

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 ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ
(ТИП ПРАКТИКИ: ПРЕДДИПЛОМНАЯ)**

Для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной
формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы по преддипломной практике / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов специалитета по специальностям 10.05.01 и 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 преддипломной практике, её проведению и к зачёту по практике.

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 подготовки к преддипломной практике	4
2. Методические указания.....	6
2.1. Раздел 1. Подготовительный этап.....	6
2.2. Раздел 2. Экспериментальный этап.....	10
2.3. Раздел 3. Заключительный этап.....	19
2.4. Раздел 4. Отчет по практике	22

1. ЛИТЕРАТУРА ДЛЯ ПОДГОТОВКИ К ПРЕДИПЛОМНОЙ ПРАКТИКЕ

1. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с. <https://biblio-online.ru/viewer/zaschita-informacii-osnovy-teorii-433715>.

2. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 – Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991205252.html>.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

3.2 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

3.3 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.

3.4 Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования (утв. [приказом](#) Министерства образования и науки РФ от 27 ноября 2015 г. № 1383). Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_190917/.

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

3.6 Постановление Правительства РФ от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

3.7 Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Постановление Правительства РФ от 3 ноября 1994г. № 1233

3.8 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/

3.9 . 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/

4. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

5. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт. журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: http://journals.tsu.ru/pdm/&journal_page=archive&id=1823

6. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). **URL:** <http://edu.ulsu.ru/courses/750/interface/>.

7. Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2019 – 63 с.

8. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2019 – 103 с.

9. 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>.

10. 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>

11. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»; ИНФРА-М, 2014. – 416 с. ил.

12. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. - 392с.

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.

14. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации: Учебное пособие. Изд. 4-е, перераб. и доп. – М.:ЛЕНАНД, 2016. – 416.с.

15. Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. – Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП

Контрольные вопросы для подготовки к преддипломной практике:

1. Классификация угроз информации. Источники угроз информационной безопасности РФ. Модель действий нарушителя
2. Понятие информационной войны. Составные части и методы информационного противоборства. Информационное оружие
3. Концепция защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности
4. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Структура системы защиты информации от НСД, назначение и функции элементов
5. Правила разграничения доступа к информации. Мандатная и дискреционная модели управления доступом
6. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Основные методы аутентификации
7. Технология межсетевых экранов (МЭ). Виды МЭ
8. Основные понятия и функции виртуальных частных сетей (VPN)
9. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу
10. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности
11. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн
12. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии
13. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации
14. Методы и средства инженерной защиты объектов информатизации
15. Программные и аппаратные средства защиты информации от несанкционированного доступа
16. Общие положения инженерно-технической защиты информации. Классификация технических каналов утечки информации
17. Скрытие демаскирующих признаков при противодействии техническим средствам разведки (ТСР)
18. Физические и технические основы противодействия видовой разведке. Технический контроль эффективности противодействия видовой разведке

Рекомендации по подготовке к контрольным вопросам раздела 1:

Вопросы 1-2 изложены в учебном пособии [7] на с. 20-62.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [11] на с. 15-25.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [12] на с. 50-57 и к учебному пособию [14] на с. 17-23.

Вопросы 3-5 изложены в учебном пособии [8] на с. 8-31.

Вопрос 6 изложен в учебном пособии [8] на с. 59-66.

Для самостоятельного изучения вопроса 6 следует обратиться к учебному пособию [11] на с. 142-146.

Вопросы 7-8 изложены в учебном пособии [8] на с. 72-102.

Для самостоятельного изучения вопроса 7 следует обратиться к учебному пособию [11] на с. 193-214.

Для самостоятельного изучения вопроса 8 следует обратиться к учебному пособию [11] на с. 217-240.

Вопрос 9 изложен в учебном пособии [10] на с. 278-296.

Вопрос 10 изложен в учебном пособии [11] на с. 9-15, в учебном пособии [12] на с. 8-13.

Для самостоятельного изучения вопроса 10 следует обратиться к [3.7-3.9].

