МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра информационной безопасности и систем связи

Авторы-составители: **Карпов Михаил Юрьевич**
Никитина Елена Юрьевна

Рабочая программа дисциплины

ПРОТИВОДЕЙСТВИЕ ТЕХНИЧЕСКИМ СРЕДСТВАМ РАЗВЕДКИ

Код УМК 69464

Утверждено
Протокол №6
от «26» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Противодействие техническим средствам разведки

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в вариативную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность

специализация Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Противодействие техническим средствам разведки** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

ПК.12 Способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований

ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

ПК.20 Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации

ПК.21 Способность принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации

ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

4. Объем и содержание дисциплины

Направления подготовки	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	11
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение практических занятий, семинаров	56
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Письменное контрольное мероприятие (8)
Формы промежуточной аттестации	Экзамен (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Противодействие техническим средствам разведки.Первый семестр

Нормативные документы, регламентирующие инженерно-техническую защиту информации

1) Перечень сведений конфиденциального характера;
2) Федеральные законы:
   - об информации, информационных технологиях и защите информации;
   - о коммерческой тайне;
   - персональных данных;
   - об утверждении перечня сведений конфиденциального характера;
3) Специальные требования и рекомендации по защите информации конфиденциального характера;
4) Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам;
5) Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах.

Виды защищаемой информации, классификация источников информации, источники опасных сигналов

1) Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности её защиты.
2) Понятие о демаскирующих признаках объектов защиты. Характеристики и особенности.
3) Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности. Видовые, сигнальные и вещественные демаскирующие признаки. Понятие о признаковых структурах.
4) Основные видовые демаскирующие признаки объектов наблюдения.
5) Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства и системы.
6) Побочные электромагнитные излучения и наводки.
7) Акустоэлектрические преобразователи, их виды и принципы работы.
8) Высокочастотное навязывание. Методы реализации. Высокочастотные и низкочастотные побочные электромагнитные излучения технических средств и систем.
9) Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС. Паразитные наводки в цепях электропитания, заземления, в токопроводящих конструкциях помещений.

Органы разведки и технические средства дистанционного добывания информации

1) Роль разведки в деятельности государств и коммерческих структур. Структура органов разведки.
2) Виды зарубежной разведки и разведки коммерческих структур. Классификация технической разведки по физической природе носителя. Носители технических средств разведки. Принципы ведения разведки.
3) Принципы доступа к источникам информации без физического проникновения к контролируемую зону.
4) Классификация и характеристики наземных средств дистанционного съема информации с носителей. Принципы доступа к источникам информации без нарушения государственной границы.
5) Возможности зарубежной космической, воздушной и морской разведки в мирное время.

Технические каналы утечки информации, способы перехвата информативных сигналов

1) Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура и основные характеристики ТКУИ. Способы комплексного

использования злоумышленниками технических каналов утечки информации
2) Оптические каналы утечки информации. Структура оптического канала утечки информации. Характеристики среды распространения оптичееских лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации. Варианты оптических каналов утечки информации для типовых контролируемых зон организации.
3) Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации.
4) Акустические каналы утечки информации. Структура акустического канала утечки информации. Отражение и поглощение акустических волн в среде распространения.

Технические средства измерения сигналов, способы и методики работы
1) Принципы конструкции и работы, виды и характеристики анализаторов спектра;
2) Особенности конструкции и эксплуатации программно-аппаратных измерительных комплексов;
3) Виды и характеристики селективных микровольтметров и селективных нановольтметров;
4) Характеристики активных и пассивных антенн для измерения электромагнитных полей;
5) Принципы работы и характеристики генераторов НЧ и ВЧ сигналов.

Специальные электронные устройства несанкционированного перехвата информации
1) Способы и средства подслушивания акустических сигналов;
2) Структура и характеристики технических средств подслушивания. Классификация и характеристики микрофонов;
3) Виды и принципы работы остронаправленных микрофонов. Стетоскопы;
4) Принципы работы и характеристики диктофонов для скрытной записи;
5) Классификация и характеристики закладных устройств;
6) Варианты камуфлирования закладных устройств;
7) Способы и средства лазерного подслушивания и ВЧ-навязывания.

