ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

ГОСТ Р О 0043—004— 2013

Защита информации

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Программа и методики аттестационных испытаний

Издание официальное

Москва
Стандартинформ
2016

Предисловие

Цели и принципы стандартизации в области национальных стандартов ограниченного распространения установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» и постановлением Правительства Российской Федерации от 17 октября 2009 г. № 822 «Об утверждении Положения об особенностях стандартизации оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну, а также процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения указанной продукции»

Сведения о стандарте

1 РАЗРАБОТАН Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл»)

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 12 апреля 2013 г. № 1-ст РО

4 ПЕРЕИЗДАНИЕ, февраль 2016 г.

Информация об изменениях стандарта, его пересмотре или отмене публикуется в «Указателе национальных стандартов ограниченного распространения» и в периодических информационных указателях (ИУС)

Содержание

ГОСТ РО 0043 — 004— 2013

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Защита информации

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Программа и методики аттестационных испытаний

Дата введения — 2013—12—01

1 Область применения

Настоящий стандарт устанавливает общие требования к структуре, содержанию, оформлению, утверждению программ и методик аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации, выполнение которых позволяет защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на нее и ее носители.

Положения настоящего стандарта применяются для объектов информатизации, в которых обрабатывается (циркулирует) информация, составляющая государственную тайну, или иная информация, доступ к которой ограничен федеральными законами или по желанию обладателя информации, создаваемых и эксплуатируемых в различных областях деятельности (управление, исследования, проектирование и т. п.).

Настоящий стандарт не распространяется на аттестацию объектов информатизации Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации, Федеральной службы безопасности Российской Федерации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения

ГОСТ РО 0043—003—2012 Защита информации. Аттестация объектов информатизации. Общие положения

ГОСТ Р 53114—2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 7.0.12—2011 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила

ГОСТ 34.003—90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ 28147—89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

Издание официальное

Примечание — При пользовании настоящим стандартом необходимо проверить действие ссылочных стандартов по действующему «Указателю национальных стандартов ограниченного распространения», ежегодно издаваемому указателю «Национальные стандарты» и по соответствующим информационным указателям. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ Р 53114, ГОСТ 34.003, а также следующие термины с соответствующими определениями:

3.1.1 **автоматизированная система;** АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

[ГОСТ Р 53113.1—2008, статья 3.1]

3.1.2 **автоматизированное рабочее место;** АРМ: Объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

3.1.3 **аттестация объектов информатизации:** Комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации.

3.1.4 **аттестационные испытания:** Определение количественных и качественных характеристик объекта информатизации и его системы защиты информации с целью оценки их соответствия требованиям безопасности информации.

3.1.5 **вспомогательные технические средства и системы;** ВТСС: Технические средства и системы, не предназначенные для передачи, обработки и хранения защищаемой информации, устанавливаемые совместно с основными техническими средствами и системами или в выделенных (защищаемых) помещениях.

3.1.6 **выделенное помещение;** ВП: Помещение (служебный кабинет, актовый зал, конференц-зал, и т. д.), предназначенное для проведения закрытых мероприятий (совещаний, обсуждений, переговоров и т. п.) по секретным вопросам, а также помещение, оборудованное средствами специальной связи.

3.1.7 **защищаемое помещение;** ЗП: Помещение (служебный кабинет, актовый зал, конференц-зал и т. д.), предназначенное для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т. п.).

3.1.8 **защищаемые информационные ресурсы автоматизированной системы:** Информационные ресурсы автоматизированной системы, для которых должен быть обеспечен требуемый уровень их защищенности.

Примечание — Информационные ресурсы включают в себя документы и массивы документов, хранящиеся и обрабатываемые в автоматизированных системах.

3.1.9 **заявитель:** Юридическое лицо, которое для подтверждения соответствия своего объекта информатизации требованиям безопасности информации обращается за получением аттестата соответствия.

3.1.10 **знак соответствия:** Зарегистрированный в установленном порядке знак, который по правилам, установленным в данной системе сертификации, подтверждает соответствие маркированной им продукции установленным требованиям.

Примечание — Наличие знака соответствия обязательно для сертифицированных средств защиты информации.

3.1.11 **информационная система:** Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Примечание — Информационные системы являются одной из разновидностей автоматизированных систем, результатом функционирования которых является представление выходной информации для последующего использования.

3.1.12 **информативный сигнал:** Электрические, акустические сигналы, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта защищаемая информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и обсуждаемая в выделенных (защищаемых) помещениях.

3.1.13 **контролируемая зона;** КЗ: Пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Примечания

1 Границей КЗ могут являться:

- периметр охраняемой территории предприятия (учреждения, организации);
- ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного (защищаемого) помещения.

2 В отдельных случаях на период обработки техническими средствами информации ограниченного доступа (проведения закрытого мероприятия) КЗ временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

3.1.14 **локальная информационная система:** Совокупность автоматизированных рабочих мест и (или) отдельных средств вычислительной техники, объединенных между собой в единую систему посредством линий передачи данных, не выходящих за пределы контролируемой зоны.

3.1.15 **объект информатизации;** ОИ: Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

[ГОСТ Р 51275—2006, статья 3.1]

3.1.16 **объект вычислительной техники;** ОВТ: Совокупность информационных ресурсов, средств вычислительной техники, используемых в соответствии с заданной информационной технологией, а также средств обеспечения их функционирования и помещений, в которых они размещены.

3.1.17 **орган по аттестации объектов информатизации:** Юридическое лицо, выполняющее работы по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

3.1.18 **основные технические средства и системы;** ОТСС: Технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации, составляющей государственную тайну, и иной информации конфиденциального характера.

3.1.19 **распределенная информационная система:** Комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа.

3.1.20 **система защиты информации объекта информатизации:** Проводимые мероприятия по защите информации и средства защиты информации (в том числе криптографические, средства защиты от несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства и системы), а также используемые информационные технологии.

3.1.21 **средство вычислительной техники;** СВТ: Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

[ГОСТ Р 50739—95, раздел 1]

3.1.22 **средство обработки речевой и видеоинформации:** Техническое средство (система), предназначенное для записи, хранения, воспроизведения, передачи по линиям связи речевой и (или) видеоинформации.

Примечание — К средствам (системам) обработки речевой и видеоинформации относятся телефонные аппараты, переговорные устройства, системы звукоусиления, средства записи и воспроизведения, теле- и видеосистемы и др.

3.1.23 **технический канал утечки информации;** ТКУИ: Путь утечки информации от объекта защиты, образуемый совокупностью объекта защиты, физической среды и средства технической разведки.

3.1.24 **требования безопасности информации:** Требования, выполнение которых позволяет защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на нее и ее носители.

Примечание — Требования безопасности информации устанавливаются федеральными законами, нормативными правовыми актами Президента Российской Федерации, Правительства Российской Федерации, уполномоченных федеральных органов исполнительной власти, национальными стандартами, владельцем информации или объекта информатизации.

3.1.25 **уполномоченные федеральные органы исполнительной власти:** Федеральные органы исполнительной власти, устанавливающие в пределах своих полномочий обязательные требования безопасности информации, а также порядок сертификации продукции, используемой в целях защиты информации, и аттестации объектов информатизации.

3.2 В настоящем стандарте приняты следующие сокращения:

ВОСП — волоконно-оптическая система передачи данных;
НСД — несанкционированный доступ;
ПЭМИ — побочные электромагнитные излучения;
ПЭМИН — побочные электромагнитные излучения и наводки;
РД — руководящий документ;
СЗИ — средство защиты информации;
СИРД — средство изготовления и размножения документов;
ТСИП — техническое средство иностранного производства;
ЭВМ — электронно-вычислительная машина.

4 Общие положения

4.1 Целью аттестационных испытаний является определение соответствия ОИ требованиям безопасности информации.

4.2 Видами ОИ являются:

а) АС, а именно:

1) автоматизированные рабочие места без подключения к внешним информационным системам, в том числе к сетям общего пользования;

2) автоматизированные рабочие места с подключением к внешним информационным системам, в том числе к сетям общего пользования;

3) локальные информационные системы без подключения к внешним информационным системам, в том числе к сетям общего пользования;

4) локальные информационные системы с подключением к внешним информационным системам, в том числе к сетям общего пользования;

5) распределенные информационные системы без подключения к внешним информационным системам и сетям общего пользования, в том числе использующие ВОСП;

6) распределенные информационные системы с подключением к внешним информационным системам и сетям общего пользования, в том числе использующие ВОСП;

б) средства изготовления и размножения документов, использующие методы обработки информации, не предусматривающие использование ЭВМ;

в) средства обработки речевой и видеоинформации, эксплуатация которых не предусматривает использование ЭВМ;

г) выделенные (защищаемые) помещения.

4.3 Технические средства и системы, входящие в состав ОИ, указанных в перечислениях а), б) и в) 4.2, и предназначенные для передачи, обработки и хранения защищаемой информации, являются ОТСС ОИ.

В состав ОИ также могут входить ВТСС, не предназначенные для передачи, обработки и хранения защищаемой информации.

4.4 Задачи аттестационных испытаний ОИ заключаются в оценке соответствия системы защиты информации ОИ требованиям безопасности информации.

4.5 При проведении аттестационных испытаний применяются методы проверки и испытаний в соответствии с ГОСТ РО 0043—003 (пункт 6.5.2).

4.6 Аттестационные испытания проводятся в реальных условиях эксплуатации технических средств и систем ОИ (с использованием информации, не содержащей сведения ограниченного доступа) с применением поверенных средств измерений, контрольной аппаратуры и сертифицированных средств контроля эффективности защиты информации.

Примечание — Особенности аттестационных испытаний распределенных информационных систем, предназначенных для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, указаны в ГОСТ РО 0043—003 (пункт 6.5.3) и в 6.1.3.

4.7 Результаты аттестационных испытаний ОИ используются для оценки его соответствия требованиям безопасности информации.

4.8 Порядок проведения аттестации ОИ — по ГОСТ РО 0043—003 (раздел 6).

5 Общие требования к разработке, структуре, оформлению и утверждению программы и методик аттестационных испытаний объектов информатизации

5.1 Аттестационные испытания ОИ проводят члены аттестационной комиссии по согласованным с заявителем программе и методикам испытаний, разработанным по результатам анализа исходных данных об ОИ и предварительного ознакомления с аттестуемым ОИ.

5.2 Программа и методики аттестационных испытаний разрабатываются:

- органом по аттестации (при обработке информации, содержащей сведения, составляющие государственную тайну);
- организацией, имеющей право на деятельность в области технической защиты конфиденциальной информации (при обработке информации конфиденциального характера).

5.3 Программа и методики аттестационных испытаний ОИ подписываются руководителем аттестационной комиссии и утверждаются руководителем органа по аттестации (организации, имеющей право на деятельность в области технической защиты конфиденциальной информации).

Программа и методики аттестационных испытаний подлежат согласованию с заявителем до начала аттестационных испытаний.

5.4 В ходе аттестационных испытаний ОИ программа и методики аттестационных испытаний, при необходимости, уточняются и корректируются решением руководителя органа по аттестации по согласованию с заявителем.

5.5 Программа и методики аттестационных испытаний ОИ составляются от имени юридического лица — органа (организации), ответственного за их разработку. Форма титульного листа программы и методик аттестационных испытаний приведена в приложении А.

