Аттестация объектов информатизации

Гр. ИТЗ – 410
Антипин Максим
Мурзин Юрий
Селяева Анастасия
Явтущенко Юлия

Документы:

- **ПЕРЕЧЕНЬ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ И НОРМАТИВНЫХ ДОКУМЕНТОВ, НА СООТВЕТСТВИЕ КОТОРЫМ ПРОВОДЯТСЯ АТТЕСТАЦИОННЫЕ ИСПЫТАНИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**
- Закон Российской Федерации "О государственной тайне". Постановление Верховного Совета РФ от 21.07.93 № 5485-1, № 5486-1.
- Закон Российской Федерации "Об информации, информационных технологиях и о защите информации". Принят Государственной Думой 08.07.2006, утвержден Президентом РФ 27.07.2006, N 149- ФЗ.
- Указ Президента Российской Федерации "О перечне сведений, отнесенных к государственной тайне". Указ Президента Российской Федерации от 24.01.1998, № 61.
- Правила отнесения сведений, составляющих государственную тайну, к различной степени секретности. Постановление Правительства Российской
  Федерации от 04.04.1995, № 870.
- Положение о подготовке к передаче сведений, составляющих государственную тайну, другим государствам. Постановление Правительства Российской Федерации от 02.08.1997, № 973.

- Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам. Постановление Совета Министров Правительства РФ от 15.09.1993, № 921 -51.
- Положение о сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26.06.1995, № 608.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Гостехкомиссии России 25.11.1994.
- Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР). Решение Гостехкомиссии России от 23 мая 1997 № 55, с изменениями и дополнениями (Извещения №№ 1-2005, 1-2006; 1-2008);
- Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Гостехкомиссия России, 1998.
- Сборник методических документов по контролю защищенности информации, обрабатываемой СВТ от утечки за счет ПЭМИН (новая редакция). ФСТЭК России, 2005.
- Сборник руководящих документов по защите информации от несанкционированного доступа (НСД). Гостехкомиссия России, 1998.

- РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей; Приказ Председателя Гостехкомиссии России от 04.06.99, № 114.
- РД. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Гостехкомиссия России, 2000.
- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации. Гостехкомиссия России, 2000.
- ОТТ 2.1.27-94. Общие требования к методам контроля за эффективностью защиты от иностранной технической разведки.
- ТТТ 1.2.8-89. Средства противодействия иностранной технической разведке. Общие тактико-технические требования.
- Нормативно-методические документы (НМД) по противодействию средствам иностранной радиотехнической разведки. Решение Гостехкомиссии СССР от 12.6.90, № 86-2.
- НМД по противодействию средствам иностранной фоторазведки и оптико-электронной разведки. Решение Гостехкомиссии СССР от 12.6.90, № 86-2.
- НМД по противодействию иностранной радиоразведке. Решение Гостехкомиссии России от 16.11.93, № 7.

- Сборник методик по оценке защищенности аппаратуры и объектов АСУ от утечки информации за счет побочных электромагнитных излучений и наводок. МРП СССР, 1985.
- Порядок контроля защищенности объектов от разведки побочных электромагнитных излучений. Гостехкомиссия СССР, 1989.
- ГОСТ 24.104-85. Автоматизированные системы управления. Общие требования.
- ГОСТ 28806-90. Качество программных средств. Термины и определения.
- ГОСТ 29339-92. Защита информации от утечки за счет ПЭМИН. Общие технические требования,
- ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
- ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
- ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания.
- ГОСТ 34.603-92. Виды испытаний автоматизированных систем.

- ГОСТ РВ 50170-92. Противодействие иностранной технической разведке. Термины и определения.
- ГОСТ РВ 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения.
- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
- ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.
- ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
- ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
- ГОСТ Р 51275-99. Защита информации. Объект информатизации Факторы, воздействующие на информацию. Общие положения.

1. Общие положения

- Под аттестацией объекта информатизации (ОИ) понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией РФ. Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

- **Обязательной** аттестации подлежат ОИ, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

  В остальных случаях аттестация носит **добровольный** характер.
- При аттестации ОИ подтверждается его соответствие требованиям по защите информации от НСД, в том числе от компьютерных вирусов, от утечки за счет ПЭМИН при специальных воздействиях на объект, от утечки или воздействия на нее за счет специальных устройств, встроенных в ОИ.
- Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого ОИ в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации

2. Организационная структура системы аттестации ОИ

- Организационную структуру системы аттестации ОИ образуют:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - Гостехкомиссия России;

- органы по аттестации ОИ;

- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;

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

- Органы по аттестации ОИ аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации ОИ.
- Органы по аттестации:

- аттестуют ОИ и выдают "Аттестаты соответствия";

- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных ОИ, и за их эксплуатацией;

- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов ОИ, участвуют в их разработке;

- ведут информационную базу аттестованных этим органом ОИ;

- осуществляют взаимодействие с Гостехкомиссией России и ежеквартально информируют его о своей деятельности в области аттестации.

- Орган по аттестации несет ответственность за:
  - соответствие проведенных им аттестационных испытаний ОИ требованиям стандартов и иных нормативных и методических документов по безопасности информации, а также достоверность и объективность их результатов;
  - полноту и качество выполнения функций и обязанностей, возложенных на него;
  - формирование и квалификацию аттестационных комиссий;
  - соблюдение требований нормативных и методических документов, предъявляемых к порядку проведения аттестования;
  - соблюдение установленных сроков и условий проведения аттестации, зафиксированных в договоре с заявителем;
  - обеспечение сохранности государственной тайны и коммерческой тайны заявителя;
  - соблюдение действующего законодательства.

3. Порядок проведения аттестации и контроля

- Порядок проведения аттестации ОИ включает следующие действия:
- - подачу и рассмотрение заявки на аттестацию;
- - предварительное ознакомление с аттестуемым объектом;
- - испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте;
- - разработка программы и методики аттестационных испытаний;
- - заключение договоров на аттестацию;
- - проведение аттестационных испытаний объекта информатизации;
- - оформление, регистрация и выдача "Аттестата соответствия";
- - осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и

4. Требования к нормативным и методическим документам по аттестации ОИ

- Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России.
- В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.