Технические средства и тактические способы выявления устройств несанкционированного перехвата информации
Ознакомление студентов с основными принципами работы различных технических средств контроля окружающей обстановки. В ходе работы студенты с помощью имеющихся поисковых технических средств должны выявить замаскированные имитаторы закладных устройств, ознакомиться с основными принципами установки ЗУ на объектах, потренироваться в обнаружении имитаторов ЗУ различными средствами контроля.
Замечание: занятия проводится в лаборатории информационной безопасности с использованием технических средств контроля кафедры ПУиИБ ПГУ, а также на территории ЗАО «Проминформ».

Аттестация защищаемых помещений по требованиям безопасности информации
1) Понятие ограждающих конструкций защищаемого помещения, границы контролируемой зоны, охраняемой территории;
2) Непреднамеренное прослушивание речевой конфиденциальной информации, нормативы защищенности;
3) Строительные требования и рекомендации по доработке защищаемого помещения до требований безопасности информации;
4) Методика инструментального контроля акустической и виброакустической защищенности защищаемого помещения;
5) Технические средства контроля звукоизоляции ограждающих конструкций защищаемого помещения;
6) Технические средства активной защиты, обеспечивающие выполнение требований безопасности

информации;
7) Методика расчета защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу;
8) Требования к организационно-распорядительной документации подготавливаемой при аттестации защищаемого помещения;
9) Порядок и методика проведения аттестации защищаемого помещения.

Аттестация средств вычислительной техники по требованиям безопасности информации
1) Понятие границы контролируемой зоны, охраняемой территории;
2) Технические требования к проводным коммуникациям объекта информатизации, нормативы защищенности;
3) Требования к помещению, в котором располагается объект информатизации;
4) Методика инструментального контроля электромагнитных и магнитных полей создаваемых средствами вычислительной техники, проверка коммуникаций сети электропитания;
5) Методика инструментального контроля заземления объекта информатизации;
6) Технические средства контроля электромагнитных и магнитных полей;
7) Технические средства активной защиты, обеспечивающие выполнение требований безопасности информации;
8) Методика расчета защищенности СВТ от утечки информации по техническим каналам;
9) Требования к организационно-распорядительной документации подготавливаемой при аттестации объекта информатизации;
10) Порядок и методика проведения аттестации средств вычислительной техники и технических средств размножения документов.

Волоконно - оптические линии связи. Технические каналы утечки информации и защита от несанкционированного доступа в них

Способы и средства инженерной защиты и технической охраны
1) Сущность инженерной защиты и технической охраны источников информации;
2) Понятие об информационном портрете объекта защиты. Способы изменения информационного портрета при маскировке и дезинформировании;
3) Зависимость качества информации от отношения мощностей носителя информации и помехи. Сущность энергетического скрытия;
4) Показатели эффективности инженерно-технической защиты информации;
5) Концепция охраны объектов. Категорирование объектов охраны;
6) Демаскирующие признаки злоумышленника и стихийных сил (пожара, воды). Модели злоумышленников. Уровни физической безопасности объектов охраны. Типовая структура системы охраны. Системы автономной и централизованной охраны;
7) Показатели эффективности инженерно-технической охраны объектов;
8) Способы и средства инженерной защиты объектов. Типовые инженерные конструкции. Естественные и искусственные преграды;
9) Структура комплекса технических средств охраны. Классификация извещателей;
10) Способы и средства видеоконтроля. Структура системы видеоконтроля.

Организация инженерно-технической защиты информации
1) Основные направления инженерно-технической защиты информации в организации. Сущность организационных и технических мер по защите информации в организации;
2) Задачи и виды контроля эффективности защиты информации.

3) Виды моделей угроз информации: путей физического проникновения злоумышленника к источнику и каналов утечки. Методические рекомендации по определению путей проникновения злоумышленника к источнику информации, формы моделей;
4) Типовые индикаторы каналов утечки. Методические рекомендации по моделированию каналов утечки. Формы представления результатов моделирования. Рекомендации по оценке угроз безопасности информации;
5) Основные способы и средства защиты информации от типовых вариантов угроз. Рекомендации по оценке затрат на защиту и форме их представления.