5.5.1 Программа и методики аттестационных испытаний ОИ выполняются в виде единого документа. Текст документа должен отвечать следующим требованиям:

- соответствовать действующим нормативным правовым актам, методическим документам и документам по стандартизации в области защиты информации и иметь ссылки на них (при необходимости);
- состоять из кратко, четко и в логической последовательности изложенных формулировок, не допускающих различных толкований.

5.5.2 Программа и методики аттестационных испытаний ОИ должны состоять из следующих разделов:

- общие положения;
- программа аттестационных испытаний конкретного ОИ на соответствие требованиям безопасности информации;
- методики аттестационных испытаний конкретного ОИ на соответствие требованиям безопасности информации.

Примечание — Допускается совмещение в одном документе программ и методик аттестационных испытаний разных типов ОИ.

5.5.3 В разделе «Общие положения» должны содержаться:

- сведения о наименовании аттестуемого (или аттестуемых) ОИ, краткая характеристика каждого ОИ (категория, класс защищенности (уровень защищенности) от НСД, принадлежность к структурному подразделению организации-заявителя, место расположения);

- сведения о руководителе аттестационной комиссии, персональный состав аттестационной комиссии;

- перечень нормативных правовых актов, методических документов и документов по стандартизации в области защиты информации, на соответствие требованиям которых проводятся аттестационные испытания ОИ;

- перечень задач, решаемых в ходе аттестационных испытаний ОИ (отдельно для каждого вида ОИ);

- описание применяемых в ходе аттестационных испытаний методов проверок аттестуемых ОИ на соответствие требованиям безопасности информации;

- перечень контрольной аппаратуры, средств измерений и инструментальных средств контроля эффективности защиты информации от НСД с указанием сведений о поверках и действующих сертификатах;

- порядок действий аттестационной комиссии и организации-заявителя при обнаружении недостатков или нарушений, которые не позволяют сделать вывод о соответствии ОИ требованиям безопасности информации.

Типовая форма раздела «Общие положения» программы и методик аттестационных испытаний ОИ приведена в приложении Б.

5.5.4 Требования к содержанию программы и методик аттестационных испытаний конкретного вида ОИ на соответствие требованиям безопасности информации указаны в разделах 6 и 7.

5.5.5 Оформление документа выполняют в соответствии с требованиями настоящего стандарта. Сокращение русских слов и словосочетаний — по ГОСТ Р 7.0.12.

При оформлении документа применяют формат А4 (210×297 мм). Текст печатают через один или полтора межстрочных интервала, кегль 12 — 14. Реквизиты документа отделяют друг от друга двумя-тремя межстрочными интервалами. Реквизиты, состоящие из нескольких строк, печатают через один межстрочный интервал. Наименование документа печатают прописными буквами.

Номера страниц должны быть проставлены по центру внизу поля листа арабскими цифрами без слова «страница (стр.)» и знаков препинания.

6 Требования к содержанию программы аттестационных испытаний объектов информатизации

6.1 Требования к содержанию программы аттестационных испытаний автоматизированных систем, средств изготовления и размножения документов, средств обработки речевой и видеоинформации

6.1.1 Программа аттестационных испытаний АС должна содержать перечень конкретных работ, которые требуется провести для оценки и подтверждения выполнения предъявляемых требований безопасности информации, перечень объектов испытаний с указанием продолжительности работ и используемых при этом методов проверок и испытаний.

6.1.2 Программа аттестационных испытаний АС должна включать:

- проверку структуры, состава и условий эксплуатации АС;

- проверку правильности категорирования и классификации АС (определения уровня защищенности информации);

- проверку достаточности представленных документов и соответствия их содержания установленным требованиям, наличия сертификатов соответствия требованиям безопасности информации и (или) предписаний на эксплуатацию, заключений о специальной проверке, а также проверку их выполнения;

- проверку уровня подготовки специалистов, обеспечивающих защиту информации, и распределения ответственности должностных лиц, эксплуатирующих АС, за выполнение требований безопасности информации;

- проверку выполнения требований безопасности информации к помещению, в котором проводится обработка информации;

- проведение испытаний АС на соответствие требованиям по защите информации от утечки по техническим каналам;

- проведение испытаний АС на соответствие требованиям по защите информации от НСД;

- подготовку отчетной документации и оценку результатов испытаний аттестуемой АС;

- разработку протоколов оценки эффективности принятых мер по защите информации от утечки по техническим каналам;

- оформление материалов аттестационных испытаний (протоколов испытаний и заключения по результатам аттестационных испытаний);
- установление продолжительности работ по пунктам программы;
- проведение контроля соответствия системы защиты информации аттестованной АС требованиям безопасности в процессе ее эксплуатации.

6.1.3 Дополнительно в программе аттестационных испытаний распределенных информационных систем, предназначенных для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, допускается устанавливать особенности аттестации распределенной информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов (составных частей), реализующих полную технологию обработки информации конфиденциального характера, а также условия и порядок распространения аттестата соответствия на другие сегменты информационной системы.

Сегмент считается соответствующим аттестованному сегменту распределенной информационной системы, если для обоих сегментов установлены одинаковые классы защищенности и состав актуальных угроз безопасности информации, реализованы одинаковые проектные решения по системе защиты информации распределенной информационной системы.

Соответствие сегмента, на который распространяется аттестат соответствия, аттестованному сегменту распределенной информационной системы подтверждается в ходе приемочных испытаний распределенной информационной системы или сегментов распределенной информационной системы.

В сегментах распределенной информационной системы, на которые распространяется аттестат соответствия, оператор обеспечивает соблюдение требований эксплуатационной документации на систему защиты информации распределенной информационной системы и организационно-распределительных документов по защите информации.

Повторная аттестация распределенной информационной системы осуществляется в случаях окончания срока действия аттестата соответствия, изменения класса защищенности распределенной информационной системы (уровня защищенности информации), состава актуальных угроз безопасности информации или проектных решений по системе защиты информации распределенной информационной системы (в том числе состава используемых СЗИ).

6.1.4 Требования к содержанию программы аттестационных испытаний СИРД и средств обработки речевой и видеоинформации аналогичны требованиям к содержанию программы аттестационных испытаний АС с учетом актуальных для них угроз безопасности информации.

Типовая программа аттестационных испытаний АС приведена в приложении В.

6.2 Требования к содержанию программы аттестационных испытаний выделенных (защищаемых) помещений

6.2.1 Программа аттестационных испытаний ВП (ЗП) должна содержать перечень конкретных работ, которые требуется провести для оценки и подтверждения выполнения предъявляемых требований безопасности информации, перечень объектов испытаний с указанием продолжительности работ и используемых при этом методов проверок и испытаний.

6.2.2 Программа аттестационных испытаний ВП (ЗП) должна включать:
- проверку структуры, состава и условий эксплуатации ВП (ЗП);
- проверку правильности категорирования ВП;
- проверку достаточности представленных документов и соответствия их содержания установленным требованиям;
- проверку наличия сертификатов соответствия требованиям безопасности информации и (или) предписания на эксплуатацию, а также заключений о специальной проверке для всех технических средств и систем, установленных в ВП (ЗП);
- проверку уровня подготовки специалистов, обеспечивающих защиту информации в ВП (ЗП) и распределения ответственности должностных лиц, эксплуатирующих данные объекты, за выполнение требований безопасности информации;
- проведение испытаний ВП (ЗП) на соответствие требованиям по защите акустической речевой информации от утечки по техническим каналам;
- подготовку отчетной документации и оценку результатов испытаний аттестуемых ВП (ЗП);
- разработку протокола инструментальной проверки выполнения требований по защите акустической речевой информации;

-оформление материалов аттестационных испытаний (протоколов испытаний и заключения по результатам аттестационных испытаний);

- установление продолжительности работ по пунктам программы;

- проведение контроля соответствия системы защиты информации аттестованного ВП (ЗП) требованиям безопасности в процессе его эксплуатации.

Типовая программа аттестационных испытаний ВП (ЗП) приведена в приложении Г.

7 Требования к содержанию методик аттестационных испытаний объектов информатизации

7.1 Требования к содержанию методик аттестационных испытаний автоматизированных систем, средств изготовления и размножения документов, средств обработки речевой и видеоинформации

7.1.1 Методики аттестационных испытаний должны содержать подробное описание и порядок выполнения практических действий, осуществляемых при оценке количественных и качественных характеристик ОИ и его системы защиты информации, перечень требований, подлежащих проверке, и условий, в которых проводится проверка, а также критерии, по которым делаются выводы о соответствии аттестуемого ОИ (АС, СИРД, средства обработки речевой и видеоинформации) требованиям безопасности информации на каждом этапе проводимых работ, с указанием используемых при этом нормативных правовых актов, методических документов и документов по стандартизации в области защиты информации.

7.1.2 Методики аттестационных испытаний АС должны включать:

- анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств АС;

- исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки и передачи информации ОТСС;

- проверку состояния организации работ и выполнения организационных и технических требований по защите информации, оценку правильности категорирования и классификации (уровня защищенности), оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации, оценку уровня подготовки кадров, обеспечивающих защиту информации в АС и распределения ответственности пользователей АС за выполнение требований безопасности информации, проверку помещения, в котором производится обработка информации, на соответствие требованиям по защите информации от утечки вследствие просмотра видовой информации с экранов дисплеев и других средств отображения информации, входящих в состав ОТСС, путем непосредственного наблюдения и (или) с помощью оптических средств;

- проверку АС на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений от ОТСС и наводок информативных сигналов на цепи электропитания и заземления ОТСС, а также наводок информативных сигналов на ВТСС и их кабельные коммуникации, имеющие выход за границу КЗ;

- проверку выполнения требований по защите информации АС от утечки за счет возможно внедренных электронных закладочных устройств в ОТСС иностранного производства;

- проверку АС на соответствие требованиям по защите информации от НСД;

- проверку АС на соответствие требованиям по защите информации от специальных программных воздействий на нее и ее носители.

7.1.3 Требования к содержанию методик аттестационных испытаний СИРД и средств обработки речевой и видеоинформации аналогичны требованиям к содержанию методик аттестационных испытаний АС, с учетом актуальных для них угроз безопасности информации.

Типовые методики аттестационных испытаний АС приведены в приложении Д.

7.2 Требования к содержанию методик аттестационных испытаний выделенных (защищаемых) помещений

7.2.1 Методики аттестационных испытаний ВП (ЗП) должны содержать подробное описание и порядок выполнения практических действий, осуществляемых при оценке количественных и качественных характеристик ВП (ЗП) и его системы защиты информации, перечень требований, подлежащих проверке, и условий, в которых проводится проверка, а также критерии, по которым делаются выводы о соответствии аттестуемого помещения требованиям безопасности информации на каждом этапе проводимых работ, с указанием используемых при этом нормативных правовых актов, методических документов и документов по стандартизации в области защиты информации.

7.2.2 Методики аттестационных испытаний ВП (ЗП) должны включать:

- анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств, установленных в ВП (ЗП) (при их наличии);
- проверку состояния организации работ и выполнения требований по защите информации, оценку правильности категорирования ВП, оценку полноты и уровня отработки проектной, эксплуатационной и организационно-распорядительной документации, оценку уровня подготовки специалистов, обеспечивающих защиту информации в ВП (ЗП), и проверку наличия распределения их ответственности за выполнение требований безопасности информации;
- проверку выполнения требований по защите ВП (ЗП) от утечки акустической речевой информации по акустическому и виброакустическому каналам;
- проверку наличия протоколов специальных исследований и предписаний на эксплуатацию всех установленных в ВП (ЗП) ОТСС и ВТСС и выполнения требований предписаний по защите информации от утечки за счет акустоэлектрических преобразований и паразитной генерации;
- проверку выполнения требований по защите ВП от утечки информации за счет возможно внедренных электронных закладочных устройств в ТСИП (и (или) предметах интерьера помещения).

