Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

Для студентов специалитета по специальностям 10.05.03
очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Аттестация объектов информатизации» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов специалитета по специальностям 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам, лабораторным и курсовым работам и к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/19 от 19.03.2019 г.).

Содержание

1. Литература для изучения дисциплины…….…….....……..4
2. Методические указания……..…….....…8
2.1. Раздел 1. Аттестация объектов информатизации. Тема 1. Перечень нормативных правовых актов по обеспечению безопасности информации.…….8
2.2. Раздел 1. Тема 2. Порядок создания и эксплуатации объектов информатизации (автоматизированных систем и выделенных помещений)…….....11
2.3. Раздел 1. Тема 3. Порядок аттестации объектов информатизации (автоматизированных систем) на соответствие требованиям безопасности ……..13
2.4. Раздел 1. Тема 4. Порядок аттестации объектов информатизации (выделенных помещений) на соответствие требованиям безопасности ……..……15
2.5. Раздел 2. Объектовые специальные исследования при аттестации объектов информатизации. Тема 5. Объектовые специальные исследования при аттестации объектов информатизации (автоматизированных систем).……...…17
2.6. Раздел 2. Тема 6. Объектовые специальные исследования при аттестации объектов информатизации (выделенных помещений)……..……19
2.7. Раздел 2. Тема 7 Назначение и порядок проведения объектовых специальных исследований……..21

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

основная

1. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.

2. Бузов Г.А., Калинин С.В., Кондратьев А.В., Зашита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил.

3. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html

4. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

5. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html

6. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282. ДСП

7. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 27.04.2020) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_147084/

8. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_146520

9. Информационное сообщение ФСТЭК России от 15.07.2013 № 240/22/2637 «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах" и приказа ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"» Режим доступа: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/64-deyatelnost/informatsionnye-i-analiticheskie-materialy/716-informatsionnoe-soobshchenie-fstek-rossii-1

10. Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_165503

11. Информационное сообщение ФСТЭК России от 25.06.2014 № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14.03.2014 г. № 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"» Режим доступа: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/865-2748informatsionnoe-soobshchenie-fstek-rossii

12. Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_159975

13. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_294287/

14. Информационное сообщение ФСТЭК России от 04.05.2018 № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации» Режим доступа: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1585-informatsionnoe-soobshchenie-fstek-rossii-ot-4-maya-2018-g-n-240-22-2339

15. Проект методического документа «Методика моделирования угроз безопасности информации» Режим доступа: https://fstec.ru/tekhnicheskaya-

zashchita-informatsii/dokumenty/149-proekty

16. «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

17. «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

18. «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

19. «Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электро-акустических преобразований во вспомогательных технических средствах и системах». Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП

дополнительная

1. Сычев М.П., Лабораторный практикум по курсу "Акустика" [Электронный ресурс]: Учеб. пособие / М.П. Сычев, С.Б. Козлачков. - М.: Издательство МГТУ им. Н. Э. Баумана, 2011. - 76 с. - ISBN - Режим доступа: http://www.studentlibrary.ru/book/bauman_0568.html. Нет подписки

2. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201216.html.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Указ Президента РФ от 16.08.2004 № 1085 (ред. от 31.08.2020) «Вопросы Федеральной службы по техническому и экспортному контролю» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_14031

3.2 «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Гостехкомиссии РФ 25.11.1994 Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_111428

3.3 Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» (ред. от 29.07.2018) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481

3.4 Федеральный закон от 27.07.2006 № 149 - ФЗ «Об информации,

информационных технологиях и о защите информации» (ред. от 08.06.2020)
Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_61798/
3.5 Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ (ред. от 28.11.2018) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241
3.6 Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" [Электронный ресурс] : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий, Каф. информ. безопасности и теории управления. - Электрон. текстовые дан. (1 файл : 352 КБ). - Ульяновск : УлГУ, 2017. URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915/Andreev_2017.pdf
2. Андреев А. С. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" [Электронный ресурс] / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Ульяновск : УлГУ, 2015. URL: http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. Раздел 1. Аттестация объектов информатизации

Тема 1. Перечень нормативных правовых актов по обеспечению безопасности информации

Основные вопросы:

1. Структура нормативных правовых актов по обеспечению безопасности информации в Российской Федерации (Федеральные законы, Указы Президента Российской Федерации, Постановления Правительства Российской Федерации, Специальные нормативные документы ФСТЭК России и ФСБ России, Национальные стандарты).
2. Основные термины и определения в области обеспечения безопасности информации.
3. Требования к органам по аттестации объектов информатизации.