Вопрос 11 изложен в учебном пособии [12] на с. 62-71.

Для самостоятельного изучения вопроса 11 следует обратиться к [3.1, 3.3, 3.5 и 3.7].

Вопрос 12 изложен в учебном пособии [6] на с. 7-40.

Для самостоятельного изучения вопроса 12 следует обратиться к [3.2].

Вопрос 13 изложен в [3.5, 3.6].

Для самостоятельного изучения вопроса 13 следует обратиться к учебному пособию [6] на с. 7-40.

Вопрос 14 изложен в учебном пособии [13] на с. 280-299.

Для самостоятельного изучения вопроса 14 следует обратиться к учебному пособию [12] на с. 157-208.

Вопрос 15 изложен в учебном пособии [12] на с. 358-384.

Вопрос 16 изложен в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопроса 16 следует обратиться к [10] на с. 248-278.

Вопросы 17-18 изложены в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопросов 17-18 следует обратиться к [10] на с. 248-278.

Тесты для самостоятельной работы:

1. Кто является обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений?

- а) Работник
- б) Работодатель
- в) Пенсионный фонд
- г) Налоговая служба

2. На какие документы, из перечисленных, следует опираться при создании системы защиты ПДн на предприятии? Выбрать 2 позиции.

- а) № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- б) ПП РФ N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
- в) Конституция РФ
- г) N 152-ФЗ «О персональных данных»

3. Какой организации следует отправлять Уведомление о намерении осуществлять обработку ПДн, если организация является оператором по обработке ПДн?

- а) Роскомнадзор
- б) ФСТЭК
- в) Налоговая служба
- г) ФСБ

4. На кого возлагается организация сертификации средств ЗИ? Выбрать 3 позиции.

- а) ФСТЭК
- б) МВК по ЗГТ
- в) ФСБ
- г) Аттестационная комиссия
- д) МО РФ

5. Какая организация занимается координацией работ по организации сертификации?

- а) ФСТЭК
- б) МВК по ЗГТ
- в) ФСБ

6. Какие органы, из перечисленных, уполномочены на ведение лицензионной деятельности? Отметить 2 позиции.

- а) ФСТЭК
- б) СВР РФ
- в) МВК

г) ФСБ РФ

7. 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

8. В течение какого времени организация должна подать заявление о переоформлении лицензии, если изменились условия ведения лицензируемого вида деятельности?

- а) В течение 7 дней
- б) В течение 30 дней
- в) В течение 15 дней

9. Какая организация занимается лицензированием деятельности по ТЗИ конфиденциальной информации?

- а) ФСТЭК
- б) МВК
- в) ФСБ

10. Объектом интеллектуальной собственности не является:

- а) Программа для ЭВМ
- б) Юридический документ
- в) Базы данных
- г) Секреты производства

11. В каких правах может быть ограничено лицо, допущенное или ранее допускавшееся к ГТ?

- а) В праве на неприкосновенность частной жизни во время оформления допуска к ГТ
- б) В праве выезжать за пределы города, в котором проживает
- в) В праве вступать в брак

12. Кто несет ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти и в организациях?

- а) Заместитель руководителя организации по безопасности
- б) Руководитель организации
- в) Начальник режимно-секретного подразделения

13. Какой федеральный орган исполнительной власти является уполномоченным в области технической защиты информации?

- а) Минобороны России
- б) ФСТЭК России
- в) ФСБ

14. С чьей санкции осуществляется взаимная передача сведений, составляющих государственную тайну, между организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ?