Типовые методики аттестационных испытаний ВП (ЗП) приведены в приложении Е.

8 Требования обеспечения защиты сведений, составляющих государственную тайну, и иной информации ограниченного доступа

8.1 Разработку документов по аттестации ОИ, содержащих сведения, составляющие государственную тайну, и иную информацию ограниченного доступа, осуществляют с учетом требований действующего законодательства.

8.2 При разработке документов по аттестации ОИ с применением электронных носителей информации должны быть осуществлены необходимые мероприятия по защите сведений, составляющих государственную тайну, и иной информации ограниченного доступа, исключающие доступ лиц, которым они не предназначены.

8.3 Документы, не содержащие сведений, составляющих государственную тайну, но содержащие библиографические и нормативные ссылки на настоящий стандарт, включающие его полное наименование, должны иметь пометку «Для служебного пользования».

Приложение А
(рекомендуемое)

Форма титульного листа программы и методик аттестационных испытаний

Орган по аттестации объектов информатизации по требованиям безопасности информации
(аттестат аккредитации № _____)

СОГЛАСОВАНО
Руководитель организации-заявителя
(должность и название организации)

_____ И. Фамилия
м. п.

«_____» _____ 20____ г.

УТВЕРЖДАЮ
Руководитель органа по аттестации
(должность и название организации)

_____ И. Фамилия
м. п.

«_____» _____ 20____ г.

ПРОГРАММА И МЕТОДИКИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

ОБЪЕКТА (ОБЪЕКТОВ) ИНФОРМАТИЗАЦИИ

_____
(название организации — владельца объекта (ов) информатизации)

20__

Приложение Б
(рекомендуемое)

Типовая программа и методики аттестационных испытаний объектов информатизации. Раздел «Общие положения»

Б.1 Настоящий документ определяет цели, задачи, методы, условия, объем, порядок и методику проведения аттестационных испытаний на соответствие требованиям безопасности информации ОИ *(название организации-заявителя)*[1], расположенных в *(наименование или номер корпуса, здания) по адресу: г.* _____, *ул.* _____, *д.* _____ *(приводится перечень аттестуемых ОИ):*

а) автоматизированной системы *(полное наименование объекта информатизации)* класса (уровня) защищенности _____, размещенной в комнате № _____ *(первичная или повторная аттестация)*[2];

б) выделенного помещения *(полное наименование объекта информатизации)* _____ категории, расположенного в комнате № _____ *(первичная или повторная аттестация);*

в) распределенной информационной системы *(полное наименование объекта информатизации, первичная или повторная аттестация):*

- сегмента *(наименование)* распределительной информационной системы _____ класса (уровня) защищенности, расположенного *(место размещения сегмента распределенной информационной системы);*

. . . . . .

- сегмента *(наименование)* распределительной информационной системы _____ класса (уровня) защищенности, расположенного *(место размещения сегмента распределенной информационной системы).*

Б.2 Результаты аттестационных испытаний сегмента *(наименование)* распределенной информационной системы и аттестат соответствия распространяются на:

- *(наименование сегмента распределенной информационной системы, класс (уровень) защищенности, место размещения);*

. . . . . .

- *(наименование сегмента распределенной информационной системы, класс (уровень) защищенности, место размещения).*

Б.3 В соответствии с п. 3 «Положения об органе по аттестации объектов информатизации» (аттестат аккредитации в системе сертификации средств защиты информации по требованиям безопасности информации № СЗИ RU._____) аттестационная комиссия назначается руководителем органа по аттестации из числа штатных сотрудников *(наименование организации, аккредитованной уполномоченным федеральным органом исполнительной власти)*, назначенных в состав экспертов органа по аттестации.

В соответствии с приказом руководителя *(наименование организации, аккредитованной уполномоченным федеральным органом исполнительной власти)* от ___.___.20___ г. №_____ руководителем аттестационной комиссии назначен *(фамилия, инициалы) — (должность)*, заместителем руководителя аттестационной комиссии назначен *(фамилия, инициалы) — (должность)*, в состав аттестационной комиссии назначены:

(фамилия, инициалы) — (должность);
(фамилия, инициалы) — (должность);
(фамилия, инициалы) — (должность);

. . . . . .

(фамилия, инициалы) — (должность).

Б.4. Целью аттестационных испытаний является определение соответствия ОИ *(название организации-заявителя)* требованиям безопасности информации. Аттестационные испытания проводятся на соответствие положениям и требованиям действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты информации *(перечень документов приводится в приложении к программе и методикам аттестационных испытаний).*

Б.5 Задачей аттестационных испытаний АС является оценка соответствия системы защиты информации АС требованиям безопасности информации, выполнение которых позволяет защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на нее и ее носитель вследствие:

---

[1] Здесь и далее в приложении Б курсивом выделены данные, относящиеся к аттестационным испытаниям конкретного ОИ.

[2] Здесь и далее подчеркиванием выделены примеры описания аттестуемых ОИ.

- побочных электромагнитных излучений информативного сигнала[1];
- наводок побочных электромагнитных излучений информативного сигнала от ОТСС на ВТСС и их кабельные и проводные коммуникации, имеющие выход за границу контролируемой зоны;
- наводок побочных электромагнитных излучений информативного сигнала от ОТСС на цепи электропитания и заземления ОТСС;
- перехвата циркулирующей в ВОСП информации по оптическому каналу (при наличии линий ВОСП, выходящих за границу КЗ;
- информативных сигналов от возможно внедренных в ТСИП, входящих в состав ОТСС, электронных закладочных устройств;
- несанкционированного доступа к информации, обрабатываемой в АС;
- специальных программных воздействий, нарушающих целостность обрабатываемой в АС информации и (или) работоспособность СВТ или средств защиты информации;
- хищения технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотра видовой информации с экранов дисплеев и других средств отображения информации, входящих в состав ОТСС, путем непосредственного наблюдения и (или) с помощью оптических средств.

Б.6 Задачей аттестационных испытаний распределенной информационной системы является оценка соответствия системы защиты информации требованиям безопасности информации, выполнение которых позволяет защитить информацию от утечки по техническим каналам, от НСД и от специальных воздействий на нее и ее носители *(аналогично пункту Б.5 приводится описание угроз безопасности информации применительно к аттестуемым сегментам распределенной информационной системы).*

Б.7 Задачей аттестационных испытаний ВП (ЗП) является оценка соответствия системы защиты информации требованиям безопасности информации, выполнение которых позволяет защитить акустическую речевую информацию от ее утечки вследствие:

- излучений акустических речевых сигналов[2];
- вибрационных сигналов, возникающих посредством преобразования акустических речевых сигналов при воздействии их на строительные конструкции и инженерно-технические коммуникации ВП (ЗП);
- радиоизлучений, модулированных акустическим речевым сигналом, возникающим при работе различных генераторов, входящих в состав ОТСС и ВТСС, или при наличии паразитной высокочастотной генерации в их узлах (элементах);
- электрических сигналов, возникающих в результате акустоэлектрических преобразований в ОТСС и ВТСС и распространяющихся по отходящим от них проводным линиям за пределы КЗ;
- акустических речевых сигналов, возникающих в результате использования возможно внедренных в ТСИП и (или) предметы интерьера ВП (ЗП) электронных закладочных устройств;
- размещения технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

Б.8 При проведении аттестационных испытаний применяются следующие методы проверок и испытаний *(приводится перечень применяемых при проведении аттестационных испытаний методов проверок и испытаний):*

- экспертно-документальный метод[3];
- инструментальные измерения и оценка защищенности информации от ее утечки по техническим каналам;
- проверка функций или комплекса функций защиты информации от НСД с помощью инструментальных средств контроля, а также путем пробного запуска СЗИ от НСД и наблюдения за выполнением их функций;
- проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;
- проверка подсистем защиты информации от НСД, целостности применяемых СЗИ от НСД, в том числе с использованием специальных средств контроля эффективности защиты информации;
- проверка программной совместимости и корректности функционирования всего комплекса используемых СВТ с продукцией, используемой в целях защиты информации;
- испытания системы защиты информации от НСД путем попыток осуществить НСД к тестовой защищаемой информации в обход используемой системы защиты информации, в том числе с использованием специальных программных тестирующих средств;
- инструментальные измерения звукопоглощающих (звукоизолирующих) характеристик ограждающих конструкций ВП (ЗП) и оценка защищенности акустической речевой информации от ее утечки по техническим каналам;
- инструментальные измерения и оценка эффективности применяемых средств защиты речевой информации.

---

[1] Здесь и далее подчеркиванием выделены примеры описания угроз безопасности информации применительно к аттестуемым АС.

[2] Здесь и далее подчеркиванием выделены примеры описания угроз безопасности информации применительно к аттестуемым ВП (ЗП).

[3] Здесь и далее подчеркиванием выделены примеры описания применяемых при проведении аттестационных испытаний методов проверок и испытаний.

Б.8.1 Экспертно-документальный метод предусматривает проверку соответствия системы защиты информации ОИ установленным требованиям безопасности информации на основании экспертной оценки полноты и достаточности необходимых мер защиты информации в представленных документах, а также на основании соответствия реальных условий эксплуатации требованиям к размещению, монтажу и эксплуатации технических средств.

Б.8.2 Измерения и оценка защищенности осуществляются с помощью поверенных средств измерений и инструментальных средств контроля эффективности защиты информации в соответствии с действующими нормативными и методическими документами по защите информации от ее утечки по техническим каналам. Примерный перечень используемых средств измерений и инструментальных средств контроля защищенности от НСД к информации приведен в таблицах Б.1 и Б.2.