Рекомендации по изучению темы:

Для самостоятельного изучения вопроса 1 в части видов информации ограниченного доступа следует обратиться к интернет ресурсу https://studylib.ru/doc/2424641/vidy-informacii-ogranichennogo-dostupa-po-rossijskomu

Перечень нормативных правовых актов, методических документов и национальных стандартов, необходимых для выполнения работ по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, утвержден директором ФСТЭК России в 2020 году. Перечень имеет пометку ДСП и предназначен для «*органов по аттестации, а также для организаций, претендующих на аккредитацию в качестве органов по аттестации*»

Перечень нормативных правовых актов, методических документов и национальных стандартов, необходимых для выполнения работ по аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации, утвержден директором ФСТЭК России 12.08.2020 г. и доступен на интернет ресурсе https://fstec.ru/normotvorcheskaya/litsenzirovanie/76-inye/2101-perechen-utverzhden-direktorom-fstek-rossii-12-avgusta-2020-g

Для самостоятельного изучения вопроса 2 следует обратиться к национальным стандартам:

- Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации»;
- Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Для самостоятельного изучения вопроса 3 следует обратиться к национальному стандарту ГОСТ Р 58189-2018 «Защита информации. Требования к органам по аттестации объектов информатизации» (предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну) и «Положению о лицензировании деятельности по технической защите конфиденциальной информации», утвержденным постановлением Правительства Российской Федерации от 03.02.2012 № 79 (ред. от 15.06.2016), доступном на интернет ресурсе http://www.consultant.ru/document/cons_doc_LAW_125798

Контрольные вопросы по теме 1:

1. Перечислить нормативные правовые акты, необходимые для аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.
2. Перечислить нормативные правовые акты, необходимые для аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации.
3. Перечислить основные термины по защите информации
4. Перечислить требования, предъявляемые к органам по аттестации объектов информатизации.
5. Перечислить требования, предъявляемые к лицензиатам, аттестовывающих объекты информатизации, предназначенных для обработки конфиденциальной информации.

Тесты для самостоятельной работы:

1. Какой из перечисленных документов является действующим?

а) «Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждено Председателем Гостехкомиссии России 25.11.1994 г.

б) «Положение о сертификации средств защиты информации по требованиям безопасности информации», введено в действие приказом Председателя Гостехкомиссии России от 27.10.1995 г. № 199

в) Руководящий документ «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия недекларированных возможностей», утверждено решением Председателя Гостехкомиссии России от 04.06.1999 № 114.

2. Каким документом следует руководствоваться при аттестации объекта информатизации, предназначенного для обработки конфиденциальной информации?

а) «Специальные требования и рекомендации по технической защите конфиденциальной информации»

б) «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

в) «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

г) «Требованиям безопасности информации к операционным системам»

3. Какие требования предъявляются к должностному лицу, руководящим работами по аттестации объектов информатизации?

а) иметь высшее профессиональное образование по данному направлению и более 5 лет стажа

б) иметь высшее профессиональное образование и более 10 лет стажа

в) иметь высшее профессиональное образование, пройти обучение по программам профессиональной переподготовки по данному направлению и более 5 лет стажа

г) одно из вышеперечисленное

2.2. Раздел 1. Аттестация объектов информатизации

Тема 2. Порядок создания и эксплуатации объектов информатизации (автоматизированных систем и выделенных помещений).

Основные вопросы:

1. Общие положения аттестации объектов информатизации.
2. Основные этапы создания и ввода в эксплуатацию объектов информатизации.
3. Разрабатываемая документация на объекты информатизации.