- а) Органа, уполномоченного на ведение лицензионной деятельности в области защиты государственной тайны
- б) Органа государственной власти, в распоряжении которого находятся эти сведения
- в) ФСТЭК

15. Основанием для освобождения руководителей организаций от государственной аттестации является:

- а) Наличие у руководителя допуска к государственной тайне по второй форме
- б) Наличие стажа работы в сфере защиты государственной тайны более 5 лет
- в) Наличие документа об образовании и (или) о повышении квалификации, выданного организацией, включенной в перечень, определяемый МВК по ЗГТ, если со времени ее окончания прошло не более 5 лет

16. 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»

2.2. РАЗДЕЛ 2. ЭКСПЕРИМЕНТАЛЬНЫЙ ЭТАП

Контрольные вопросы для подготовки к экспериментальному этапу преддипломной практике:

1. Совершенные по Шеннону шифры. Необходимые и достаточные условия совершенных шифров. Теорема К.Шеннона. Табличное и модульное гаммирование
2. Имитация и подмена шифрованных сообщений. Оценки для вероятностей имитации и подмены сообщений. Критерии достижимости нижних оценок

3. Симметричные блочные шифры. Шифры Фейстеля и их обратимость. Российский стандарт шифрования ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров
4. Шифр “Кузнечик” из ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров
5. Ассиметричные блочные шифры. Схема Диффи-Хеллмана. Шифр RSA. Шифр Эль-Гамала. Шифр Шамира
6. Модификация асимметричных шифров на эллиптических кривых. Модификация схемы Диффи-Хеллмана. Модификация шифра Эль-Гамала. Модификация шифра Месси-Омуры
7. Хеш-функции. Требования, предъявляемые к хеш-функциям. Криптографические хеш-функции. Способы построения криптографических хеш-функций
8. Коды аутентификации. Понятие имитации и подмены сообщения. Нижние оценки для вероятностей успеха имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации
9. Электронная подпись. Электронная подпись на основе асимметричных систем шифрования: электронная подпись RSA, электронная подпись Фиата-Шамира, электронная подпись Эль-Гамала, электронная подпись Шнорра
10. Методы пассивной и активной защиты утечки информации по акустическому (вибраакустическому) каналу
11. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности
12. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн
13. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии
14. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации
15. Методы и средства инженерной защиты объектов информатизации
16. Программные и аппаратные средства защиты информации от несанкционированного доступа
17. Общие положения инженерно-технической защиты информации. Классификация технических каналов утечки информации
18. Скрытие демаскирующих признаков при противодействии техническим средствам разведки (ТСР)
19. Физические и технические основы противодействия видовой разведке. Технический контроль эффективности противодействия видовой разведке

Рекомендации по подготовке к контрольным вопросам раздела 2:

Вопрос 1 изложен в параграфах 6.4-6.8 учебного пособия [15].

Вопрос 2 изложен в параграфе 6.9 учебного пособия [15].

Вопрос 3 изложен в параграфах 8.1-8.8 учебного пособия [15].

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [11] на с. 123-134.

Вопрос 4 изложен в параграфе 8.8 учебного пособия [15].

Вопрос 5 изложен в параграфах 9.1-9.7 учебного пособия [15].

Для самостоятельного изучения вопроса 5 следует обратиться к учебному пособию [11] на с. 135-141.

Вопрос 6 изложен в параграфах 9.2-9.7 учебного пособия [15].

Вопрос 7 изложен в параграфах 10.1-10.4 учебного пособия [15].

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [11] на с. 110-113.

Вопрос 8 изложен в параграфах 11.1-11.3 учебного пособия [15].

Вопрос 9 изложен в параграфах 12.1-12.7 учебного пособия [15].

Вопрос 10 изложен в учебном пособии [10] на с. 278-296.

Вопрос 11 изложен в учебном пособии [11] на с. 9-15, в учебном пособии [12] на с. 8-13.

Для самостоятельного изучения вопроса 11 следует обратиться к [3.7-3.9].

Вопрос 12 изложен в учебном пособии [12] на с. 62-71.

Для самостоятельного изучения вопроса 12 следует обратиться к [3.1, 3.3, 3.5 и 3.7].

Вопрос 13 изложен в учебном пособии [6] на с. 7-40.

Для самостоятельного изучения вопроса 13 следует обратиться к [3.2].

Вопрос 14 изложен в [3.5, 3.6].

Для самостоятельного изучения вопроса 14 следует обратиться к учебному пособию [6] на с. 7-40.

