МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Техническая защита информации»

Направление подготовки 10.03.01 – Информационная безопасность

Квалификация (степень) выпускника Бакалавр

Профиль (направленность) Информационно-аналитические системы финансового мониторинга

Академический бакалавриат

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Министерства образования и науки №1515 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

старший преподаватель _____ С.О. Иванов

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информационных систем
«30» августа 2017г., протокол №1

заведующий кафедрой _____ Д.В. Ильин

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета _____ А.В. Щипцова

Директор научной библиотеки _____ Н.Д. Никитина

Начальник управления информатизации _____ И.П. Пивоваров

Начальник учебно-методического управления _____ В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях.

Основными задачами дисциплины являются изучение:

- технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- способов и средств защиты информации, обрабатываемой техническими средствами;
- основ организации технической защиты информации на объектах информатизации.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Техническая защита информации» относится к числу дисциплин базовой части образовательной программы. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Физика», «Основы информационной безопасности».

Дисциплина является предшествующей для дисциплин: «Информационная безопасность web-ресурсов», «Аудит информационных технологий и систем обеспечения информационной безопасности», «Аттестация объектов информатизации по требованиям безопасности информации», прохождения преддипломной практики, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);
- способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);
- способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- нормативные правовые акты в области технической защиты информации (З1);
- угрозы безопасности информации и возможные пути их реализации (З2);
- особенности информационных элементов и технических средств объектов информатизации (З3);
- технические каналы утечки информации (З4);

уметь:

- использовать нормативные правовые акты в области технической защиты информации (У1);
- определять информационные ресурсы, подлежащие защите (У2);
- методами и средствами анализа защищенности объектов информатизации (У3);

- методами и средствами выявления каналов утечки информации (У4);

владеть:

- способами поиска нормативных правовых актов в области технической защиты информации (Н1);
- анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (Н2);
- аттестации объектов информатизации (Н3);
- технического контроля эффективности мер защиты информации (Н4).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (лабораторные работы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Технические каналы утечки информации	ОПК-7, ПК-12	З2, З4
Тема 1.1. Основные понятия и определения		
Тема 1.2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами		
Тема 1.3. Технические каналы утечки акустической (речевой) информации		
Раздел 2. Способы и средства защиты информации от утечки по техническим каналам	ОПК-7, ПК-12	У2,4, Н4
Тема 2.1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами		
Тема 2.2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам		
Раздел 3. Методы и средства контроля эффективности технической защиты информации	ОПК-5, ПК-5	З1, З3
Тема 3.1. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами		
Тема 3.2. Методы и средства контроля эффективности защиты выделенных помещений от		

утечки речевой информации по техническим каналам		
Тема 3.3. Методы и средства выявления электронных устройств негласного получения информации		
Раздел 4. Организация технической защиты информации	ОПК-5, ПК-5	У1,3, Н1,3
Тема 4.1. Основы физической защиты объектов информатизации		
Тема 4.2. Организация технической защиты информации на объектах информатизации		
РГР	ОПК-5, ОПК-7, ПК-5, ПК-12	У3, Н3, Н4
Экзамен	ОПК-7, ПК-5, ПК-12	З2,34, У2,3,4

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Технические каналы утечки информации								
Тема 1.1. Основные понятия и определения	4	2				2		
Тема 1.2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	16	4	8			4	4	
Тема 1.3. Технические каналы утечки акустической (речевой) информации	4	2				2		
Раздел 2. Способы и средства защиты информации от утечки по техническим каналам								
Тема 2.1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	16	4	8			4	4	
Тема 2.2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	12	4				8	2	
Раздел 3. Методы и средства контроля эффективности технической защиты информации								
Тема 3.1. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	8	2				6	2	
Тема 3.2. Методы и средства контроля	8	2	4			2	2	

эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам								
Тема 3.3. Методы и средства выявления электронных устройств негласного получения информации	12	4	4			4	2	
Раздел 4. Организация технической защиты информации								
Тема 4.1. Основы физической защиты объектов информатизации	4	2				2		
Тема 4.2. Организация технической защиты информации на объектах информатизации	22	6	8			8	6	
РГР	2				2			
Экзамен	36							36
Итого	144 4 з.е.	32	32	0	2	42	22	36

5. Содержание разделов дисциплины

5.1. Лекции и лабораторные занятия

Раздел 1. Технические каналы утечки информации

Тема 1.1. Основные понятия и определения

Лекция 1. Основные понятия и определения

Технические разведки и их цели. Классификация технической разведки по физической природе носителя информации. Характеристика объекта информатизации (выделенного помещения), как объекта защиты от технических разведок. Основные и вспомогательные технические средства и системы. Контролируемая зона объекта. Определение технического канала утечки информации. Цели и задачи защиты информации от утечки по техническим каналам (технической защиты информации).