Рекомендации по изучению темы:

Для самостоятельного изучения вопроса 1 следует обратиться к «Положению по аттестации объектов информатизации по требованиям безопасности информации» и к национальному стандарту ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»

Для самостоятельного изучения вопросов 2-3 следует обратиться к национальному стандарту ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» а также к соответствующим разделам документов:

- [6] 3. Организация работ по защите информации;
- [7] II. Требования к организации защиты информации, содержащейся в информационной системе;
- [10] II. Требования к организации защиты информации в автоматизированной системе управления;
- [13] II. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов.

Контрольные вопросы по теме 2:

1. Назовите основные положения в области аттестации объектов информатизации
2. Перечислите основные этапы создания объектов информатизации (информационных систем, автоматизированных систем управления, значимых объектов критической информационной инфраструктуры)
3. Перечислите основные документы на объекты информатизации (информационные системы, автоматизированные системы управления, значимые объекты критической информационной инфраструктуры)

Тесты для самостоятельной работы:

1. Основные организации, составляющие систему аттестации объектов информатизации:

а) ФСТЭК России

б) органы по аттестации

в) головное подразделение отрасли по защите информации

г) владельцы объектов информатизации

д) представитель заказчика

2. Какой их перечисленных видов работ не относится к аттестации объектов информатизации?

а) анализ исходных данных и предварительное ознакомление

б) обследования объекта информатизации и анализ разработанной документации по защите информации

в) поставка, монтаж и настройка средств защиты информации

г) проведение комплексных аттестационных испытаний объекта информатизации

д) утверждение заключения по результатам аттестации

3. Кто оплачивает расходы по проведению всех работ и услуг по обязательной аттестации объектов информатизации?

а) заявители

б) вышестоящие организации, в подчинении которых находятся аттестуемые организации

в) органы государственного управления, на территории которого находятся аттестуемые организации

4. В какой срок орган по аттестации обязан рассмотреть заявку на проведение аттестации?

а) 15 дней

б) 2 недели

в) 1 месяц

2.3. Раздел 1. Аттестация объектов информатизации

Тема 3. Порядок аттестации объектов информатизации (автоматизированных систем) на соответствие требованиям безопасности

Основные вопросы:

1. Типовая программа и методики аттестационных испытаний информационных (автоматизированных) систем.
2. Порядок проведения аттестации информационных (автоматизированных) систем.
3. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний информационных (автоматизированных) систем.
4. Оформление аттестата соответствия на информационную (автоматизированную) систему

Рекомендации по изучению темы:

Для самостоятельного изучения вопросов 1-3 следует обратиться к национальному стандарту ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»

Для самостоятельного изучения вопроса 4 следует обратиться к Приложению 2 «Положения по аттестации объектов информатизации по требованиям безопасности информации», Приложению 2 [6] и к Приложению Б национального стандарта ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»

Контрольные вопросы по теме 3:

1. Перечислите основные разделы типовой программы и методики аттестационных испытаний
2. Перечислите основные этапы аттестации информационных (автоматизированных) систем.
3. Перечислите основные разделы протоколов аттестационных испытаний
4. Перечислите основные разделы заключения по результатам аттестационных испытаний
5. Перечислите основные разделы аттестата соответствия на информационную (автоматизированную) систему.

Тесты для самостоятельной работы:

1. Расставить в правильном порядке проверки при аттестационных испытаниях автоматизированной системы

а) Проверка уровня подготовки специалистов и распределения ответственности должностных лиц

б) Проверка правильности категорирования

в) Проверка достаточности представленных документов и соответствия их содержания

г) Проверка наличия сертификатов соответствия требованиям безопасности информации

д) Проверка соответствия состава и структуры программно-технических средств автоматизированной системы

е) Проверка правильности классификации

2. Расставить в правильном порядке проверки при аттестационных испытаниях автоматизированной системы на соответствие требованиям по защите информации от утечки по техническим каналам

а) Экспертиза протоколов измерения и предписаний на эксплуатацию

б) Проверка выполнений требований к электропитанию и заземления

в) Проверка средств защиты информации

г) Проверка взаимного размещения технических средств

д) Проверка соответствия фактических размеров контролируемой зоны

е) Проверка соответствия размеров контролируемой зоны требованиям предписаний на эксплуатацию

3. Расставить в правильном порядке проверки при аттестационных испытаниях автоматизированной системы на соответствие требованиям по защите информации от несанкционированного доступа

а) Проверка подсистемы обеспечения целостности

б) Проверка подсистемы управления доступом

в) Проверка соответствия описания технологического процесса обработки, хранения и передачи защищаемой информации реальному технологическому процессу обработки

г) Проверка подсистемы регистрации и учета

4. В течение какого времени действует аттестат соответствия на автоматизированную систему?