Итоговое контрольное мероприятие

Итоговая теоретическая контрольная работа. Студенты должны продемонстрировать знание основных принципов организации инженерно-технической защиты объекта.

Волоконно - оптические линии связи. Технические каналы утечки информации и защита от несанкционированного доступа в них

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Торокин А. А. Иженерно-техническая защита информации:учеб. пособие/А. А. Торокин.-М.:Гелиос АРВ,2005, ISBN 5-85438-140-0.-960.-Библиогр.: с. 934-949

Дополнительная:

1. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки:учеб. пособие/Ю. К. Меньшаков.-М.:РГГУ,2002, ISBN 5-7281-0487-8.-399.-Библиогр.: с. 396-399

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Противодействие техническим средствам разведки** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

1. Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice», Alt Linux;
2. Электронно-измерительное оборудование (измерители параметров электрических цепей, осциллографы и т.п.).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий требуется аудитория, оснащенная презентационной тех-никой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения практических занятий - компьютерный класс. Состав оборудования определен в Паспорте компьютерного класса.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.

Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

Дополнительно при освоении дисциплины используются технические средства контроля защищенности информации и техника защиты информации, имеющаяся в лаборатории информационной безопасности, а также предполагаются выездные занятия на базе лабораторий специальных исследований и специальных проверок ЗАО «Проминформ» в составе:

1. Программно-аппаратный комплекс «Сигурд» на базе анализатора спектра
2. Программно-аппаратный комплекс «Легенда» на базе анализатора спектра «Agilent Tchnologies 4405B» (выездное занятие в ЗАО «Проминформ»)
3. Измерительные антенны электромагнитных сигналов (комплект антенн в диапазоне 0,009 – 10000 МГц)
4. Комплект тестовых программ
5. Генератор высокочастотный IFR 2064 (выездное занятие в ЗАО «Проминформ»)
6. Цифровой осциллограф DSO 6032A
7. Программно-аппаратный комплекс оценки акустоэлектрических преобразований «Талис-НЧ-Лайт»
8. Селективный микровольтметр SMV 8,5(выездное занятие в ЗАО «Проминформ»)
9. Селективный микровольтметр SMV 11 (выездное занятие в ЗАО «Проминформ»)
10. Селективные нановольтметры «Unipan» мод. 232B, 237 (выездное занятие в ЗАО «Проминформ»)
11. Генератор низкочастотный Г3 – 118 (выездное занятие в ЗАО «Проминформ»)
12. Тестовое автоматизированное рабочее место (выездное занятие в ЗАО «Проминформ»)
13. Измеритель шума и вибраций «Ассистент» версия 1
14. Генератор тестового аку

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Противодействие техническим средствам разведки

Планируемые результаты обучения по дисциплине для формирования компетенции и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.12 Способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований	Знать основные понятия в области информационной безопасности Знать основные требования нормативно-методических документов ФСТЭК России по безопасности информации Знать методику выполнения измерений на лабораторной технике Знать порядок выполнения работ по аттестации объектов информатизации Знать как подразделяются объекты информатизации Знать порядок оформления отчетной документации по результатам проведенных исследовательских работ Уметь выполнять измерения сигналов на различных средствах измерений в ходе проведения экспериментально-исследовательских работ Уметь правильно оформить и интерпретировать полученные результаты исследовательских работ	**Неудовлетворител** Знает менее 50% основных понятий в области информационной безопасности Не знает основные требования нормативно-методических документов ФСТЭК России по безопасности информации Не знает методику выполнения измерений Не может представить алгоритм выполнения работ по аттестации различных объектов информатизации Не знает основные требования по порядку оформления отчетной документации Не может оформить (с отдельными ошибками) полученные результаты исследовательских работ Не может сделать оценку защищенности объекта на основании полученных результатов измерений Не умеет работать с техническими средствами измерений, представленными в ходе проведения экспериментально-исследовательских работ **Удовлетворительн** Знает не менее 50% основных понятий в области информационной безопасности Знает основные требования нормативно-методических документов ФСТЭК России по безопасности информации Частично знает методику выполнения измерений Может в общих чертах представить алгоритм выполнения работ по аттестации различных объектов информатизации Знает основные требования по порядку оформления отчетной документации Может оформить (с отдельными ошибками) полученные результаты исследовательских