Таблица Б.1 — Используемые средства измерения и инструментальные средства контроля эффективности защиты информации от ее утечки по техническим каналам

Вид оборудования	Наименование, заводской номер	Основные технические характеристики	Сведения о поверке, сертификате и знаке соответствия
Измерительный приемник — анализатор спектра		Диапазон частот от 0,009 до 7000 МГц	Свидетельство о поверке №_____, действительно до_____ (число, месяц, год)
Комплект измерительных антенн		Диапазон частот: от 0,009 до 30 МГц от 0,009 до 2000 МГц	
Токосъемник индукционный		Диапазон частот от 0,009 до 300 МГц	Свидетельство о поверке №_____, действительно до_____ (число, месяц, год)
Автоматизированная система исследования эффекта акустоэлектрических преобразований в технических средствах и в отходящих от них линиях		Предназначена для проведения исследований характеристик технических средств с целью выявления наличия в них акустоэлектрических преобразований, возникающих при воздействии на них акустическим сигналом	Свидетельство о поверке №_____, действительно до_____ (число, месяц, год) Техническое средство контроля защищенности технических средств и отходящих от них линий от утечки речевой информации — сертификат ФСТ ЭК России №_____, действителен до_____, (число, месяц, год) знак соответствия №_____
Система измерительная автоматизированная		Диапазон частот от 100 до 10 000 Гц; максимальный уровень звукового давления 94 дБ; чувствительность преобразователей: микрофона — 1,6 мВ/Па; вибрации — 1,0 мВ/м/с	Программно-техническое средство контроля эффективности защиты информации, обрабатываемой в выделенных помещениях — сертификат ФСТЭК России № _____, действителен до _____, (число, месяц, год) знак соответствия № _____, поверено _____ (число, месяц, год)
Генератор		Диапазон частот от 0,009 до 3000 МГц	Не требуется
Цифровой осциллограф		Полоса пропускания амплитудно-частотной характеристики от 0 до 100 МГц	Не требуется

Таблица Б.2 — Используемые инструментальные средства контроля защищенности от НСД к информации

Используемые средства	Сведения о сертификате, знаке соответствия
Программа фиксации и контроля исходного программного комплекса	Сертификат ФСТЭК России №_____, действителен до_____ (число, месяц, год) знак соответствия № _____
Средство контроля защищенности АС от НСД	Сертификат ФСТЭК России №_____, действителен до_____ (число, месяц, год) знак соответствия № _____
Программа контроля полномочий доступа к информационным ресурсам	Сертификат ФСТЭК России №_____, действителен до_____ (число, месяц, год) знак соответствия № _____
Программа поиска и гарантированного уничтожения информации на дисках	Сертификат ФСТЭК России №_____, действителен до_____ (число, месяц, год) знак соответствия № _____
Сетевой сканер безопасности	Сертификат ФСТЭК России №_____, действителен до_____ (число, месяц, год) знак соответствия № _____
Программа инвентаризации ресурсов	Сертификат ФСТЭК России №_____, действителен до_____ (число, месяц, год) знак соответствия № _____

Б.8.3 Проверка и испытания комплекса функций защиты информации от НСД проводятся для программно-технической среды АС в целом в соответствии с действующими документами по защите информации от НСД.

Б.9 Проверка соответствия ОИ требованиям безопасности информации проводится на основании анализа общих результатов испытаний и выявленных в процессе испытаний недостатков и нарушений.

Б.10 В случае выявления по результатам испытаний несоответствия ОИ установленным требованиям по защите информации комиссия может рассмотреть возможность оперативного устранения выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры *(приводится перечень мер по устранению выявленных недостатков и нарушений)*:

- доработка организационно-распорядительной документации[1)];
- исключение отдельных технических средств из состава АС;
- исключение отдельных технических средств из состава ВП (ЗП);
- применение дополнительных организационных и технических мер защиты;
- применение дополнительных сертифицированных средств защиты информации.

[1)] Здесь и далее подчеркиванием выделены примеры описания мер по устранению выявленных недостатков и нарушений.

Приложение В
(рекомендуемое)

Типовая программа аттестационных испытаний автоматизированной системы

В.1 Аттестационные испытания АС проводятся в соответствии с программой, включающей следующий перечень работ и порядок их проведения

В.1.1 Проверка структуры, состава и условий эксплуатации АС, включающая:

- анализ полноты исходных данных и проверку их соответствия реальным условиям размещения, монтажа и эксплуатации АС;
- исследование технологического процесса обработки, хранения и передачи информации;
- анализ информационных потоков;
- определение состава использованных для обработки, хранения и передачи информации ОТСС.

В.1.2 Проверка состояния организации работ и выполнения требований по защите информации, включающая:

- оценку правильности классификации АС;
- оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации;
- оценку уровня подготовки специалистов, обеспечивающих защиту информации в АС, и проверку наличия распределения ответственности пользователей АС за выполнение требований безопасности информации.

В.1.3 Проверка АС на соответствие требованиям безопасности информации, включающая:

- проверку наличия необходимых документов и соответствия их содержания установленным требованиям, наличия сертификатов соответствия требованиям безопасности информации и (или) предписаний на эксплуатацию, проверка их выполнения;
- проверку уровня подготовки специалистов, обеспечивающих защиту информации на ОИ, и распределения ответственности должностных лиц, эксплуатирующих данные объекты, за выполнение требований безопасности информации;
- проверку выполнения требований безопасности информации к помещению, в котором проводится обработка информации.

В.1.4 Проведение испытаний АС на соответствие требованиям по защите информации от утечки по техническим каналам.

В.1.5 Проведение испытаний АС на соответствие требованиям по защите информации от НСД.

В.1.6 Подготовка отчетной документации и оценка результатов испытаний аттестуемой АС:

а) результаты проведения испытаний АС на соответствие требованиям по защите информации отражаются в протоколе контроля защищенности информации или оценки эффективности принятых мер по защите информации от утечки за счет ПЭМИН и в протоколе проверки выполнения требований по защите информации от НСД;

б) материалы аттестационных испытаний оформляются протоколами испытаний, содержащими:

- наименование аттестуемого объекта;
- цель испытаний;
- перечень использованных нормативных документов и методик испытаний;
- перечень средств измерений и средств контроля защиты информации от НСД;
- описание проверок;
- результаты испытаний;

в) на основании данных документов составляется заключение по результатам аттестационных испытаний, включающее:

- оценку соответствия АС требованиям безопасности информации;
- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- вывод о возможности (невозможности) выдачи «Аттестата соответствия».

В.2 Продолжительность работ по пунктам «Программы аттестационных испытаний» (для аттестации одного автоматизированного рабочего места) составляет:

- по В.1.1, В.1.2, В.1.3 — до__дней;
- по В.1.4, В.1.5 — до__дней;
- по В.1.6 — до__дней.

Примечание — Для локальных и распределенных информационных систем продолжительность работ определяется исходя из количества ОТСС и сложности построения системы защиты информации.

В.3 Контроль соответствия системы защиты информации аттестованных АС требованиям безопасности информации в процессе эксплуатации проводится в виде ежегодного объектового контроля

В.3.1 Контроль организуется подразделением по защите информации организации — владельца АС (оператора информационной системы) и осуществляется организацией, имеющей лицензию уполномоченного федерального органа исполнительной власти (в части осуществления мероприятий по контролю защищенности информации).

В.3.2 К проведению контроля привлекаются сотрудники, ответственные за эксплуатацию аттестованной АС и, при необходимости, сотрудники режимно-секретного подразделения (подразделения, отвечающего за обеспечение безопасности информации ограниченного доступа) организации.

В.3.3 В ходе проведения контроля осуществляются следующие мероприятия:

- в соответствии с Д.2, Д.3.1, Д.3.2 и Д.3.7 (приложение Д) на основе анализа материалов аттестационных испытаний проверяется неизменность условий эксплуатации АС и правильность ведения документации на АС;
- в соответствии с Д.4.1, Д.4.3 и Д.4.5 (приложение Д) проверяется выполнение требований по защите информации от утечки за счет ПЭМИН;
- в соответствии с Д.6.3, Д.6.5, Д.6.6 и Д.6.7 (приложение Д) проверяется выполнение требований по защите информации от НСД.

В.3.4 По результатам контроля непосредственно на проверяемой АС представителями организации, проводящей работы по контролю, и представителями собственника АС (оператора информационной системы) составляется в двух экземплярах двусторонний акт о проведенных при контроле работах и выявленных нарушениях, влияющих на безопасность информации (или их отсутствии).

В.3.5 Материалы контроля аттестованной АС оформляются организацией, проводящей работы по контролю, в виде заключения по результатам контроля защищенности информации и выдаются владельцу проверяемой АС (оператору информационной системы).

К заключению по результатам контроля защищенности информации с учетом выполненных проверок прилагают:

- протокол контроля системы защиты информации от несанкционированного доступа (в части проверки соответствия контрольных сумм и действительности сертификата, неизменности установленного программного обеспечения и актуальности антивирусных баз данных);
- протокол контроля защищенности информации от утечки за счет ПЭМИН (при отсутствии на АС СЗИ от утечки за счет ПЭМИН проверяется неизменность условий эксплуатации);
- протокол оценки эффективности принятых мер защиты информации от утечки за счет ПЭМИН (при наличии на АС СЗИ от утечки за счет ПЭМИН проверяется эффективность применения СЗИ и действительность их сертификатов).

Приложение Г
(рекомендуемое)

Типовая программа аттестационных испытаний выделенных (защищаемых) помещений

Г.1 Аттестационные испытания ВП (ЗП) проводятся в соответствии с программой, включающей следующий перечень работ и порядок их проведения.

Г.1.1 Проверка структуры, состава и условий эксплуатации ВП (ЗП), включающая:

- анализ полноты исходных данных;
- проверку соответствия исходных данных фактическим условиям размещения, монтажа и эксплуатации технических средств, установленных в ВП (ЗП).

Г.1.2 Проверка состояния организации работ и выполнения требований по защите информации, включающая:

- проверку правильности категорирования ВП;
- проверку достаточности представленных документов и соответствия их содержания установленным требованиям;
- проверку наличия сертификатов соответствия требованиям безопасности информации и (или) предписаний на эксплуатацию для всех технических средств и систем, установленных в ВП (ЗП);
- проверку уровня подготовки специалистов, обеспечивающих защиту информации в ВП (ЗП), и наличия распределения ответственности должностных лиц, эксплуатирующих данные объекты, за выполнение требований безопасности информации.

Г.1.3 Проведение испытаний ВП (ЗП) на соответствие требованиям по защите акустической речевой информации от утечки по техническим каналам.

Г.1.4 Подготовка отчетной документации и оценка результатов испытаний аттестуемых ВП (ЗП).

Г.1.4.1 Результаты проведения испытаний ВП (ЗП) на соответствие требованиям по защите информации от утечки по техническим каналам отражаются в протоколе инструментальной проверки выполнения требований по защите информации от акустической речевой разведки.

Г.1.4.2 Материалы аттестационных испытаний оформляются протоколом испытаний, содержащим:

- наименование аттестуемого объекта;
- цель испытаний;
- перечень использованных нормативных документов и методик испытаний;
- перечень средств измерений;
- описание проверок;
- результаты испытаний.

Г.1.4.3 На основании данных документов составляется заключение по результатам аттестационных испытании, содержащее:

- оценку соответствия ВП (ЗП) требованиям безопасности информации;
- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- вывод о возможности (невозможности) выдачи «Аттестата соответствия».

Г.2 Продолжительность работ по пунктам «Программы аттестационных испытаний» на каждое ВП (ЗП) составляет:

- по Г.1.1, Г.1.2 — до__дней;
- по Г.1.3 — до__дней;
- по Г.1.4 — до__дней.

Примечание —Продолжительность работ определяется исходя из размеров помещения, количества установленных в помещении технических средств и сложности построения системы защиты информации.

Г.3 Контроль соответствия системы защиты информации аттестованных ВП (ЗП) требованиям безопасности в процессе эксплуатации проводится в виде ежегодного объектового контроля.

Г.3.1 Контроль организуется подразделением по защите информации организации — владельца ВП (ЗП) и осуществляется организацией, имеющей лицензию уполномоченного федерального органа исполнительной власти (в части осуществления мероприятий по контролю защищенности информации).

Г.3.2 К проведению контроля привлекаются сотрудники, ответственные за эксплуатацию аттестованного ВП (ЗП) и, при необходимости, сотрудники режимно-секретного подразделения (подразделения, отвечающего за обеспечение безопасности информации в организации).

Г.3.3 В ходе проведения контроля осуществляются следующие мероприятия:

- в соответствии с Е.2.1 и Е.2.2 (приложение Е) на основе анализа материалов аттестационных испытаний проверяется неизменность условий эксплуатации ВП (ЗП) и выполнение требований предписаний на эксплуатацию установленных в нем технических средств;

- в соответствии с Е.3.3, Е.3.4 и Е.3.5 (приложение Е) проверяется выполнение требований по защите речевой информации от ее утечки по акустическому и вибрационному каналам (инструментальные измерения характеристик ограждающих конструкций и инженерно-технических коммуникаций и оценка эффективности применяемых мер по защите речевой информации).

