями;
- ежегодно представлять отчет о результатах своей деятельности в орган по сертификации;
- обеспечивать соответствие технического состояния контрольно-измерительной аппаратуры и испытательного оборудования требованиям эксплуатационной документации, обеспечивать их своевременную поверку и аттестацию;

- обеспечивать содержание производственных помещений для проведения испытаний в соответствии с санитарно-гигиеническими нормами и правилами, требованиями техники безопасности и охраны окружающей среды, требованиями методик испытаний; незамедлительно уведомлять орган по сертификации о любых изменениях в статусе и технической оснащенности испытательной лаборатории.

Для каждой категории специалистов в испытательной лаборатории должны быть должностные инструкции, устанавливающие их функции, обязанности, права и ответственность, требования к качеству проведения работ, к образованию, техническим знаниям и опыту работы.

Сотрудники испытательной лаборатории, непосредственно участвующие в проведении испытаний, должны быть аттестованы на право их проведения в рамках действующего порядка аттестации.

Должно быть обеспечено систематическое повышение квалификации специалистов испытательной лаборатории путем стажировки в соответствующих институтах повышения квалификации, лабораториях и центрах.

Испытательная лаборатория должна располагать документацией, включающей:

- государственные и международные нормативные документы, регламентирующие технические требования и методы испытаний средств защиты на соответствие требованиям безопасности информации;
- программы и методики сертификационных испытаний средств защиты на соответствие требованиям безопасности информации;
- графики поверки и аттестации контрольно-измерительной аппаратуры и испытательного оборудования;
- методики аттестации испытательного оборудования и проверки нестандартизованных средств измерений;
- документацию по эксплуатации средств испытаний (испытательного оборудования);
- рабочие журналы, протоколы испытаний и копии выданных заключений по результатам испытаний.

Испытательная лаборатория должна располагать оборудованными помещениями для приема, хранения и отправки образцов, представляемых на испытания, в соответствии с требованиями нормативной документации на них.

3.3 Испытательная лаборатория несет ответственность за:

- правильность и полноту выполнения функций и обязанностей, возложенных на испытательную лабораторию;
- правильность и полноту проведения испытаний, объективность,
- точность и достоверность их результатов и выводов;
- соблюдение требований нормативных документов (государственных и международных), предъявляемых к порядку и правилам испытаний;

- сохранность и работоспособное состояние предъявляемых на сертификационные испытания средств защиты информации;
- выполнение установленных сроков проведения испытаний, обработки и оформления их результатов;
- своевременное продление аккредитации на право проведения сертификационных испытаний;
- сохранность сведений, составляющих государственную или коммерческую тайны заявителя;
- соблюдение прав собственности заявителя на испытываемые средства защиты информации, включая его авторское право.

Ответственность регулируется действующим законодательством, постановлениями Правительства России, нормативными актами Гостехкомиссии России.