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн работ Не может сделать оценку защищенности объекта на основании полученных результатов измерений Неуверенно может работать с техническими средствами измерений, представленными в ходе проведения экспериментально-исследовательских работ **Хорошо** Знает не менее 60% основных понятий в области информационной безопасности На хорошем уровне знает основные требования нормативно-методических документов ФСТЭК России по безопасности информации Знает методику выполнения измерений Знает требования по порядку оформления отчетной документации Хорошо знает (с отдельными неточностями) алгоритм выполнения работ по аттестации различных объектов информатизации Может оформить (с отдельными ошибками) полученные результаты исследовательских работ Может сделать оценку защищенности объекта на основании полученных результатов измерений Уверенно может работать с техническими средствами измерений, представленными в ходе проведения экспериментально-исследовательских работ **Отлично** Знает все основные понятия в области информационной безопасности Знает основные требования нормативно-методических документов ФСТЭК России по безопасности информации Знает в деталях методику выполнения измерений Знает требования по порядку оформления отчетной документации Хорошо знает алгоритм выполнения работ по аттестации различных объектов информатизации

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Может оформить полученные результаты исследовательских работ Может сделать качественную оценку защищенности объекта на основании полученных результатов измерений Уверенно работает с техническими средствами измерений, представленными в ходе проведения экспериментально-исследовательских работ
ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения	Знать базовые модели решения профессиональной задачи. Уметь построить правильную модель решения учебно-практической задачи на основании имеющихся исходных данных. Уметь правильно интерпретировать полученные экспериментальные данные. Уметь теоретически обосновать выбранный алгоритм решения учебно-практической задачи.	**Неудовлетворител** Не знает, как правильно решать учебно-практические задачи Не знает, как применить полученные экспериментальные данные Не способен обосновать правильность применяемых средств и методов выбранных для решения учебно-практической задачи **Удовлетворительн** Знает менее 50% теории построения модели решения учебно-практических задач Может на основании полученных экспериментальных данных (с частичными ошибками) обосновать оценку защищенности объекта Частично способен обосновать правильность применяемых средств и методов выбранных для решения учебно-практической задачи **Хорошо** Хорошо знает (с некоторыми неточностями) теорию построения модели решения учебно-практических задач Может на основании полученных экспериментальных данных (с ошибками) обосновать оценку защищенности объекта Способен обосновать правильность применяемых средств и методов выбранных для решения учебно-практической задачи **Отлично** Отлично знает теорию построения модели решения учебно-практических задач Может на основании полученных экспериментальных данных обосновать оценку защищенности объекта

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Способен без ошибок обосновать правильность применяемых средств и методов выбранных для решения учебно-практической задачи
ПК.20 Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации	Знать виды оборудования по защите информации. Владеть навыками оценки технического состояния средств измерения и защиты информации Уметь выполнить мелкий ремонт и регламентные работы с оборудованием	**Неудовлетворител** Не способен оценить техническое состояние средств измерения и защиты информации Не знает порядок проведения регламентных работ с оборудованием Не может выполнить (с подсказками) мелкий ремонт оборудования **Удовлетворительн** В общих чертах способен оценить техническое состояние средств измерения и защиты информации Частично знает порядок проведения регламентных работ с оборудованием Мелкий ремонт оборудования способен выполнить самостоятельно не более чем на 50% **Хорошо** Способен оценить техническое состояние средств измерения и защиты информации Знает порядок проведения регламентных работ с оборудованием Мелкий ремонт оборудования способен выполнить самостоятельно не более чем на 70% **Отлично** Способен оценить техническое состояние средств измерения и защиты информации Знает порядок проведения регламентных работ с оборудованием Мелкий ремонт оборудования способен выполнить самостоятельно
ПК.21 Способность принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты	Уметь восстановить работоспособности оборудования Знать порядок настройки/ регулировки оборудования защиты информации Уметь настроить оборудование защиты на основании	**Неудовлетворител** Не умеет восстановить работоспособности оборудования В общих чертах знает порядок настройки оборудования защиты информации Не умеет настроить оборудование защиты на основании полученных экспериментальных данных