Г.3.4 По результатам контроля представителями организации, осуществляющей работы по контролю, и представителями собственника ВП (ЗП) составляется в двух экземплярах двусторонний акт о проведенных работах и выявленных нарушениях, влияющих на безопасность информации (или об их отсутствии).

Г.3.5 Материалы контроля аттестованного ВП (ЗП) оформляются организацией, осуществляющей работы по контролю, в виде заключения по результатам контроля защищенности информации и выдаются собственнику проверяемого ВП (ЗП).

К заключению по результатам контроля защищенности информации с учетом выполненных проверок прилагают:

- протокол инструментальной проверки выполнения требований по противодействию акустической речевой разведке (для ВП);

- протокол инструментальной проверки защищенности помещения от утечки речевой конфиденциальной информации (для ЗП).

Приложение Д
(рекомендуемое)

Типовые методики аттестационных испытаний автоматизированной системы

Д.1 Общие положения

Д.1.1 Настоящие методики предназначены для проведения аттестационных испытаний АС *(название организации-заявителя)*[1] на соответствие требованиям безопасности информации.

Д.1.2 Аттестационные испытания проводятся в указанном ниже порядке и включают:

- анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации АС, исследование технологического процесса обработки, хранения и передачи информации, анализ информационных потоков, определение состава использованных для обработки, хранения и передачи информации ОТСС;
- проверку состояния организации работ и выполнения требований по защите информации, оценку правильности категорирования и классификации АС, оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации, оценку уровня подготовки специалистов, обеспечивающих защиту информации в АС и распределения ответственности пользователей АС за выполнение требований безопасности информации;
- проверку АС на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений от ОТСС и наводок информативных сигналов на цепи электропитания и заземления ОТСС, а также наводок информативных сигналов на ВТСС и их кабельные коммуникации, имеющие выход за границу контролируемой зоны;
- проверку выполнения требований по защите АС от утечки информации за счет возможно внедренных электронных закладочных устройств в технические средства иностранного производства;
- проверку АС на соответствие требованиям по защите информации от НСД;
- проверку АС на соответствие требованиям по защите информации от специальных программных воздействий на нее и ее носители;
- подготовку отчетной документации.

Д.2 Анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации автоматизированной системы, исследование технологического процесса обработки, хранения и передачи информации, анализ информационных потоков, определение состава использованных для обработки, хранения и передачи информации основных технических средств и систем

Д.2.1 Аттестационной комиссии должны быть представлены:

- перечень защищаемых информационных ресурсов с документальным подтверждением степени секретности (уровня конфиденциальности) каждого ресурса;
- акт категорирования ОТСС (для АС, предназначенной для обработки секретной информации);
- акт классификации АС по требованиям защиты информации от НСД (в соответствии с нормативными правовыми актами и методическими документами уполномоченного федерального органа исполнительной власти и национальными стандартами);
- оформленный технический паспорт на АС;
- предписания на эксплуатацию ОТСС и протоколы специальных исследований ОТСС (для АС, предназначенной для обработки секретной информации);
- акты или заключения о специальной проверке ОТСС (для АС, предназначенной для обработки секретной информации);
- сертификаты соответствия требованиям безопасности информации на программные и технические средства АС, используемые средства защиты;
- состав технических и программных средств, входящих в АС;
- план размещения ОТСС и ВТСС в помещении объекта информатизации;
- план КЗ *(название организации-заявителя)*;
- схемы прокладки линий передачи данных ОТСС (ВОСП) и проводных линий ВТСС;
- схемы и характеристики систем электропитания и заземления ОТСС и ВТСС;
- состав и схемы размещения средств защиты информации;
- организационно-распорядительная документация разрешительной системы доступа пользователей АС к защищаемым информационным ресурсам АС;
- описание технологического процесса обработки информации в АС;

---

[1] Здесь и далее в приложении Д курсивом в скобках выделены данные, относящиеся к аттестационным испытаниям конкретного ОИ.

- перечень программного обеспечения, установленного в АС
- инструкции администратору защиты информации и пользователям АС;
- инструкции по эксплуатации средств защиты информации;
- данные о наличии нормативной и методической документации по защите информации и контролю эффективности защиты;
- данные по уровню подготовки специалистов, обеспечивающих защиту информации.

Приведенный перечень исходных данных и документации при необходимости может уточняться по результатам анализа и проверки в зависимости от особенностей АС по согласованию с аттестационной комиссией.

Д.2.2 При исследовании технологического процесса автоматизированной обработки и хранения информации проверяют:

- объект доступа — средства обработки и передачи информации, носители информации на магнитной и бумажной основе, накопители и все виды памяти ЭВМ, которые могут содержать информацию, отдельные документы и их архивы, используемые в технологическом процессе обработки информации, файлы, записи и другие информационные ресурсы, доступ к которым необходимо регламентировать;
- субъект доступа — пользователи АС, а также программные средства, посредством которых осуществляется доступ к объектам доступа.

Д.2.3 Используя разрешительную систему доступа пользователей АС к защищаемым информационным ресурсам и данные по технологии обработки и передачи защищаемой информации, анализируют обобщенную технологическую схему АС с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

Д.2.4 Проверяют соответствие описания технологического процесса обработки, хранения и передачи защищаемой информации реальному технологическому процессу обработки.

Д.2.5 Проверяют паспортные (исходные) данные АС, комплектность и характеристики средств защиты и устанавливают угрозы безопасности информации в АС, уязвимые критические места АС, снижающие уровень ее защиты.

Д.2.6 Проверяют наличие оформленных разрешений на допуск пользователей АС к информации, соответствие им грифов секретности (уровня конфиденциальности) на носителях информации, соответствие инструкций пользователей и администратора защиты информации АС установленным требованиям.

Д.2.7 По результатам исследований уточняют схему технологического процесса в отношении отдельных средств обработки и передачи информации и каждого пользователя АС.

Д.3 Проверка состояния организации работ и выполнения требований безопасности информации

Д.3.1 *Проверка соответствия содержания представленных документов установленным требованиям*

Проверяют соответствие представленных документов требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также стандартов и иных документов органов государственного управления в пределах компетенции.

Проверяют соответствие приведенных в представленных документах сведений о составе АС (типы, заводские номера, места размещения и т. д.) ее реальному составу.

Проверка считается успешной, если представленные документы полностью соответствуют требуемому составу, не содержат противоречивых сведений и оформлены в соответствии с установленными требованиями.

Д.3.2 *Проверка соответствия состава и структуры программно-технических средств АС представленной документации*

С представленной документацией сверяют состав и структуру программно-технических средств АС, включенных в реальный технологический процесс обработки информации.

С использованием стандартных средств операционной системы или других программ фиксируют перечень технических и программных средств и сверяют с приведенным в техническом паспорте, документах разрешительной системы доступа и описании технологического процесса обработки защищаемой информации.

Проверка считается успешной, если состав, номенклатура, структура программно-технических средств АС и их размещение полностью соответствуют представленной документации на АС.

Д.3.3 *Проверка правильности категорирования ОТСС (для АС, предназначенной для обработки секретной информации)*

Проверку проводят на основании исходных данных о максимальной степени секретности обрабатываемой информации, которые должны быть подтверждены документально в перечне защищаемых информационных ресурсов АС.

По результатам проверки определяют допустимые категории технических средств. Эти категории сравнивают с категориями, указанными в актах категорирования соответствующих технических средств.

Д.3.4 *Проверка правильности классификации АС*

Определяют максимальную степень секретности (конфиденциальности) обрабатываемой в АС информации, анализируют уровни полномочий по доступу к секретной (конфиденциальной) информации различных пользователей АС, режимы обработки данных в АС и устанавливают класс АС в соответствии с нормативными правовыми актами и методическими документами уполномоченного федерального органа исполнительной власти и национальными стандартами.

Проверка считается успешной, если класс аттестуемой АС соответствует представленному на аттестационные испытания акту классификации автоматизированной системы.

Д.3.5 *Проверка уровня подготовки специалистов и распределения ответственности пользователей АС*

Проверку проводят на основе следующих показателей:

- оценка знания инструкций по безопасности информации пользователями АС;
- наличие системы распределения ответственности пользователей АС за выполнение требований безопасности информации.

На основании опроса пользователей АС проверяют знание ими руководящих документов и инструкций.

Проводят выборочную проверку персонала из каждой категории организационно-штатной структуры АС на предмет владения технологиями безопасной обработки информации и знания соответствующих инструкций.

Проверяют организацию обучения и повышения квалификации пользователей АС.

Проверка считается успешной, если уровень подготовки пользователей АС обеспечивает выполнение требований безопасности информации.

Д.3.6 *Экспертиза протоколов специальных исследований и предписаний на эксплуатацию технических средств и систем*

Проверяют соответствие содержания и оформления протоколов специальных исследований и предписаний на эксплуатацию технических средств и систем установленным требованиям.

Проверка считается успешной при выполнении всех установленных требований.

Д.3.7 *Проверка выполнения требований к помещениям, в которых производится обработка информации*

Внешним осмотром проверяют соответствие помещения АС установленным к нему требованиям.

Проверяют выполнение установленных требований действующей инструкции по обеспечению режима секретности.

Проверяют выполнение установленных требований по условиям размещения ОТСС внутри помещения. Размещение ОТСС должно исключать возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

Проверка считается успешной при выполнении всех установленных требований.

Если ОТСС размещены в ВП (ЗП), то проверяют документы, подтверждающие отсутствие дополнительных каналов утечки акустической речевой информации за счет использования этих средств.

Д.3.8 По результатам проверок аттестационная комиссия делает выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям.

Д.4 Проверка автоматизированной системы на соответствие требованиям по защите информации от ее утечки по техническим каналам за счет побочных электромагнитных излучений и наводок

Д.4.1 *Проверка выполнения требований по защите информации от утечки за счет побочных электромагнитных излучений средств вычислительной техники*

Д.4.1.1 Проверка соответствия фактических размеров КЗ представленным документам

Проверяют соответствие размеров КЗ в представленных документах ее фактическим размерам. Определяют минимальное значение расстояния от источника информативных сигналов до границы КЗ.

Д.4.1.2 Проверка соответствия размеров КЗ требованиям предписаний на эксплуатацию ОТСС и других документов, определяющих требования к размеру зоны 2

Сравнивают требуемое значение расстояния (размера зоны 2), указанного в предписании на эксплуатацию ОТСС, с фактическим наименьшим значением расстояния до границы КЗ ($R_{кз}$). Опасными режимами работы ОТСС считаются такие, для которых не обеспечивается условие $R2 < 0{,}71R_{кз}$.

Д.4.1.3 Проверка средств защиты информации

В ходе проверки устанавливают:

- соответствие видов и типов установленных средств защиты (средств активной защиты, экранирующих конструкций, фильтров) тем, которые указаны в предписаниях на эксплуатацию технических средств;
- наличие сертификатов соответствия на средства защиты и знаков соответствия;
- выполнение правил монтажа и эксплуатации средств защиты.

Применяемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации. Проверяют наличие сертификатов соответствия на средства защиты информации, подтверждающих возможность применения этих средств для защиты информации от ее утечки за счет побочных электромагнитных излучений. Сертификаты должны быть выданы уполномоченными ФОИВ и подтверждены знаками соответствия. Действие сертификатов не должно быть просрочено на момент проведения аттестационных испытаний.

Д.4.1.4 Испытания (с использованием технических средств) с целью проверки защищенности информации от утечки за счет побочных электромагнитных излучений ОТСС

Испытания проводят при использовании на АС средств активной защиты информации. При этом оценивается эффективность принятых мер по защите информации от утечки за счет побочных электромагнитных излучений в соответствии с методическими документами федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

Д.4.2 По результатам проверки аттестационная комиссия делает выводы о выполнении требований по защите информации от утечки за счет побочных электромагнитных излучений средств вычислительной техники.

Примечание — АС с линиями ВОСП, выходящими за границу КЗ, дополнительно проверяются на соответствие требованиям по защите информации от утечки по оптическому каналу в соответствии с требованиями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти.

Д.4.3 *Проверка выполнения требований по защите информации от утечки за счет наводок информативных сигналов на цепи электропитания и заземления ОТСС*

Д.4.3.1 Проверка выполнения требований к электропитанию технических средств

Проверяют выполнение установленных требований к схеме электропитания технических средств:

- размещение трансформаторной подстанции;
- монтаж фидерных линий, их экранирование и фильтрация;
- монтаж средств активной защиты и сетевых фильтров.

Д.4.3.2 Проверка выполнения требований к заземлению технических средств

Проверяют:

- правильность размещения заземляющего устройства;
- наличие протоколов измерения величины сопротивления току растекания заземляющего устройства;
- отсутствие соединений системы заземления с металлоконструкциями, выходящими за пределы КЗ.

Д.4.3.3 Проверка средств защиты информации (проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации) — по Д.4.1.3.

Д.4.3.4 Испытания (с использованием технических средств) с целью проверки эффективности защиты информации от утечки по цепям заземления и электропитания технических средств проводят в случае невыполнения установленных требований к системам электропитания и заземления, а также при использовании на АС средств активной защиты информации. При этом оценивается эффективность принятых мер по защите информации от утечки за счет наводок информативных сигналов на цепи электропитания и заземления ОТСС в соответствии с методическими документами федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

Д.4.4 По результатам проверки аттестационная комиссия делает выводы о выполнения требований по защите информации от утечки за счет наводок информативных сигналов на цепи электропитания и заземления ОТСС.

Д.4.5 *Проверка выполнения требований по защите информации от утечки за счет наводок информативных сигналов на ВТСС и их кабельные коммуникации, имеющие выход за границу КЗ*

Д.4.5.1 Проверяют взаимное размещение ОТСС и ВТСС на соответствие требованиям предписаний на эксплуатацию технических средств и других документов, определяющих размеры зон 1 и 1'.

Проверяют выполнение требований по удалению ВТСС, линии которых имеют выход за пределы КЗ, от ОТСС на расстояния не менее, чем r1 и r1', где r1 и r1' — допустимые расстояния, определяемые предписаниями на эксплуатацию технических средств.

Д.4.5.2 Проверка средств защиты информации (проверка выполнения правил монтажа и эксплуатации средств защиты информации) — по Д.4.1.3.

Д.4.5.3 Испытания (с использованием технических средств) с целью проверки защищенности информации от утечки за счет наводок на ВТСС и их кабельные коммуникации проводят в случае не выполнения требований предписаний на эксплуатацию ОТСС и (или) при использовании на объекте вычислительной техники средств активной защиты информации. При этом оценивают эффективность принятых мер по защите информации от утечки за счет ПЭМИН в соответствии с методическими документами федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

Д.4.6 По результатам проверки аттестационная комиссия делает выводы о выполнения требований по защите информации от утечки за счет наводок информативных сигналов на ВТСС и их кабельные коммуникации, имеющие выход за границу КЗ.

Д.5 Проверка выполнения требований по защите основных технических средств и систем от утечки информации за счет возможно внедренных в них электронных закладочных устройств

Проверяется наличие актов или заключений о специальной проверке ТСИП, входящих в состав АС, наличие специальных голографических меток на проверенных средствах. Если в документах о специальной проверке указаны номера этих меток, то проводится проверка соответствия номеров.

Д.6 Испытания автоматизированной системы на соответствие требованиям по защите информации от несанкционированного доступа

Д.6.1 Испытания проводятся на соответствие требованиям руководящих документов [1] и [2]. По результатам испытаний аттестационная комиссия делает выводы о выполнении требований по защите информации от НСД.

Д.6.2 *Проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации*

Проверяют соответствие представленных сертификатов установленным (используемым) в АС средствам защиты информации от НСД. Основным инструментальным средством аттестационных испытаний на данном этапе является программа фиксации и контроля исходного состояния *(наименование программы)*. Программа используется в режиме фиксации исходного состояния файлов программного комплекса. При этом рассчитывают контрольные суммы для указанных в формуляре (паспорте) программных модулей СЗИ от НСД. Расчет производят по алгоритму формирования имитовставки в соответствии с ГОСТ 28147 или по контрольным суммам другого аттестованного алгоритма. Полученные значения контрольного суммирования сравнивают со значениями, указанными в формуляре (паспорте) средства защиты информации.

Проверка считается успешной:

- если действующие сертификаты соответствуют требованиям безопасности информации на все используемые в АС средства защиты информации от НСД;
- если используемое СЗИ от НСД соответствует классу АС и используемой технологии обработки информации;
- если результаты контрольного суммирования программных модулей СЗИ от НСД полностью соответствуют значениям, указанным в формуляре (паспорте) данного средства защиты.

Д.6.3 *Проверка соответствия описания технологического процесса обработки и хранения защищаемой информации реальному процессу*

Д.6.3.1 Заявитель представляет аттестационной комиссии описание технологического процесса обработки информации в аттестуемой АС, которое включает:

- перечень объектов и субъектов доступа;
- перечень штатных средств доступа к информации в АС;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков в АС.

В качестве объектов доступа могут быть приняты:

- система в целом;
- терминалы, ЭВМ, узлы сети ЭВМ, каналы связи, внешние устройства ЭВМ;
- программы;
- тома, каталоги, файлы, записи, поля записей.

Носители информации должны иметь гриф секретности (метку конфиденциальности) и находиться на учете.

В качестве субъектов доступа могут рассматриваться лица и процессы (программы пользователей), имеющие возможность доступа к штатными средствами АС. Субъекты доступа должны иметь официальное разрешение на доступ к информации определенной степени секретности (уровня конфиденциальности).

Примечание — Под штатными средствами АС понимаются общесистемные и прикладные системы, средства и программы, предоставляющие субъектам документированные возможности доступа к объектам доступа.

Д.6.3.2 Аттестационная комиссия проверяет:

- соответствие технологического процесса обработки и хранения защищаемой информации требованиям безопасности информации;
- соответствие описания технологического процесса обработки и хранения защищаемой информации реальному процессу.

Д.6.4 *Испытания подсистемы управления доступом*

Д.6.4.1 Для проведения испытаний требуются следующие средства:

- загрузочная дискета операционной системы (MS DOS, DR DOS, Unix и т. д.);
- загрузочный компакт-диск (CD);
- программа фиксации и контроля исходного состояния;
- средство контроля защищенности АС от НСД *(наименование средства)*.

Д.6.4.2 Проверка подсистемы идентификации и аутентификации субъектов доступа

Д.6.4.2.1 Проверка наличия и работоспособности подсистемы идентификации

Проверяют правильность идентификации субъектов доступа путем обращения субъектов доступа АС к объектам доступа при помощи штатных средств.

При обращении должна проводиться проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных в АС идентификаторов. Если субъект доступа предъявляет идентификатор, не известный подсистеме идентификации, то средства управления должны прекращать процесс предоставления доступа.

Д.6.4.2.2 Проверка наличия и надежности подсистемы аутентификации

Проверяют правильность аутентификации субъекта доступа. Если субъект доступа предъявляет пароль, не соответствующий идентификатору субъекта, то средства управления должны прекращать процесс предоставления доступа.

Проверяют возможность компрометации пароля методом его подбора. Для АС, где подсистема аутентификации предусматривает средства, обеспечивающие блокировку подбора пароля. Проверку осуществляют следующим образом. Выполняют неоднократные попытки ввода неверного пароля. При превышении предельного числа попыток ввода информации идентификации/аутентификации, установленного политикой безопасности, подсистема управления доступом должна полностью блокировать ввод информации идентификации/аутентификации субъекта доступа. Правом снятия блокировки должен обладать исключительно администратор (служба) защиты информации в АС.

Д.6.4.2.3 Проверка отсутствия условий компрометации подсистемы идентификации и аутентификации

Проверяют условия хранения, выдачи, использования устройств и информации об идентификации и аутентификации. Организационные и технические мероприятия АС должны надежно препятствовать несанкционированному получению или хищению устройств и информации об идентификации и аутентификации.

Проверяют возможность несанкционированного изменения информации об идентификации и аутентификации. Доступ субъектов АС к файлам, содержащим информацию об идентификации и аутентификации, должен быть полностью закрыт для прикладных программ. На СВТ, входящих в состав АС, должны отсутствовать прикладные программные средства прямого доступа к устройствам и оперативной памяти, средства разработки и отладки программ.

Д.6.4.2.4 Проверка средств загрузки операционной системы АС в обход подсистемы идентификации и аутентификации

Для проведения испытаний необходимы загрузочная дискета и загрузочный CD.

Осуществляют попытки загрузки операционной системы с загрузочной дискеты и загрузочного CD. Настройка СЗИ от НСД АС должна обеспечивать блокировку загрузки операционной системы с устройств, не предусмотренных технологией инициализации АС.

Д.6.4.2.5 Проверка времени действия пароля

На ЭВМ производят перевод системного времени вперед, при этом не превышая установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему. Подсистема идентификации и аутентификации должна разрешить вход пользователя в систему, но соответствующим сообщением предупредить его о необходимости замены пароля.

На ЭВМ производят перевод системного времени вперед на интервал, больший установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему. Подсистема идентификации и аутентификации должна блокировать вход пользователя в систему.

После проведения испытаний на ЭВМ устанавливают текущее время.

Д.6.4.2.6 Проверка длины пароля

Подсистема контроля доступа должна предусматривать средства, обеспечивающие установку минимальной длины пароля. Проверку осуществляют попыткой смены длины пароля субъектом доступа. Проверка считается успешной, если подсистема контроля доступа отказала субъекту в замене пароля.

Право установки минимальной размерности пароля должно предоставляться администратору АС.

Д.6.4.3 Проверка подсистемы идентификации объектов доступа

Д.6.4.3.1 Проверка идентификации аппаратурных объектов доступа

Идентификация внешних устройств ЭВМ должна осуществляться по одному из ниже перечисленных типов идентификаторов:

- по логическим адресам (номерам);
- по логическим именам;
- по логическим именам и (или) адресам;
- по физическим адресам (номерам);
- по уникальным встроенным устройствам.

Основными средствами проверки являются средства контроля защищенности АС от НСД *(наименования средств)*. С их помощью производится сканирование периферийных устройств ЭВМ (принтеров, НГМД, приводов CD-ROM), доступных для пользователя. Перед началом сканирования в настройках этих средств контроля необходимо задать поиск неизвестных устройств.

Проверка считается успешной, если во время работы со средствами контроля защищенности АС от НСД *(наименования средств)* не выявлены неизвестные (неидентифицированные) объекты доступа.