Вопрос 15 изложен в учебном пособии [13] на с. 280-299.

Для самостоятельного изучения вопроса 15 следует обратиться к учебному пособию [12] на с. 157-208.

Вопрос 16 изложен в учебном пособии [12] на с. 358-384.

Вопрос 17 изложен в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопроса 17 следует обратиться к [10] на с. 248-278.

Вопросы 18-19 изложены в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопросов 18-19 следует обратиться к [10] на с. 248-278.

Тесты для самостоятельной работы:

1. Что из перечисленного относится к случайным акустоэлектрическим преобразователям?

а) Металлические корпуса средств и приборов

- б) Монтажные провода, соединительные кабели, токопроводы печатных плат
- в) Ферромагнитные материалы в виде сердечников трансформаторов и дросселей

2. Основным распределенным источником магнитного, электрического и электромагнитного полей является:

- а) Анизотропный излучатель
- б) Симметричный/несимметричный кабель
- в) Цепь звукоусилительной аппаратуры
- г) Кабель внутренней АТС

3. Цепи заземления в общем случае создаются для выполнения следующих функций:

- а) Создание электрического поля
- б) Модуляция тока электропитания токами радиоэлектронного средства
- в) Обеспечение путей для протекания возвратных (обратных) питающих и сигнальных токов

4. 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

5. Что необходимо сделать для предотвращения утечки информации по техническому каналу?

- а) Увеличить мощность носителя
- б) Нейтрализовать преднамеренные и случайные воздействия на источник информации
- в) Уменьшить информативность признаковой структуры объектов защиты

6. Что является способом защиты от утечки, возникшей за счет высокочастотного облучения и ВЧ-навязывания?

- а) Генерирование «розового» шума
- в) Осуществление периодических проверок на увеличение тока потребления
- г) Создание помех в диапазоне от 100 до 1000 мГц
- д) Соблюдение размеров контролируемых зон

7. Что является важнейшим показателем технического канала утечки?

- а) Пропускная способность
- б) Информативность
- в) Длина
- г) Среда

8. Каким показателем характеризуется источник сигнала?

- а) Мощность помех
- б) Чувствительность
- в) Диаграмма направленности излучения
- г) Скорость распространения сигнала в среде

9. Каким из параметров обладает приемник сигналов?

- а) Динамический диапазон сигнала
- б) Параметр спектра сигнала
- в) Пространственная селективность приемной антенны
- г) Амплитудно-частотная характеристика

10. К какому каналу утечки относятся трубы водоснабжения?

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

11. Что относится к активным способам защиты выделенных помещений?

- а) Использование генераторов шума
- б) Использование двойных дверей
- в) Звукоизоляция помещений

12. Что относится к активным способам защиты выделенных помещений?

- а) Использование генераторов шума
- б) Использование двойных дверей
- в) Звукоизоляция помещений

13. Что из перечисленного относится к портативным подавителям диктофонов?

- а) «ANG-2000»
- б) «Шумотрон-3»
- в) «Шорох»

14. Какой из перечисленных приборов является генератором шума?

- а) «Порог-2М»
- б) «Шторм»
- в) «Штурм»
- г) ST-031M «Пиранья»

15. Что из перечисленного относится к стационарным подавителям диктофонов?

- а) VNG-006

- б) «Буря-4»
- в) «Шорох»

16. 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

17. 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

18. 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 r_1 , и расстояние до случайной распределённой антенны было более r_1
- в) Чтобы была возможность непосредственного подключения к случайной антенне только в пределах контролируемой зоны объекта средств разведки ПЭМИН

19. 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

20. 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

21. На что направлены активные методы защиты?

- а) На ослабление наводок побочных электромагнитных излучений
- б) На создание маскирующих пространственных электромагнитных помех
- в) На исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания

22. За счет чего происходит ослабление побочных электромагнитных излучений 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

23. 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

24. На какие группы по способу регистрации можно разбить закладные устройства?