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
информации	полученных экспериментальных данных	**Удовлетворительн** Может (с частичными подсказками) восстановить работоспособности оборудования Знает не менее 50% методики настройки оборудования защиты информации Умеет (с подсказками) настроить оборудование защиты на основании полученных экспериментальных данных **Хорошо** Может самостоятельно восстановить работоспособности оборудования Знает не менее 70% методики настройки оборудования защиты информации Умеет настроить оборудование защиты на основании полученных экспериментальных данных **Отлично** Может самостоятельно восстановить работоспособность оборудования Знает методики настройки оборудования защиты информации Умеет безошибочно настроить оборудование защиты на основании полученных экспериментальных данных
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Знать организационно-режимные меры защиты объектов информатизации Знать средства и методы организации технической защиты информации на объектах информатизации Знать программные способы защиты, уметь установить и настроить систему антивирусной защиты	**Неудовлетворител** Знает менее 50% основных требований при защите объектов информатизации организационно-режимными методами Не знает условий применения различных средств технической защиты информации Не знает методы организации технической защиты информации на объектах информатизации Не может представить алгоритм выполнения работ по комплексной технической защите объектов информатизации Не знает основные средства антивирусной защиты, достоинства и недостатки каждого Знает менее 50% порядка установки и настройки средства антивирусной защиты в компьютерную систему **Удовлетворительн** Знает не менее 50% основных требований при защите объектов информатизации

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн организационно-режимными методами Знает не менее 50% условия применения различных средств технической защиты информации Знает в общих чертах методы организации технической защиты информации на объектах информатизации Не может представить алгоритм выполнения работ по комплексной технической защите объектов информатизации Не знает основные средства антивирусной защиты, достоинства и недостатки каждого Знает менее 50% порядка установки и настройки средства антивирусной защиты в компьютерную систему **Хорошо** Знает не менее 70% основных требований при защите объектов информатизации организационно-режимными методами Знает условия применения различных средств технической защиты информации Знает (с неточностями) методы организации технической защиты информации на объектах информатизации Представляет алгоритм выполнения работ по комплексной технической защите объектов информатизации Знает (с неточностями) основные средства антивирусной защиты, достоинства и недостатки каждого Знает порядок установки и настройки средства антивирусной защиты в компьютерную систему **Отлично** Знает основных требований при защите объектов информатизации организационно-режимными методами Знает условия применения различных средств технической защиты информации Знает методы организации технической защиты информации на объектах информатизации Представляет алгоритм выполнения работ по комплексной технической защите объектов

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично информатизации Знает основные средства антивирусной защиты, достоинства и недостатки каждого Знает порядок установки и настройки средства антивирусной защиты в компьютерную систему

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.12 Способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований	Нормативные документы, регламентирующие инженерно-техническую защиту информации **Письменное контрольное мероприятие**	Устная контрольная работа, включающая в себя набор терминов из обозначенного раздела, требований нормативных документов, методик выполнения работПрактическая учебно – исследовательская работа на различном оборудовании
ПК.20 Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации **ПК.21** Способность принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации	Технические средства измерения сигналов, способы и методики работы **Письменное контрольное мероприятие**	Письменная работа, включающая в себя решение учебно-практической задачи на основании имеющихся экспериментальных данных

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.20 Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации **ПК.21** Способность принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации	Специальные электронные устройства несанкционированного перехвата информации **Письменное контрольное мероприятие**	Практическая учебно – исследовательская работа на различном оборудовании объединяющая компетенции ПК.20 и ПК.21Письменная работа, включающая в себя знание методик выполнения ремонтных, регламентных и настроечных работ
ПК.12 Способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Аттестация защищаемых помещений по требованиям безопасности информации **Письменное контрольное мероприятие**	Устная контрольная работа, включающая в себя набор терминов из обозначенного раздела, требований нормативных документов, методик выполнения работПрактическая учебно – исследовательская работа на различном оборудованииПисьменная работа, включающая в себя решение учебно-практической задачи на основании имеющихся экспериментальных данных