Д.6.4.3.2 Проверка идентификации информационных объектов доступа

Проверяют механизм подсистемы контроля доступа, обеспечивающий проверку идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

Основными средствами проверки являются средства контроля защищенности АС от НСД *(наименования средств)*.

С помощью средств контроля защищенности АС от НСД *(наименования средств)* проводится сканирование ресурсов файловой системы АС (логических дисков, каталогов, файлов), доступных для пользователя. Перед началом сканирования в настройках комплекса необходимо задать поиск неизвестных устройств.

Проверка считается успешной, если в выходном отчете комплексов средств контроля не будут указаны неизвестные (неидентифицированные) объекты доступа.

Д.6.4.4 Проверка подсистемы управления потоками информации

Д.6.4.4.1 Основными средствами аттестационных испытаний на данном этапе являются средства контроля защищенности АС от НСД *(наименования средств)*, средства операционной системы.

Д.6.4.4.2 Для проведения проверки подсистемы управления потоками информации необходимо проанализировать матрицу доступа. При этом классификационные категории должны быть объединены в иерархические группы, по которым строятся комбинации иерархических и неиерархических категорий, — классификационные уровни. Каждому классификационному уровню должна соответствовать уникальная классификационная метка.

Классификационные метки, как основа мандатного принципа доступа, должны присваиваться каждому объекту и отражать место данного объекта в соответствующей иерархии.

Разработка модели подсистемы разграничения доступа с помощью средства контроля защищенности АС от НСД *(наименование средства)* должна осуществляться в полном соответствии с политикой безопасности и матрицей доступа, учитывающей мандатные правила разграничения доступа, принятые в аттестуемой АС.

Проверка считается успешной, если в АС осуществляется управление потоками информации с помощью меток, соответствующих степени секретности (уровню конфиденциальности). При этом гриф секретности (уровень конфиденциальности) накопителей должен быть не ниже грифа секретности (уровня конфиденциальности) записываемой на них информации.

Д.6.4.4.3 Проверяется настройка СЗИ от НСД в части назначения объектам меток, соответствующих степеням секретности (уровням конфиденциальности) ресурсов. С использованием штатных средств операционной системы осуществляются попытки переноса информации на носитель с другим грифом секретности (уровнем конфиденциальности).

Проверка считается успешной, если СЗИ от НСД запретила операцию копирования.

Д.6.5 *Испытания подсистемы регистрации и учета*

Д.6.5.1 Для проведения испытаний необходимы:

- программа фиксации и контроля исходного состояния *(наименование программы)*;
- программа поиска информации на дисках *(наименование программы)*.

Регистрация и учет событий должны проводиться на всех этапах технологического процесса хранения и обработки защищаемой информации.

Д.6.5.2 Испытания включают:

- проверку регистрации начала и окончания работ;
- проверку регистрации выдачи документов на «твердую» копию;
- проверку регистрации использования программных средств;
- проверку регистрации доступа программных средств к защищаемым файлам;
- проверку регистрации доступа программных средств к дополнительным защищаемым объектам доступа;
- проверку автоматического учета создания новых объектов доступа;
- проверку учета защищаемых носителей информации;
- проверку очистки освобождаемых областей памяти.

Д.6.5.3 Проверка регистрации начала и окончания работ

Проверка осуществляется штатными средствами АС.

Проводится загрузка операционной системы и запуск программных комплексов АС, предусмотренных технологией инициализации АС.

Осуществляются попытки входа в систему по неверному идентификатору доступа, по верному идентификатору доступа и неверному паролю, по идентификатору и паролю легитимного субъекта доступа.

Производится программный останов АС.

Производится загрузка операционной системы, запуск программных комплексов АС, предусмотренных технологией инициализации АС, вход в систему с правами администратора защиты и исследование журнала регистрации доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности АС, обеспечивается ведение журнала регистрации доступа (аппаратного журнала), в котором фиксируется регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. При этом регистрационные записи для каждого события должны содержать:

- дату и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная — несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.

Д.6.5.4 Проверка регистрации выдачи документов на «твердую» копию

В соответствии с принятой в АС технологией проводится выдача произвольного документа на «твердую» копию.

В соответствии с принятой в АС технологией проводится выдача документа иной степени секретности (уровня конфиденциальности) на «твердую» копию. Во время операции вывода документа на «твердую» копию проводится принудительное отключение электропитания устройства вывода и выполняются действия, предусмотренные документацией АС для внештатных ситуаций.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности АС, обеспечивается регистрация выдачи документов на «твердую» копию. При этом регистрационные записи для каждого события должны содержать:

- дату и время выдачи документа (обращения к подсистеме вывода документа);
- спецификацию устройства выдачи (логическое имя внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и гриф секретности (уровень конфиденциальности) документа;
- идентификатор субъекта доступа, запросившего документ;

Выдача документов сопровождается автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц).

Д.6.5.5 Проверка регистрации использования программных средств

В соответствии с принятой в АС технологией производится запуск программ обработки информации и объектами обработки выбираются файлы, входящие в перечень защищаемых ресурсов.

Запуск программ производится как в штатном режиме, предусматривающем безаварийную (штатную) обработку информации и завершение работы, так и во внештатном. В последнем случае моделируется ситуация несанкционированного использования программы. При этом используют следующие приемы:

- задают неверные параметры обработки;
- задают в качестве объекта обработки несуществующий файл;
- делают попытки запустить программы, доступ к которым закрыт подсистемой разграничения доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности АС, была обеспечена регистрация запуска и завершения использованных на данном этапе испытаний программ и процессов (заданий, задач). При этом регистрационные записи для каждого события должны содержать:

- дату и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс);
- результат запуска (успешный, неуспешный — несанкционированный).

Д.6.5.6 Проверка регистрации доступа программных средств к защищаемым файлам

В соответствии с принятой в АС технологией производится запуск программ обработки информации и объектами обработки выбираются файлы, входящие в перечень защищаемых ресурсов.

Запуск программ производится как в штатном режиме, предусматривающем безаварийную (штатную) обработку информации и завершение работы, так и во внештатном. В последнем случае моделируется ситуация несанкционированного доступа к объектам защиты штатными программными средствами. При этом используют следующие приемы:

- задают неверные параметры обработки;
- задают в качестве объекта обработки несуществующий файл;
- задают в качестве объекта обработки файл, доступ к которому закрыт подсистемой разграничения доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности АС, была обеспечена регистрация попыток доступа использованных на данном этапе испытаний программных средств (программ, процессов, задач, заданий) к защищаемым файлам. При этом регистрационные записи для каждого события должны содержать:

- дату и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная;
- идентификатор субъекта доступа;
- спецификацию защищаемого файла.

Д.6.5.7 Проверка регистрации доступа программных средств к дополнительным защищаемым объектам доступа

Составляется список объектов испытаний. В список включаются объекты доступа, входящие в перечень защищаемых ресурсов, по одному (как минимум) для каждого из следующих типов:

- внешние устройства ЭВМ;
- программы;
- тома, каталоги, файлы;
- записи, поля записей.

В соответствии с принятой в АС технологией производится запуск программ, алгоритм работы которых предусматривает обращение к объектам, входящим в список объектов испытания.

Запуск программ производится как в штатном режиме, так и во внештатном. В последнем случае моделируется ситуация несанкционированного доступа к объектам защиты. При этом используют следующие приемы:

- задают неверные параметры запуска (обращения к устройствам);
- задают неверные логические имена (номера);
- осуществляют обращение к объекту, доступ к которому закрыт подсистемой разграничения доступа.

Проверка считается успешной, если средствами ЗИ обеспечивается регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к заданным на данном этапе испытаний дополнительным защищаемым объектам доступа. При этом регистрационные записи для каждого события должны содержать:

- дату и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная — несанкционированная;
- идентификатор субъекта доступа;
- спецификацию защищаемого объекта [логическое имя (номер)].

Д.6.5.8 Проверка автоматического учета создания новых объектов доступа

Субъект доступа, имеющий полномочия администратора защиты, создает новые объекты доступа, предусмотренные политикой безопасности АС. В качестве новых объектов доступа рассматриваются файлы защищаемой информации.

С помощью штатных средств подсистемы разграничения доступа осуществляется контроль маркирования вновь созданных объектов доступа и проверка соответствия маркировки степени секретности (уровню конфиденциальности). При создании субъектом нового объекта доступа подсистема регистрации и учета должна установить для данного объекта метку доступа (маркер), соответствующую минимальному уровню доступа субъекта по записи.

Проверка считается успешной:

- если подсистема регистрации и учета АС произвела автоматический учет создаваемых на данном этапе испытаний объектов доступа с помощью их дополнительной маркировки, используемой в подсистеме управления доступом;
- если маркировка отражает степень секретности (уровень конфиденциальности) объекта доступа.

Д.6.5.9 Проверка учета защищаемых носителей информации

Проверяется выполнение организационных и технических мероприятий по учету защищаемых носителей информации.

Проверка считается успешной, если организационно-технические мероприятия, проводимые в соответствии с политикой безопасности АС, обеспечивают:

- учет всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал (учетную карточку);
- учет защищаемых носителей в журнале (картотеке) регистрации их выдачи /приема;
- дополнительный (дублирующий) учет защищаемых носителей информации с регистрацией их выдачи / приема.

Д.6.5.10 Проверка очистки освобождаемых областей памяти

Д.6.5.10.1 Исследуются сертификаты (при необходимости — эксплуатационная документация) СЗИ на предмет подтверждения соответствия используемых методов очистки (обнуления, обезличивания) освобождаемых (перераспределяемых) областей оперативной памяти и внешних носителей требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

Проверка считается успешной, если сертификаты и эксплуатационная документация СЗИ подтверждают возможность выполнения очистки (обнуления, обезличивания) освобождаемых (перераспределяемых) областей оперативной памяти и внешних носителей двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Д.6.5.10.2 Проверка очистки внешней памяти при ее освобождении (перераспределении)

Основным средством проверки очистки внешней памяти при проведения аттестационных испытаний АС является программа *(наименование программы)*, которая используется для контроля очистки памяти при ее освобождении на внешних носителях информации посредством поиска задаваемых экспертом сигнатур. Объектами исследований являются накопители на гибких и жестких магнитных дисках. Поиск задают или по всему физическому диску, или в пределах логического диска. Область применения охватывает операционные среды MS Windows.

Проверка считается успешной:

- если контекст контрольной информации не был обнаружен на внешнем носителе;
- если сектора, которые ранее содержали контекст контрольной информации, заполнены маскирующей информацией.

Д.6.6 *Испытание подсистемы обеспечения целостности*

Д.6.6.1 Проверка организационно-штатных мероприятий по защите информации

Исследуется организационно-штатная структура и нормативная документация АС на предмет организации службы защиты информации АС.

Методом выборочного опроса проверяют знание должностными лицами службы защиты информации их функциональных обязанностей и оценивают уровень их профессиональной подготовки.

Проверка считается успешной:

- если организационно-штатная структура АС предусматривает наличие службы (администратора) защиты информации;
- если уровень профессиональной подготовки должностных лиц службы защиты информации обеспечивает выполнение требований безопасности информации в АС;
- если деятельность службы защиты информации регламентирована организационно-распорядительными документами АС.

Д.6.6.2 Проверка средств контроля целостности программных компонентов СЗИ НСД

Перед проведением проверки штатными средствами АС осуществляется резервное копирование программных компонентов СЗИ от НСД.