- а) С помощью проводных линий
- б) С помощью оптического канала
- в) С помощью микрофона

25. На какие группы по способу передачи можно разбить закладные устройства?

- а) С помощью радиоканала
- б) С помощью пьезокристаллического датчика
- в) С помощью модуляции отраженного луча от светоотражающих поверхностей

26. На что направлены пассивные методы защиты акустической информации?

- а) Создание маскирующих акустических и вибрационных помех
- б) Создание маскирующих электромагнитных помех
- в) Ультразвуковое подавление диктофонов в режиме записи
- г) Обнаружение излучений акустических закладок

27. На что направлены активные методы защиты акустической информации?

- а) Ослабление акустических (речевых) сигналов
- б) Ослабление информационных электрических сигналов
- в) Электромагнитное подавление диктофонов в режиме записи

28. Какое устройство используется для локализации установленных закладных устройств?

- а) «Рубеж»
- б) «Дельта»
- в) «Сова»

29. Какое устройство используется для обнаружения работающих в режиме записи диктофонов?

- а) TRD-800
- б) SMP-700
- в) OSCOR OSC-500

30. Какое устройство используется для электромагнитного подавления диктофонов?

- а) ST-031 «Пиранья»
- б) NR-90EM
- в) «Рубеж»

31. Для чего предназначен генератор шума ANG-2000?

- а) Для создания виброакустических помех с целью защиты от проводных и радиомикрофонов
- б) Для защиты информации от утечки по акустическим и виброакустическим каналам
- в) Для защиты объектов информатизации 1 категории и противодействия техническим средствам перехвата речевой информации

32. 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

33. 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

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

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

35. Какое устройство, из перечисленных, предназначено для проверки телефонных коммуникаций?

- а) Цифровой мультиметр
- б) OSC-5000
- в) NR-900EM

Индивидуальные задания по практике:

1. Изучить средства защиты баз данных, ОС, антивирусные средства и др., имеющиеся на предприятии
2. Ознакомиться с имеющимися на предприятии аппаратно-программными средствами защиты информации и документацией на них
3. Изучить имеющиеся на предприятии инструкции (руководства) по пропускному режиму, по обеспечению информационной безопасности (перечни сведений, составляющих коммерческую тайну, персональные данные и др., соглашения о неразглашении и др.)
4. Изучить должностные инструкции специалистов по ИБ предприятия
5. Изучить имеющиеся на предприятии доступные руководящие документы, касающиеся защиты информации
6. Ознакомиться с имеющимися на предприятии криптографическими средствами защиты информации и документацией на них
7. Ознакомиться с порядком и документами лицензирования в области защиты информации предприятия
8. Ознакомиться с порядком и документами сертификации средств защиты предприятия
9. Ознакомиться с доступными методами и средствами инженерной защиты объектов информатизации предприятия
10. Ознакомиться с доступными программными и аппаратными средствами защиты информации от несанкционированного доступа предприятия
11. Ознакомиться с доступной пассивной и активной защитой от утечки информации по акустическому (виброакустическому) каналу
12. Ознакомиться с доступными методами и средствами пассивной и активной защиты от утечки в электромагнитном канале предприятия

2.3. РАЗДЕЛ 3. ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

Контрольные вопросы для подготовки к заключительному этапу преддипломной практике:

1. Классификация угроз информации. Источники угроз информационной безопасности РФ. Модель действий нарушителя
2. Понятие информационной войны. Составные части и методы информационного противоборства. Информационное оружие
3. Концепция защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности
4. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Структура системы защиты информации от НСД, назначение и функции элементов
5. Правила разграничения доступа к информации. Мандатная и дискреционная модели управления доступом
6. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Основные методы аутентификации
7. Технология межсетевых экранов (МЭ). Виды МЭ
8. Основные понятия и функции виртуальных частных сетей (VPN).
9. Совершенные по Шеннону шифры. Необходимые и достаточные условия совершенных шифров. Теорема К.Шеннона. Табличное и модульное гаммирование
10. Имитация и подмена шифрованных сообщений. Оценки для вероятностей имитации и подмены сообщений. Критерии достижимости нижних оценок
11. Симметричные блочные шифры. Шифры Фейстеля и их обратимость. Российский стандарт шифрования ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров
12. Шифр “Кузнечик” из ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров
13. Ассиметричные блочные шифры. Схема Диффи-Хеллмана. Шифр RSA. Шифр Эль-Гамала. Шифр Шамира
14. Модификация асимметричных шифров на эллиптических кривых. Модификация схемы Диффи-Хеллмана. Модификация шифра Эль-Гамала. Модификация шифра Месси-Омуры
15. Хеш-функции. Требования, предъявляемые к хеш-функциям. Криптографические хеш-функции. Способы построения криптографических хеш-функций
16. Коды аутентификации. Понятие имитации и подмены сообщения. Нижние оценки для вероятностей успеха имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации
17. Электронная подпись. Электронная подпись на основе асимметричных систем шифрования: электронная подпись RSA, электронная

подпись Фиата-Шамира, электронная подпись Эль-Гамаля, электронная подпись Шнорра

18. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале

19. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу

20. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности

21. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн

22. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии

23. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации

24. Методы и средства инженерной защиты объектов информатизации

25. Программные и аппаратные средства защиты информации от несанкционированного доступа

26. Общие положения инженерно-технической защиты информации. Классификация технических каналов утечки информации

27. Скрытие демаскирующих признаков при противодействии техническим средствам разведки (ТСР)

28. Физические и технические основы противодействия видовой разведке. Технический контроль эффективности противодействия видовой разведке

Рекомендации по подготовке к контрольным вопросам раздела 3:

Вопросы 1-2 изложены в учебном пособии [7] на с. 20-62.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [11] на с. 15-25.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [12] на с. 50-57.

Вопросы 3-5 изложены в учебном пособии [8] на с. 8-31.

Вопрос 6 изложен в учебном пособии [8] на с. 59-66.

Для самостоятельного изучения вопроса 6 следует обратиться к учебному пособию [11] на с. 142-146.

Вопросы 7-8 изложены в учебном пособии [8] на с. 72-102.

Для самостоятельного изучения вопроса 7 следует обратиться к учебному пособию [11] на с. 193-214.

Для самостоятельного изучения вопроса 8 следует обратиться к учебному пособию [11] на с. 217-240.

Вопрос 9 изложен в параграфах 6.4-6.8 учебного пособия [15].

Вопрос 10 изложен в параграфе 6.9 учебного пособия [15].

Вопрос 11 изложен в параграфах 8.1-8.8 учебного пособия [15].

Для самостоятельного изучения вопроса 11 следует обратиться к учебному пособию [11] на с. 123-134.

Вопрос 12 изложен в параграфе 8.8 учебного пособия [15].

Вопрос 13 изложен в параграфах 9.1-9.7 учебного пособия [15].

Для самостоятельного изучения вопроса 13 следует обратиться к учебному пособию [11] на с. 135-141.

Вопрос 14 изложен в параграфах 9.2-9.7 учебного пособия [15].

Вопрос 15 изложен в параграфах 10.1-10.4 учебного пособия [15].

Для самостоятельного изучения вопроса 15 следует обратиться к учебному пособию [11] на с. 110-113.

Вопрос 16 изложен в параграфах 11.1-11.3 учебного пособия [15].

Вопрос 17 изложен в параграфах 12.1-12.7 учебного пособия [15].

Вопрос 18 изложен в учебном пособии [13] на с. 686-695.

Вопрос 19 изложен в учебном пособии [10] на с. 278-296.

Вопрос 20 изложен в учебном пособии [11] на с. 9-15, в учебном пособии [12] на с. 8-13.

Для самостоятельного изучения вопроса 20 следует обратиться к [3.7-3.9].

Вопрос 21 изложен в учебном пособии [12] на с. 62-71.

Для самостоятельного изучения вопроса 21 следует обратиться к [3.1, 3.3, 3.5 и 3.7].