а) 5 лет

б) 3 года

в) бессрочно

2.4. Раздел 1. Аттестация объектов информатизации

Тема 4. Порядок аттестации объектов информатизации (выделенных помещений) на соответствие требованиям безопасности

Основные вопросы:

1. Типовая программа и методики аттестационных испытаний выделенных (защищаемых) помещений.
2. Порядок проведения аттестации выделенных (защищаемых) помещений.
3. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний выделенных (защищаемых) помещений.
4. Оформление аттестата соответствия на выделенное (защищаемое) помещение.

Рекомендации по изучению темы:

Для самостоятельного изучения вопросов 1-3 следует обратиться к национальному стандарту ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»

Для самостоятельного изучения вопроса 4 следует обратиться к Приложению 2 «Положения по аттестации объектов информатизации по требованиям безопасности информации», Приложению 2 [6] и к Приложению Б национального стандарта ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»

Контрольные вопросы по теме 4:

1. Перечислите основные разделы типовой программы и методики аттестационных испытаний
2. Перечислите основные этапы аттестации выделенных (защищаемых) помещений.
3. Перечислите основные разделы протоколов аттестационных испытаний
4. Перечислите основные разделы заключения по результатам аттестационных испытаний
5. Перечислите основные разделы аттестата соответствия на выделенное (защищаемое) помещение.

Тесты для самостоятельной работы:

1. Расставить в правильном порядке проверки при аттестационных испытаниях выделенного помещения

а) Проверка соответствия состава и структуры технических средств выделенного помещения

б) Проверка правильности категорирования выделенного помещения

в) Проверка достаточности представленных документов и соответствия их содержания

г) Проверка уровня подготовки специалистов и распределения ответственности должностных лиц

д) Проверка наличия сертификатов соответствия требованиям безопасности информации

2. Расставить в правильном порядке проверки при аттестационных испытаниях выделенного помещения на соответствие требованиям по защите информации от утечки по техническим каналам

а) Проверка средств защиты информации

б) Проверка выполнений требований к электропитанию и заземлению технических средств в выделенном помещении

в) Проверка соответствия фактических размеров контролируемой зоны

г) Экспертиза протоколов измерений и предписаний на эксплуатацию технических средств

3. В течение какого времени действует аттестат соответствия на выделенное помещение?

а) 5 лет

б) 3 года

в) бессрочно

2.5. Объектовые специальные исследования при аттестации объектов информатизации

Тема 5. Объектовые специальные исследования при аттестации объектов информатизации (автоматизированных систем)

Основные вопросы:

1. Технические каналы утечки информации, создаваемые средствами вычислительной техники.
2. Оценка защищенности информации.
3. Применение средств защиты информации.

Рекомендации по изучению темы:

Для самостоятельного изучения вопроса 1 следует обратиться к национальному стандарту ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»

Для самостоятельного изучения вопросов 2-3 следует обратиться к [16,17]

Контрольные вопросы по теме 5:

1. Перечислите основные этапы методики оценки защищенности.
2. Перечислите основные моменты применения средств защиты информации.

Тесты для самостоятельной работы:

1. Какой из режимов обработки информации средствами вычислительной техники является наиболее опасным с точки зрения утечки информации?

а) Чтение информации с накопителей

б) Передача данных в каналы связи

в) Вывод информации на экран монитора

г) Ввод данных с клавиатуры

2. Какие из перечисленных цепей не формируют потенциально-информативные ПЭМИН?

а) Цепи, формирующие шину данных системной шины компьютера

б) Внутренние цепи блока питания компьютера

в) Цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора

г) Цепи, формирующие шину данных системной шины компьютера

3. Какие из перечисленных цепей формируют неинформативные ПЭМИ?