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.20 Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Аттестация средств вычислительной техники по требованиям безопасности информации **Письменное контрольное мероприятие**	Устная контрольная работа, включающая в себя набор терминов из обозначенного раздела, требований нормативных документов, методик выполнения работПрактическая учебно – исследовательская работа на различном оборудованииПисьменная работа, включающая в себя решение учебно-практической задачи на основании имеющихся экспериментальных данных
ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения **ПК.20** Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации	Волоконно - оптические линии связи. Технические каналы утечки информации и защита от несанкционированного доступа в них **Письменное контрольное мероприятие**	Письменная работа, включающая в себя определение мер и мероприятий по защите информации техническими и программными средствами, обоснование лучших вариантов защиты

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.20 Способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Способы и средства инженерной защиты и технической охраны **Письменное контрольное мероприятие**	Письменная работа, включающая в себя определение мер и мероприятий по защите информации техническими и программными средствами, обоснование лучших вариантов защиты
ПК.12 Способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований **ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Итоговое контрольное мероприятие **Письменное контрольное мероприятие**	Письменная работа, включающая в себя набор понятий и терминов дисциплины, нормативных актов, ответ на 2 теоретических вопроса, требующих знаний обучаемого для построения ответа, ответ на практическое задание

Спецификация мероприятий текущего контроля

Нормативные документы, регламентирующие инженерно-техническую защиту информации

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Знать основные понятия и определения из нормативных документов по защите информации	4
Знать технические каналы утечки информации, особенности возникновения и реализации	3
Знать виды защищаемой информации, классификацию источников опасных сигналов	2
Знать принципы действия органов разведки и технические средства дистанционного добывания информации	1

Технические средства измерения сигналов, способы и методики работы

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Способность выполнить учебно – практическую задачу с применением средств измерения опасных сигналов	10
Знать устройство и принципы функционирования основных технических средств измерения опасных сигналов	6
Уметь выполнить подключение, регулировку, настройку средств измерения опасных сигналов	4

Специальные электронные устройства несанкционированного перехвата информации

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Способность выполнить учебно – практическую задачу с применением приборов и устройств поиска СЭУ НПИ	5
Знать устройство, принципы функционирования и возможности приборов и устройств поиска СЭУ НПИ	3
Знать устройство и принципы функционирования специальных электронных устройств негласного получения информации	2

Аттестация защищаемых помещений по требованиям безопасности информации

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Способность выполнить учебно – практическую задачу с применением приборов	3

измерения параметров АЭП	
Уметь по заданным параметрам обосновать критерии защиты помещения по требованиям безопасности информации	2
Знать способы доработки помещений до требований нормативно-методической документации ФСТЭК России по безопасности информации в части защищаемых помещений	2
Знать причины возникновения акустоэлектрических преобразований (АЭП) в технических средствах	2
Знать общие положения по специальным исследованиям акустических и виброакустических каналов	1

Аттестация средств вычислительной техники по требованиям безопасности информации

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Знать порядок аттестации объектов информатизации (средств вычислительной техники)	3
Знать средства и методы организации защиты информации техническими и программными средствами	2
Уметь установить и настроить систему антивирусной защиты	2
Знать приемы антивирусной защиты при работе с компьютерными системами	2
Знать основные понятия и определения из нормативных документов по аттестации объектов информатизации	1

Волоконно - оптические линии связи. Технические каналы утечки информации и защита от несанкционированного доступа в них

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Знать угрозы безопасности волоконно-оптических технологий, приемы перехвата информации в ВОЛС и методы защиты	3
Уметь осуществить контроль ВОЛС с применением технических средств контроля	3
Знать основные понятия и определения из нормативных документов по организации и построению ВОЛС	2
Знать применение волоконно-оптических технологий в различных сферах деятельности	2

Способы и средства инженерной защиты и технической охраны

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Уметь обосновать выбор представленной системы охраны по технико-экономическим показателям в рамках учебно-практической задачи	4
Знать основные понятия и определения из нормативных документов по организации и построению систем охраны	3
Знать применение и особенности построения многорубежных систем охраны	3

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Уметь решать прикладные задачи по технической защите информации	10
Знать основные понятия и нормативные документы по защите информации	10