Вопрос 22 изложен в учебном пособии [6] на с. 7-40.

Для самостоятельного изучения вопроса 22 следует обратиться к [3.2].

Вопрос 23 изложен в [3.5, 3.6].

Для самостоятельного изучения вопроса 23 следует обратиться к учебному пособию [6] на с. 7-40.

Вопрос 24 изложен в учебном пособии [13] на с. 280-299.

Для самостоятельного изучения вопроса 24 следует обратиться к учебному пособию [12] на с. 157-208.

Вопрос 25 изложен в учебном пособии [12] на с. 358-384.

Вопрос 26 изложен в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопроса 26 следует обратиться к [10] на с. 248-278.

Вопросы 27-28 изложены в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопросов 27-28 следует обратиться к [10] на с. 248-278.

2.4. РАЗДЕЛ 4. ОТЧЕТ ПО ПРАКТИКЕ

Контрольные вопросы для подготовки к отчёту по преддипломной практике:

1. Классификация угроз информации. Источники угроз информационной безопасности РФ. Модель действий нарушителя
2. Понятие информационной войны. Составные части и методы информационного противоборства. Информационное оружие
3. Концепция защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности
4. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Структура системы защиты информации от НСД, назначение и функции элементов
5. Правила разграничения доступа к информации. Мандатная и дискреционная модели управления доступом
6. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Основные методы аутентификации
7. Технология межсетевых экранов (МЭ). Виды МЭ
8. Основные понятия и функции виртуальных частных сетей (VPN).
9. Совершенные по Шеннону шифры. Необходимые и достаточные условия совершенных шифров. Теорема К.Шеннона. Табличное и модульное гаммирование
10. Имитация и подмена шифрованных сообщений. Оценки для вероятностей имитации и подмены сообщений. Критерии достижимости нижних оценок
11. Симметричные блочные шифры. Шифры Фейстеля и их обратимость. Российский стандарт шифрования ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров
12. Шифр “Кузнечик” из ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров
13. Ассиметричные блочные шифры. Схема Диффи-Хеллмана. Шифр RSA. Шифр Эль-Гамала. Шифр Шамира
14. Модификация асимметричных шифров на эллиптических кривых. Модификация схемы Диффи-Хеллмана. Модификация шифра Эль-Гамала. Модификация шифра Месси-Омуры
15. Хеш-функции. Требования, предъявляемые к хеш-функциям. Криптографические хеш-функции. Способы построения криптографических хеш-функций
16. Коды аутентификации. Понятие имитации и подмены сообщения. Нижние оценки для вероятностей успеха имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации
17. Электронная подпись. Электронная подпись на основе асимметричных систем шифрования: электронная подпись RSA, электронная

подпись Фиата-Шамира, электронная подпись Эль-Гамалая, электронная подпись Шнорра

18. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале

19. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу

20. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности

21. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн

22. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии

23. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации

24. Методы и средства инженерной защиты объектов информатизации

25. Программные и аппаратные средства защиты информации от несанкционированного доступа

26. Общие положения инженерно-технической защиты информации. Классификация технических каналов утечки информации

27. Скрытие демаскирующих признаков при противодействии техническим средствам разведки (ТСР)

28. Физические и технические основы противодействия видовой разведке. Технический контроль эффективности противодействия видовой разведке

Рекомендации по подготовке к контрольным вопросам раздела 4:

Вопросы 1-2 изложены в учебном пособии [7] на с. 20-62.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [11] на с. 15-25.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [12] на с. 50-57.

Вопросы 3-5 изложены в учебном пособии [8] на с. 8-31.

Вопрос 6 изложен в учебном пособии [8] на с. 59-66.

Для самостоятельного изучения вопроса 6 следует обратиться к учебному пособию [11] на с. 142-146.

Вопросы 7-8 изложены в учебном пособии [8] на с. 72-102.

Для самостоятельного изучения вопроса 7 следует обратиться к учебному пособию [11] на с. 193-214.