Тема 1.2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Лекция 2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

Лабораторное занятие 1. Побочные электромагнитные излучения средств вычислительной техники

Лабораторное занятие 2. Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях

Тема 1.3. Технические каналы утечки акустической (речевой) информации

Лекция 3. Технические каналы утечки акустической (речевой) информации

Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный) канал утечки речевой информации.

Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.

Раздел 2. Способы и средства защиты информации от утечки по техническим каналам

Тема 2.1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Лекция 4. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).

Лабораторное занятие 3. Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением

Лабораторное занятие 4. Пассивные и активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях

Тема 2.2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Лекция 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Способы и средства защиты вспомогательных технических средств и систем.

Раздел 3. Методы и средства контроля эффективности технической защиты информации

Тема 3.1. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Лекция 6. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений. Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники.

Тема 3.2. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Лекция 7. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика оценки возможностей средств акустической разведки по перехвату речевой информации.

Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Лабораторное занятие 5. Контроль эффективности защиты выделенных помещений с использованием систем виброакустической маскировки.

Тема 3.3. Методы и средства выявления электронных устройств негласного получения информации

Лекция 8. Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

Лабораторное занятие 6. Выявление средств акустической разведки по перехвату речевой информации.

Раздел 4. Организация технической защиты информации

Тема 4.1. Основы физической защиты объектов информатизации

Лекция 9. Основы физической защиты объектов информатизации

Классификация категорий объектов и выбор условий их защиты. Модель «нарушителя» и возможные пути его проникновения на охраняемый объект. Общие положения современной концепции защиты объектов. Особенности, основные задачи и способы обеспечения физической защиты объектов информатизации. Назначение, типы и основные характеристики системы сбора, обработки и отображения информации. Назначение, виды и основные характеристики систем охраны, используемых на объектах информатизации.

Тема 4.2. Организация технической защиты информации на объектах информатизации

Лекция 10. Лицензирование и сертификация.

Нормативные документы по технической защите информации. Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации.

Лекция 11. Аттестация объектов информатизации.

Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию. Порядок проведения категорирования технических средств и систем и аттестации объектов информатизации (выделенных помещений) требованиям безопасности информации. Исходные данные по аттестуемому объекту информатизации. Специальное обследование объекта информатизации. Аттестационные испытания. Заключение аттестационной проверки объекта информатизации. Аттестат соответствия.

Лабораторное занятие 7. Аттестация помещения.

5.2. Вопросы для самостоятельной работы студента.

1. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»
2. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»
3. Многофункциональный комплекс радиомониторинга и выявления каналов утечки информации «АРК-Д1ТИ»

4. Комплекс «RS turbo»

5. Комплекс для измерениия характеристик акустических сигналов СПРУТ-7
6. Портативная рентгенотелевизионная установка «НОРКА»
7. Secret Net
8. Электронный замок «СОБОЛЬ»
9. Считыватели «Proximity»
10. Кейс «ТЕНЬ»
11. Устройство для быстрого уничтожения информации на жестких магнитных дисках «СТЕК-Н»

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской).

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;

– лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на экзамене и зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме экзамена, защиты расчетно-графической работы. Принимается экзамен преподавателем, читающим лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для

контроля знаний обучающихся.