а) Цепи, передающие сигналы аппаратных прерываний

б) Цепи, формирующие шину управления и шину адреса системной шины

в) Цепи формирования и передачи сигналов синхронизации

г) Внутренние цепи блока питания компьютера

д) Цепи, формирующие шину данных внутри микропроцессора

4. Где не могут возникнуть наводки информативных сигналов?

а) В линиях электропитания средств вычислительной техники

б) В цепях заземления средств вычислительной техники и ВТСС

в) В полипропиленовых трубах систем отопления

г) В линиях электропитания и соединительных линиях ВТСС

5. На что направлены пассивные методы защиты?

а) На создание маскирующих пространственных электромагнитных помех

б) На создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС

в) На ослабление побочных электромагнитных излучений

6. На что направлены активные методы защиты?

а) На ослабление наводок

б) На создание маскирующих пространственных электромагнитных помех

в) На исключение (ослабление) просачивания информационных сигналов в

цепи электропитания

2.6. Объектовые специальные исследования при аттестации объектов информатизации

Тема 6. Объектовые специальные исследования при аттестации объектов информатизации (выделенных помещений)

Основные вопросы:

1. Технические каналы утечки акустической речевой информации.
2. Оценка защищенности акустической речевой информации.
3. Применение средств защиты информации.

Рекомендации по изучению темы:

Для самостоятельного изучения вопроса 1 следует обратиться к национальному стандарту ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»

Для самостоятельного изучения вопросов 2-3 следует обратиться к [18,19]

Контрольные вопросы по теме 6:

1. Перечислите основные этапы методики оценки защищенности.
2. Перечислите основные моменты применения средств защиты информации.

Тесты для самостоятельной работы:

1. К какому каналу утечки относятся трубы водоснабжения?

а) Параметрический
б) Вибрационный
в) Оптоэлектронный
г) Виброакустический

2. Что относится к активным способам защиты выделенных помещений:

а) Использование виброгенераторов на стеклах
б) Использование акустических излучателей
в) Двойные двери
г) Звукоизоляция стен

3. Что относится к пассивным способам защиты выделенных помещений:

а) Использование виброгенераторов на стеклах
б) Двойные двери
в) Использование акустических излучателей
г) Звукоизоляция стен

4. Предъявляемые требования к средствам пассивной защиты:

а) Диапазон частот
б) Чувствительность
в) Неравномерность амплитудно-частотной характеристики
г) Коэффициент затухания

2.7. Объектовые специальные исследования при аттестации объектов информатизации

Тема 7. Назначение и порядок проведения объектовых специальных исследований

Основные вопросы:

1. Цель и предназначение объектовых специальных исследований.
2. Требования к проведению объектовых специальных исследований.

1. Порядок проведения специальных исследований средств вычислительной техники.
2. Алгоритм проведения специальных исследований помещений.
3. Документальное оформление результатов работ.

Рекомендации по изучению темы:

Вопросы 1 и 3 изложен в документах [2,3].

Вопрос 2 и 3 изложен в документах [4,5].

Контрольные вопросы по теме 12:

1. Перечислите основные этапы специальных исследований средств вычислительной техники.
2. Перечислите основные этапы специальных исследований помещений.

Тесты для самостоятельной работы:

1. За счет чего происходит ослабление побочных электромагнитных излучений?

а) При прохождении через строительные конструкции помещений и административных зданий

б) При распространении в воздухе с учетом расстояний

в) При прохождении через деревья и кустарники

г) Все вышеперечисленное

2. За счет чего происходит ослабление наводок побочных электромагнитных излучений?

а) При распространении в проводных линиях или металлических коммуникациях

б) При распространении через места соединений с другими проводными линиями, металлическими коммуникациями или оборудованием.

в) Все вышеперечисленное

3. За счет чего происходит ослабление акустических колебаний?

а) При прохождении через строительные конструкции помещений и административных зданий

б) При распространении в воздухе с учетом расстояний

в) При прохождении через естественные и искусственные преграды

в) Все вышеперечисленное