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 ПОМЕЩЕНИЙ»

Для студентов специалитета по специальности 10.05.01
очной формы обучения

Ульяновск, 2020

Методические указания для самостоятельной работы студентов по дисциплине «Аттестация помещений» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2020. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.01 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 лабораторным занятиям и к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 6/20 от 22.09.2020 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. - 586 с. - ISBN 978-5-9912-0424-8 - Текст: электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785991204248.html

2. Зайцев А.П., Технические средства и методы защиты информации : Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. Под ред. А.П. Зайцева и А. А. Шелупанова. - 7-е изд., испр. - М. : Горячая линия - Телеком, 2012. - 442 с. - ISBN 978-5-9912-0233-6 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785991202336.html

3. Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.) Режим доступа: http://docs.cntd.ru/document/902243370

4. 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

5. Некоммерческая интернет-версия СПС "КонсультантПлюс":

5.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

5.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

5.3 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. Режим доступа: http://www.consultant.ru/search/?q=2.%09

5.4 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

5.4 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

6. 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» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с.
7. Дронова Г.А., Аттестация и аудит информационной безопасности: учеб.-метод. пособие / Дронова Г.А. - Новосибирск : Изд-во НГТУ, 2016. - 19 с. - ISBN 978-5-7782-3114-6 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785778231146.html
8. Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51
9. Малюк А.А., Введение в информационную безопасность [Электронный ресурс]: Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.. Под ред. В.С. Горбатова. - М.: Горячая линия - Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201605.html.
10. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
11. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.
12. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
13. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности / А.А. Торокин. М.: Гелиос АРВ, 2005, 960 с.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

ТЕМА 1. ТРЕБОВАНИЯ ОСНОВНЫХ НОРМАТИВНЫХ ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основные вопросы:

1. Законодательство РФ о роли и месте информационной безопасности в обеспечении национальной безопасности
2. Обобщённая структура государственной системы защиты информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 11-14.

Для самостоятельного изучения вопроса 1 следует обратиться к [5.4-5.5]

Вопрос 2 изложен в документе [8].

Для самостоятельного изучения вопроса 1 следует обратиться к [5.1-5.5]

Контрольные вопросы по теме 1:

1. Что такое «Информационная безопасность»?
2. Основные положения Доктрины информационной безопасности РФ
3. Основные положения "Стратегии национальной безопасности Российской Федерации"
4. Основные положения Закона РФ «О государственной тайне»
5. Основные положения «Положения о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам»
6. Обобщённая структура государственной системы защиты информации
7. Основные мероприятия по защите информации
8. Основные задачи государственной системы защиты информации

Тесты для самостоятельной работы:

1. Какой из перечисленных документов является действующим?

а) Концепция национальной безопасности РФ

б) Стратегия национальной безопасности РФ до 2020 года

в) Стратегии нац. безопасности РФ

2. Необходимыми исходными данными для проведения классификации конкретной ИС не является:

а) Перечень защищаемых информационных ресурсов и их уровень конфиденциальности

б) Перечень лиц, имеющих доступ к штатным средствам ИС с указанием их уровня полномочий.

в) Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам ИС.

г) Перечень основных признаков ИС, необходимых для классификации

3. К числу определяющих признаков, по которым производится группировка ИС в различные классы, не относится:

а) Отсутствие в ИС информации различного уровня конфиденциальности

б) Уровень полномочий субъектов доступа ИС на доступ к конфиденциальной информации

в) Режим обработки данных в ИС – коллективный или индивидуальный

4. Организация подает документы на получение лицензии. В течение какого времени орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии?

а) В течение 7 дней

б) В течение 30 дней

в) В течение 15 дней

2.2. РАЗДЕЛ 1. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

ТЕМА 2. ОБЩИЕ ТРЕБОВАНИЯ К АТТЕСТАЦИОННЫМ ИСПЫТАНИЯМ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

Основные вопросы:

1. Обобщенный алгоритм аттестационных испытаний
2. Программа и методики аттестационных испытаний

Рекомендации по изучению темы:

Вопрос 1 изложен в документах [10,12].