Для самостоятельного изучения вопроса 8 следует обратиться к учебному пособию [11] на с. 217-240.

Вопрос 9 изложен в параграфах 6.4-6.8 учебного пособия [15].

Вопрос 10 изложен в параграфе 6.9 учебного пособия [15].

Вопрос 11 изложен в параграфах 8.1-8.8 учебного пособия [15].

Для самостоятельного изучения вопроса 11 следует обратиться к учебному пособию [11] на с. 123-134.

Вопрос 12 изложен в параграфе 8.8 учебного пособия [15].

Вопрос 13 изложен в параграфах 9.1-9.7 учебного пособия [15].

Для самостоятельного изучения вопроса 13 следует обратиться к учебному пособию [11] на с. 135-141.

Вопрос 14 изложен в параграфах 9.2-9.7 учебного пособия [15].

Вопрос 15 изложен в параграфах 10.1-10.4 учебного пособия [15].

Для самостоятельного изучения вопроса 15 следует обратиться к учебному пособию [11] на с. 110-113.

Вопрос 16 изложен в параграфах 11.1-11.3 учебного пособия [15].

Вопрос 17 изложен в параграфах 12.1-12.7 учебного пособия [15].

Вопрос 18 изложен в учебном пособии [13] на с. 686-695.

Вопрос 19 изложен в учебном пособии [10] на с. 278-296.

Вопрос 20 изложен в учебном пособии [11] на с. 9-15, в учебном пособии [12] на с. 8-13.

Для самостоятельного изучения вопроса 20 следует обратиться к [3.7-3.9].

Вопрос 21 изложен в учебном пособии [12] на с. 62-71.

Для самостоятельного изучения вопроса 21 следует обратиться к [3.1, 3.3, 3.5 и 3.7].

Вопрос 22 изложен в учебном пособии [6] на с. 7-40.

Для самостоятельного изучения вопроса 22 следует обратиться к [3.2].

Вопрос 23 изложен в [3.5, 3.6].

Для самостоятельного изучения вопроса 23 следует обратиться к учебному пособию [6] на с. 7-40.

Вопрос 24 изложен в учебном пособии [13] на с. 280-299.

Для самостоятельного изучения вопроса 24 следует обратиться к учебному пособию [12] на с. 157-208.

Вопрос 25 изложен в учебном пособии [12] на с. 358-384.

Вопрос 26 изложен в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопроса 26 следует обратиться к [10] на с. 248-278.

Вопросы 27-28 изложены в учебном пособии [9] на с. 287-300.

Для самостоятельного изучения вопросов 27-28 следует обратиться к [10] на с. 248-278.

Индивидуальные задания по практике:

1. Изучить средства защиты баз данных, ОС, антивирусные средства и др., имеющиеся на предприятии
2. Ознакомиться с имеющимися на предприятии аппаратно-программными средствами защиты информации и документацией на них
3. Изучить имеющиеся на предприятии инструкции (руководства) по пропускному режиму, по обеспечению информационной безопасности

(перечни сведений, составляющих коммерческую тайну, персональные данные и др., соглашения о неразглашении и др.)

4. Изучить должностные инструкции специалистов по ИБ предприятия
5. Изучить имеющиеся на предприятии доступные руководящие документы, касающиеся защиты информации
6. Ознакомиться с имеющимися на предприятии криптографическими средствами защиты информации и документацией на них
7. Ознакомиться с порядком и документами лицензирования в области защиты информации предприятия
8. Ознакомиться с порядком и документами сертификации средств защиты предприятия
9. Ознакомиться с доступными методами и средствами инженерной защиты объектов информатизации предприятия
10. Ознакомиться с доступными программными и аппаратными средствами защиты информации от несанкционированного доступа предприятия
11. Ознакомиться с доступной пассивной и активной защитой от утечки информации по акустическому (виброакустическому) каналу
12. Ознакомиться с доступными методами и средствами пассивной и активной защиты от утечки в электромагнитном канале предприятия