Производится моделирование несанкционированных действий по нарушению целостности программных компонентов СЗИ от НСД. Производится удаление либо переименование определенных программных модулей СЗИ от НСД.

Производится перезагрузка системы. По завершении инициализации СЗИ от НСД анализируется реакция средств подсистемы обеспечения целостности.

Проверка считается успешной, если СЗИ от НСД зафиксировали изменения в составе программных компонентов.

Д.6.6.3 Проверка тестирования функций СЗИ от НСД

Исследуется организационно-распорядительная документация АС, определяющая порядок проведения тестирования всех функций СЗИ от НСД, используемых в АС.

Проверяется наличие средств тестирования функций СЗИ от НСД, в частности настройка и использование средств диагностики СЗИ от НСД.

Проверяется периодичность проведения тестирования всех функций СЗИ от НСД. Проверка осуществляется методом экспертизы эксплуатационной документации и журналов регистрации событий СЗИ от НСД.

Проверка считается успешной, если средства тестирования всех функций СЗИ от НСД и периодичность проверок соответствуют требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации

Д.6.6.4 Проверка средств восстановления СЗИ от НСД

Исследуется организационно-распорядительная документация АС, определяющая порядок проведения резервного копирования СЗИ от НСД, используемого в АС.

Проверяется периодичность обновления и контроля работоспособности копий. Проверка осуществляется методом экспертизы эксплуатационной документации и журналов регистрации событий СЗИ от НСД.

Проверка считается успешной, если в АС осуществляется ведение двух копий программных СЗИ от НСД, а также производится периодическое обновление и контроль работоспособности копий.

Д.6.6.5 Проверка обеспечения целостности (неизменности) программной среды

Исследуется технология внесения новых программных средств в операционную среду АС. Технология должна содержать:

- процедуры экспертной оценки и верификации новых программных средств на предмет выявления потенциально опасных для СЗИ программных функций;
- критерии санкционирования ввода программ в операционную среду;
- критерии допуска определенных категорий пользователей к этим программам;
- порядок проведения антивирусного контроля программных комплексов АС.

Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду, средств антивирусного контроля.

Проверяется наличие установленных антивирусных средств на СВТ АС, а также их работоспособность, наличие механизма обновления и актуальность антивирусных баз, параметры их функционирования, наличие доверенного канала получения обновлений антивирусных баз.

Проводится экспертиза программного обеспечения АС на отсутствие:
- средств модификации объектного кода программ;
- средств разработки и отладки программ;
- программ, использование которых не требует трансляции с языков высокого уровня.

Проверка считается успешной, если принятые в АС меры обеспечения целостности (неизменности) программной среды соответствуют требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

Д.6.7 *Испытания подсистемы криптографической защиты (при ее наличии)*

Испытания проводятся в соответствии с нормативными правовыми актами и методическими документами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности.

Приложение Е
(рекомендуемое)

Типовые методики аттестационных испытаний выделенного (защищаемого) помещения

Е.1 Общие положения

Настоящие методики предназначены для проведения аттестационных испытаний выделенного (защищаемого) помещения *(название организации-заявителя)*[1] на соответствие требованиям безопасности информации.

Аттестационные испытания ВП (ЗП) включают:

- анализ полноты исходных данных, проверку их соответствия фактическим условиям размещения, монтажа и эксплуатации технических средств, установленных в ВП (ЗП), проверку состояния организации работ и выполнения требований по защите информации;
- проверку выполнения требований по защите ВП (ЗП) от утечки акустической речевой информации по акустическому и виброакустическому каналам;
- проверку ВП (ЗП) на соответствие требованиям по защите информации от утечки акустической речевой информации по проводным линиям и цепям ОТСС и ВТСС за счет акустоэлектрических преобразований и паразитной генерации;
- проверку выполнения требований по защите ВП от утечки информации за счет возможно внедренных электронных закладочных устройств;
- подготовку отчетной документации.

Е.2 Анализ полноты исходных данных, проверка их соответствия фактическим условиям размещения, монтажа и эксплуатации технических средств, установленных в выделенном (защищаемом) помещении, проверка состояния организации работ и выполнения требований по защите информации

Е.2.1 Аттестационной комиссии должны быть представлены:

- оформленный технический паспорт на ВП (ЗП);
- состав технических средств, установленных в ВП (ЗП);
- акт категорирования ВП;
- перечень защищаемых сведений с документальным подтверждением максимальной степени секретности (уровня конфиденциальности) обсуждаемых в ВП (ЗП) вопросов;
- состав и схема размещения средств защиты информации;
- инструкции по эксплуатации средств защиты информации;
- сертификаты соответствия требованиям безопасности информации на используемые средства защиты информации;
- план размещения ОТСС и ВТСС;
- предписания на эксплуатацию ОТСС и ВТСС;
- протоколы специальных исследований ОТСС и ВТСС;
- заключения о специальной проверке ТСИП, установленных в ВП;
- заключения о специальном обследовании помещения;
- план КЗ;
- схемы прокладки проводных линий ОТСС и ВТСС;
- схемы и характеристики систем электропитания и заземления;
- данные по уровню подготовки специалистов, обеспечивающих защиту информации;

Приведенный перечень исходных данных и документации может уточняться по результатам анализа и проверки в зависимости от особенностей аттестуемого ВП (ЗП) по согласованию с аттестационной комиссией.

Е.2.2 *Проверка состояния организации работ и выполнения требований по защите информации*

Е.2.2.1 Проводится проверка достаточности представленных документов и соответствия их содержания требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

Е.2.2.2 При проверке соответствия состава ОТСС и ВТСС представленной документации состав установленных в ВП (ЗП) технических средств сверяется с их перечнем в представленной документации.

Е.2.2.3 Проверка правильности категорирования ВП проводится на основании максимальной степени секретности обсуждаемых в ВП вопросов, что должно быть подтверждено документально в перечне сведений, содержащих государственную тайну, защищаемых в выделенном помещении.

Е.2.2.4 Проверка уровня подготовки специалистов, обеспечивающих защиту информации в ВП (ЗП), и распределения ответственности должностных лиц за выполнение требований безопасности информации проводится на основе следующих показателей:

---

[1] Курсивом выделены данные, относящиеся к аттестационным испытаниям конкретного ВП (ЗП).

- экспертной оценки знания нормативной и методической документации по защите информации и контролю эффективности защиты сотрудниками подразделения обеспечения безопасности информации;
- экспертной оценки знания инструкций по безопасности информации должностными лицами, эксплуатирующими ВП (ЗП).

Путем опроса должностных лиц, эксплуатирующих ВП (ЗП), проверяют доведение до сотрудников руководящих документов, необходимых инструкций, предписаний, актов, заключений.

Е.2.2.5 При проверке наличия СЗИ проверяют наличие документов (сертификатов соответствия), подтверждающих возможность применения средств защиты информации. Проводят экспертизу на соответствие требованиям нормативных документов протоколов специальных исследований и предписаний на эксплуатацию технических средств, установленных в ВП (ЗП).

В случае размещения технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, проверяют наличие сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях.

Е.2.2.6 Проводится проверка выполнения требований предписаний на эксплуатацию технических средств, установленных в ВП (ЗП).

Е.2.2.7 При проверке выполнения требований к ВП (ЗП) устанавливают их соответствие требованиям по обеспечению режима секретности (конфиденциальности).

Е.2.2.8 По результатам проверки аттестационная комиссия делает вывод о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям.

Е.3 Проверка выполнения требований по защите информации от утечки акустической речевой информации по акустическому и виброакустическому каналам

Е.3.1 Проверяют соответствие расположения и конструкций ВП (ЗП) требованиям безопасности информации от утечки по акустическому каналу и определяют места возможного перехвата акустических речевых сигналов за границей КЗ (разведопасные направления), в том числе места возможного непреднамеренного прослушивания в пределах КЗ.

Е.3.2. Проверяют соответствие расположения и конструкции ВП (ЗП) требованиям безопасности информации от утечки по виброакустическому каналу и определяют места возможного перехвата вибрационных сигналов, содержащих речевую информацию (места возможного применения разведаппаратуры, в том числе аппаратуры лазерного зондирования отражающих поверхностей).

Е.3.3 Проверка СЗИ, установленных в ВП (ЗП), проводится по следующим показателям:
- соответствие установленных в ВП (ЗП) средств защиты указанным в паспорте на ВП (ЗП);
- наличие сертификатов соответствия на средства защиты, установленные в ВП (ЗП);
- выполнение правил монтажа и эксплуатации средств защиты, установленных в ВП (ЗП);
- наличие актов ввода в эксплуатацию или протоколов проверки работоспособности средств защиты, установленных в ВП (ЗП).

Е.3.4 Испытания (с использованием технических средств) защищенности (эффективности защиты) информации от утечки по акустическому каналу проводят в местах возможного перехвата акустической речевой информации в соответствии с требованиями нормативных правовых актов и методических документов федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, а также требованиями документов по стандартизации в области защиты информации. При этом проверяют:
- для ВП — выполнение требований по противодействию акустической речевой разведке (для ВП);
- для ЗП — защищенность помещения от утечки речевой конфиденциальной информации.

Е.3.5 Испытания (с использованием технических средств) защищенности (эффективности защиты) информации от утечки по виброакустическому каналу проводят в местах возможного перехвата акустической информации, с учетом требований нормативных правовых актов и методических документов федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, а также требований документов по стандартизации в области защиты информации. При этом проверяют:
- для ВП — выполнение требований по противодействию акустической речевой разведке;
- для ЗП — защищенность помещения от утечки речевой конфиденциальной информации.

Е.4 Проверка выделенного помещения (защищаемого помещения) на соответствие требованиям по защите информации от утечки акустической речевой информации по проводным линиям и цепям основных и вспомогательных технических средств и систем за счет акустоэлектрических преобразований и паразитной генерации

Проверяется выполнение требований предписаний на эксплуатацию всех технических средств, установленных в ВП (ЗП), на предмет защищенности от утечки акустической речевой информации по проводным линиям и цепям ОТСС и ВТСС за счет акустоэлектрических преобразований и паразитной генерации.

Е.5 Проверка выполнения требований по защите выделенного помещения от утечки информации за счет внедренных электронных закладочных устройств

Проверяется наличие актов или заключений о специальной проверке ТСИП, установленных в ВП, и наличие специальных голографических меток на проверенных средствах. Если в документах о специальной проверке указаны номера этих меток, то проводится проверка соответствия номеров.

Для ВП первой категории проверяется наличие заключения по результатам специального обследования.

Библиография

[1] Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Гостехкомиссии России от 30.03.1992)

[2] Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утвержден решением председателя Гостехкомиссии России от 04.06.1999)

УДК 006.83:004.056 (083.74) ОКС 35.020 КС ОП 0043

Ключевые слова: объект информатизации, аттестация объектов информатизации, безопасность информации объекта информатизации, программа и методика проведения аттестационных испытаний

Редактор *Н. Л. Коршунова*
Редактор переиздания *А. В. Миронова*
Технический редактор *В. Н. Прусакова*
Корректор *С. И. Фирсова*
Компьютерная верстка *В. Н. Романовой*

Подписано в печать 02.02.2016. Формат 60×84 1/8. Бумага офсетная Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 4,25. Доп. тираж 153 экз. Зак. 1454.

Издано и отпечатано в ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
Набрано в Калужской типографии стандартов.