Для самостоятельного изучения вопроса 1 следует обратиться к документу [3].

Вопрос 2 изложен в документе [11].

Контрольные вопросы по теме 2:

1. Перечислить основные этапы и ключевые моменты аттестационных испытаний
2. Примерный алгоритм аттестационных испытаний
3. Категории и класса защищенности объекта аттестации
4. Технологическая схема автоматизированной обработки информации
5. Программа и методики аттестационных испытаний
6. Программа испытаний объекта на соответствие требованиям по защите от НСД
7. Программа испытаний на соответствие требованиям по защите от утечки за счет ПЭМИН
8. Ежегодный контроль эффективности защиты

Тесты для самостоятельной работы:

1. Какой их перечисленных этапов не относится к включается в аттестации объектов информатизации?

а) поставка, монтаж и настройка средств защиты информации
б) проведение комплексных аттестационных испытаний
в) обследование объекта информатизации
г) подготовка протоколов по результатам комплексных проверок с выдачей рекомендаций
д) сертификация средств защиты

2. 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

3. 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 И ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

ТЕМА 3. ОРГАНИЗАЦИЯ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Основные вопросы:

1. Понятие процедуры аттестации.
2. Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации
3. Основные документы для проведения аттестационных испытаний автоматизированной системы и выделенного помещения предприятия

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 11-12.

Для самостоятельного изучения вопроса 1 следует обратиться к документам [10-12]

Вопрос 2 изложен в документе [1].

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [7] на стр. 11-19.

Вопрос 3 изложен в документах [10-11].

Для самостоятельного изучения вопроса 3 следует обратиться к документу [3].

Контрольные вопросы по теме 3

1. Дать определение аттестации
2. Что такое объект информатизации?
3. Дать характеристику основных этапов аттестации
4. Работы при обследовании объекта информатизации
5. Разработка программы и методики аттестационных испытаний
6. Что включают в себя Комплексные аттестационные испытания?
7. Основные функции органов по аттестации
8. Порядок проведения аттестации объектов на соответствие требованиям безопасности информации
9. Основные документы для проведения аттестационных испытаний автоматизированной системы
10. Основные документы для проведения аттестационных испытаний выделенного помещения предприятия

Тесты для самостоятельной работы:

1. В течение какого времени действует аттестат соответствия на объект информатизации?

а) 1 год

б) 3 года

в) бессрочно

2. Какие действия, из перечисленных, не осуществляются, если во время аттестационных испытаний использованные средства защиты информации не имеют сертификатов соответствия?

а) организуются дополнительные сертификационные испытания этих средств защиты

б) осуществляется замена на аналогичные образцы средств защиты, имеющие сертификаты

в) изменяется методика аттестационных испытаний

3. Какими органами проводятся аттестационные испытания объектов информатизации?

а) аттестационными комиссиями органов по аттестации объектов информатизации, аккредитованными ФСТЭК России

б) аттестационными комиссиями органов по аттестации, аккредитованными органом государственного самоуправления

2.4. РАЗДЕЛ 1. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

ТЕМА 4. ОРГАНИЗАЦИЯ АТТЕСТАЦИИ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Основные вопросы:

1. Порядок проведения аттестации выделенного помещения
2. Ввод в действие и эксплуатация аттестованных по требованиям безопасности выделенных помещений
3. Контроль за соблюдением порядка аттестации и эксплуатации аттестованных помещений.

Рекомендации по изучению темы:

Вопрос 1 изложен в документе 3

Для самостоятельного изучения вопроса 1 следует обратиться к документам [10-11].

Вопрос 2 изложен в документе 3

Для самостоятельного изучения вопроса 2 следует обратиться к документам [10-11].

Вопрос 3 изложен в документе 10.

Для самостоятельного изучения вопроса 3 следует обратиться к документу [3].