7.1. Вопросы к экзамену

1. Методы активной маскировки.
2. Поясните сущность энергетической и неэнергетической маскировок.
3. Функции электросиловых сетей как каналов утечки информации.
4. Каким образом могут использоваться телефонные линии в каналах утечки информации?
5. Функции анализатора линий.
6. В каких режимах обследуются схемы силовых и телефонных линий?
7. Основные технические возможности анализаторов линий.
8. В каких случаях применяют активные средства защиты речевой информации?
9. Что представляют собой активные средства защиты речевой информации?
10. Назовите наиболее эффективный способ защиты телефонных каналов связи.
11. Перечислите известные Вам программно-аппаратные средства защиты компьютерной информации от несанкционированного доступа.
12. Перечислите функции программно-аппаратного комплекса Secret Net 5.0.
13. Назовите состав устройства ввода идентификационных признаков на базе идентификаторов Proximity.
14. Перечислите основные узлы смарт-карты.
15. Перечислите категории объектов, подлежащих охране.
16. Что относят к техническим средствам физической защиты информации?
17. Основные задачи, решаемые физическими средствами защиты.
18. Состав системы обеспечения безопасности объектов.
19. Что входит в состав системы охранно-тревожной сигнализации?
20. Что входит в состав системы контроля и управления доступом?
21. Что входит в состав системы пожарной сигнализации и пожаротушения?
22. Перечислите возможный состав периметровой охраны.
23. На каких принципах базируется обеспечение безопасности объекта?
24. Что предусматривают адекватные меры защиты?
25. Назначение системы охранно-тревожной сигнализации.
26. Назначение датчиков системы охранной сигнализации.
27. Средства, применяемые для записи видеосигналов.
28. Разделение охранных извещателей по физическому принципу действия.
29. Назовите основные типы извещателей.
30. Принципы действия пожарных извещателей.
31. Функции системы контроля и управления доступом на объекте.
32. Назначение системы пожарной сигнализации (ПС).
33. Какого типа бывают пожарные оповещатели?
34. Перечислите функциональные зоны охраны объекта.
35. В каких случаях применяются периметровые средства охраны?
36. Требования к периметровой системе охраны.
37. Принципиальные преимущества тепловизионных средств наблюдения за объектами.
38. Принцип действия емкостного средства обнаружения нарушителя.
39. Принцип действия радиолучевых охранных систем.
40. Принцип работы радиоволновой охранной системы.
41. Что понимают под аттестацией объектов информатизации?
42. Какие документы являются нормативно-техническими при проведении аттестации объектов?
43. Какие полномочия предоставляет действующий «Аттестат соответствия»?
44. Какие объекты подлежат обязательной аттестации?

45. Какие оценки включает в себя разведдоступность объекта информатизации?
46. Из какого комплекса работ состоит проверка возможности утечки информации по техническим каналам?
47. Что представляют собой специальные проверки объекта защиты?
48. Комплекс каких мероприятий входит в специальные обследования объекта защиты?
49. Для чего производится легендирование специальных обследований выделенных помещений?
50. Из каких действий состоят поисковые мероприятия на объекте?
51. С какой целью проводятся специальные исследования?
52. Что является конечным результатом специальных исследований?
53. Какие объекты являются исследуемыми при проведении специальных исследований в области акустики?
54. На чем базируется действующая методика измерений акустических и виброакустических характеристик различных сред?
55. Перечислите типовые подсистемы современного программноаппаратного комплекса для акустических измерений, например, «Спрут-7»?
56. Как определяется реальное затухание сигнала в виброакустическом канале утечки речевой информации?
57. Что понимают под прямым акустоэлектрическим преобразованием?
58. Что понимают под модуляционным акустоэлектрическим преобразованием?
59. Демаскирующие признаки сетевых акустических закладок.
60. Демаскирующие признаки проводной микрофонной системы подслушивания.
61. Демаскирующие признаки автономных некамуфлированных акустических закладок.
62. Демаскирующие признаки сетевых акустических закладок.
63. Демаскирующие признаки полуактивных акустических радиозакладок.
64. Демаскирующие признаки акустических и телефонных закладок с передачей на высокой частоте.
65. Причины возникновения паразитной генерации усилителей.
66. Почему опасно самовозбуждения усилителя?
67. Назовите наиболее простой способ выявления факта модуляции сигнала модуляционного акустоэлектрического преобразователя.

7.2. Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

7.3. Выполнение и примерные задания расчетно-графической работы

Расчетно-графическая работа выполняется в процессе изучения дисциплины. Общее руководство и контроль за ходом выполнения расчетно-графической работы осуществляет преподаватель соответствующей дисциплины. Расчетно-графическая работа выполняется в соответствии с методическими указаниями для обучающихся.