Контрольные вопросы по теме 4:

1. Что такое выделенное (защищаемое) помещение
2. Понятие процедуры аттестации выделенного помещения предприятия
3. Этапы проведения аттестации выделенного помещения
4. Основные и вспомогательные технические средства и системы (ОТСС и ВТСС)
5. Ввод в действие и эксплуатация аттестованных по требованиям безопасности выделенных помещений
6. Контроль за соблюдением порядка аттестации и эксплуатации аттестованных помещений
7. Документы для проведения аттестационных испытаний выделенного помещения предприятия

Тесты для самостоятельной работы:

1. Какой документ, из перечисленных, не относится к сфере противодействия иностранным техническим разведкам?

а) Федеральный закон от 27 декабря 2002 г. № 184 - ФЗ «О техническом регулировании»

б) Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»

в) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
г) Указ Президента Российской Федерации от 16 августа 2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»

2. Какой из нижеперечисленных факторов влияет на эффективность защиты информации от утечки?
а) Отношение сигнал/шум на входе приемника сигналов
б) Время и затраты на поиск канала утечки
в) Демаскирующие признаки носителя информации

3. Каким показателем характеризуется источник сигнала?
а) Мощность помех
б) Чувствительность
в) Диаграмма направленности излучения
г) Скорость распространения сигнала в среде

4. Каким из параметров обладает приемник сигналов?
а) Динамический диапазон сигнала
б) Параметр спектра сигнала
в) Пространственная селективность приемной антенны
г) Амплитудно-частотная характеристика

2.5. РАЗДЕЛ 2 СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ ОБЪЕКТОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 5. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ, СОЗДАВАЕМЫЕ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Основные вопросы:

1. Типовая структура и виды технических каналов утечки информации
2. Классификация технических каналов утечки информации
3. Основные показатели технических каналов утечки информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [13] на с. 171-180.

Для самостоятельного изучения вопроса 1 следует обратиться к [1] на с. 9-17.

Вопрос 2 изложен в учебном пособии [13] на с. 169-171.

Вопрос 3 изложен в учебном пособии [13] на с. 180-190.

Контрольные вопросы по теме 5:

1. Понятие утечки информации
2. Что такое технический канал утечки информации (ТКУИ)?
3. Обобщенная модель ТКУИ.
4. Основные технические средства и системы (ОТСС). Привести примеры конкретных ОТСС
5. Вспомогательные технические средства и системы (ВТСС). Привести примеры конкретных ВТСС
6. Что такое контролируемая зона технического средства передачи информации (ТСПИ)
7. Дать характеристику типовых технических каналов утечки информации
8. Привести вариант классификации технических каналов утечки информации
9. Основные показатели технических каналов утечки 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 генераторов шума
б) Использование двойных дверей

в) Звукоизоляция помещений

3. Какой из режимов обработки информации средствами ВТ 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

4. 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

5. Какие из перечисленных цепей не 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

6. Где не могут возникнуть наводки информативных сигналов?
а) В линиях электропитания ЭВМ
б) В цепях заземления ЭВМ и ВТСС
в) В полипропиленовых трубах систем отопления
г) В линиях электропитания и соединительных линиях ВТСС

2.6. РАЗДЕЛ 2 СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ ОБЪЕКТОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 6. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ, ИСПОЛЬЗУЮЩИЕ СПЕЦИАЛЬНО ВНЕДРЕННЫЕ В УКАЗАННЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ИЛИ ПОМЕЩЕНИЯ УСТРОЙСТВА НЕГЛАСНОГО СЪЕМА ИНФОРМАЦИИ

Основные вопросы:

1. Технические каналы утечки информации, создаваемые путём «высокочастотного облучения» СВТ
2. Электронные устройства перехвата информации (закладные устройства) скрытно внедряемых в технические средства и системы. Классификация технических средств негласного съема информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 15-25.

Вопрос 2 изложен в учебном пособии [1] на с. 25-36.

Контрольные вопросы по теме 6:

1. Охарактеризовать способ «высокочастотного облучения» СВТ
2. Перехват информации, обрабатываемой СВТ, методом «высокочастотного облучения»
3. Перехват информации, обрабатываемой СВТ, путём установки в них закладных устройств
4. Классификация закладных устройств
5. Перехват побочных электромагнитных излучений, возникающих при работе СВТ
6. Порядок проверки помещений и технических средств. Противодействие каналам утечки

Тесты для самостоятельной работы:

1. Что необходимо для возникновения канала утечки?

а) Чтобы соединительные линии ВТСС, линии электропитания, посторонние проводники и т.д., выполняющие роль случайных антенн, выходили за пределы контролируемой зоны объекта

б) Чтобы расстояние от СВТ до случайной сосредоточенной антенны было более r1, и расстояние до случайной распределённой антенны было более r1

в) Чтобы была возможность непосредственного подключения к случайной антенне только в пределах контролируемой зоны объекта средств разведки ПЭМИН

2. Каких закладных устройств, внедряемых в СВТ, по виду перехватываемой информации не существует?

а) Аппаратные закладки для перехвата изображений, выводимых на экран монитора

б) Аппаратные закладки для перехвата информации, хранящейся в оперативной памяти

в) Аппаратные закладки для перехвата информации, записываемой на жёсткий диск ПЭВМ

г) Аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ

3. Каким путем нельзя осуществить перехват информации, обрабатываемой СВТ?

а) Перехватом побочных электромагнитных излучений, возникающих при работе СВТ

б) Перехватом наводок информативных сигналов с соединительных линий ВТСС и посторонних проводников

в) «Низкочастотного облучения» СВТ

4. 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

5. За счет чего происходит ослабление ПЭМИН ТСПИ и их наводок в посторонних проводниках?

а) Экранирование и заземление ТСПИ и их соединительных линий

б) Фильтрация информационных сигналов

в) Пространственное и линейное зашумление

6. В каких системах, средствах информатизации и связи не может осуществляться фильтрация?

а) В высокочастотных трактах передающих и приемных устройств

б) В различных сигнальных цепях технических средств

в) В цепях электропитания, управления, контроля, коммутации технических средств

г) В металлических проводящих конструкциях

2.7. РАЗДЕЛ 2 СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ ОБЪЕКТОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕМА 7. НАЗНАЧЕНИЕ И ПОРЯДОК ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ

Основные вопросы:

1. Цель и назначение специальных исследований

2. Лабораторные специальные исследования основных технических средств

3. Специальные исследования основных и вспомогательных технических средств, располагаемых в выделенных и защищаемых помещениях на предмет возможности утечки обсуждаемой информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 343-357.

Вопрос 2 изложен в учебном пособии [1] на с. 360-370.

Для самостоятельного изучения вопроса 2 следует обратиться к [2,4,6].

Вопрос 3 изложен в учебном пособии [1] на с. 380-390.

Для самостоятельного изучения вопроса 1 следует обратиться к [8] Глава 13.

Контрольные вопросы по теме 7:

1. Для чего нужны специальные исследования
2. Порядок проведения специальных исследований
3. Что включают в себя лабораторные специальные исследования основных технических средств
4. Специальные исследования основных и вспомогательных технических средств, располагаемых в выделенных и защищаемых помещениях

Тесты для самостоятельной работы:

1. Чем технические средства расширяют и дополняют возможности человека по добыванию информации?

а) Возможностью консервировать информацию на непродолжительное время

б) Съемом информации с носителей, которые недоступны органам чувств человека

в) Возможностью добычи информации за пределами контролируемой зоны

2. Что не должно входить в состав отчетных документов о проведении обследования помещения?

а) Протоколы изъятия средств съема информации

б) Рекомендации по устранению и нейтрализации технических каналов утечки

в) Методические рекомендации о степени защищенности объекта

3. Какое устройство, из перечисленных, подходит для проверки наличия и опасности НЧ-магнитных полей?

а) D-008
б) Трап-Н50
в) МТ-402
г) Цифровой мультимер