Основными функциями руководителя расчетно-графической работы являются:

определение и формулирование задания расчетно-графической работы;

консультирование по вопросам содержания и последовательности выполнения расчетно-графической работы;

оказание помощи студенту в подборе необходимой литературы;

контроль хода выполнения расчетно-графической работы.

Примерные задания для выполнения расчетно-графической работы:

- Провести анализ возможностей других видов разведки по перехвату информации с компьютера в помещении, расположенном на первом этаже, предложить способы предотвращения утечки этой информации.
- Провести анализ способов защиты переговоров по телефону от подслушивания при помощи диктофонов и других устройств, которые могут быть подключены к телефонному кабелю
- Предложить способы, снижающие возможности перехвата телеметрической информации с борта испытываемой крылатой ракеты (КР) аппаратурой разведки.
- Определить требования к пассивной и активной защите помещения, в котором находятся телефон спецсвязи и закладное устройство (радиомикрофон).
- Определить возможности космического аппарата (КА) РРТР по обнаружению РЭС, перехвату речевых сообщений и определению местоположения РЭС (с использованием однопозиционного метода и моноимпульсного амплитудного способа пеленгования РЭС).
- Определить расстояние, на котором можно перехватить изображение компьютера и устройств ввода и восстановить изображение и оценить требования к средствам защиты.
- Оценить возможность перехвата речевой информации из рабочего кабинета через вентиляцию, закрытое и открытое окно и оценить требования к средствам защиты..
- Оценить возможности аппаратуры радиоразведки, установленной на разведывательном самолете, по обнаружению излучения наземной РЭС и перехвату телеметрического сообщения.
- Провести анализ демаскирующих признаков и оценку защищенности помещения, в котором проводятся переговоры, подлежащие защите от технических разведок.
- Провести анализ демаскирующих признаков помещения с компьютером подлежащем обязательной защите от перехвата разведкой. Определить возможно опасные виды технических разведок, возможные технические каналы утечки информации, оценить возможности потенциально опасных видов разведки по перехвату информации, циркулирующей в компьютере.

Оценивание расчетно-графической работы осуществляется в соответствии с полнотой и качеством выполнения задания на работу, качеством защиты работы (ответы на вопросы, презентация и др.). Оценка работы отражает уровень сформированности соответствующих компетенций.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература.

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с. URL: http://window.edu.ru/resource/611/63611
2.	Титов А.А. Технические средства защиты информации [Электронный ресурс] : учебное пособие / А.А. Титов. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 194 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/13989.html
3.	Бурькова Е.В. Физическая защита объектов информатизации [Электронный ресурс] : учебное пособие / Е.В. Бурькова. — Электрон. текстовые данные. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 с. — 978-5-7410-1697-8. — Режим доступа: http://www.iprbookshop.ru/71349.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Торокин, Анатолий Алексеевич.Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. — М.: Гелиос АРВ, 2005. — 960 с.: ил.
2.	Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации.: Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
3.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
4.	Xgu.ru.	http://xgu.ru/wiki/
5.	Российская Государственная Библиотека	http://www.rsl.ru
6.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
7.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
8.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
9.	Научная электронная библиотека	http://elibrary.ru
10.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
11.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

Для реализации программы обучения используется лаборатория в области технической защиты информации, оснащённая:

специализированным оборудованием по защите информации от утечки по акустическому каналу и по каналу побочных электромагнитных излучений и наводок (Система виброакустического зашумления "СонатаАВ мод.3М"в сост. виброизлучатель пьезоэлектрический ВИ-3М и ПИ-3М,аудиоизлучатель АИ-3М; Устройство защиты "МП-1А" ; Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН "Соната-Р" - 1; Фильтр сетевой помехоподавляющий "ФСП-1Ф-7А");

техническими средствами контроля эффективности защиты информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок (Устройство поисковое многофункциональное "ST 033"; Комплекс проведения акустических и виброакустических измерений "Спрут-мини-А"; Комплекс обнаружения радиоизлучающих средств и радиомониторинга "Крона"; Имитатор многофункциональный "ИМФ-2"; Прибор-приставка АСК-4106 комбинированный).

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с

целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы.

Формы организации студентов на лабораторных работах: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.