МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Мустакимова Яна Романовна**
Карпов Михаил Юрьевич

Рабочая программа дисциплины

ПРОТИВОДЕЙСТВИЕ ТЕХНИЧЕСКИМ СРЕДСТВАМ РАЗВЕДКИ

Код УМК 93532

Утверждено
Протокол №1
от «28» июня 2024 г.

Пермь, 2024

1. Наименование дисциплины

Противодействие техническим средствам разведки

2. Место дисциплины в структуре образовательной программы

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

Специальность: **10.05.04** Информационно-аналитические системы безопасности
специализация Информационная безопасность финансовых и экономических структур

3. Планируемые результаты обучения по дисциплине

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

10.05.04 Информационно-аналитические системы безопасности (специализация : Информационная безопасность финансовых и экономических структур)

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикаторы

ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

4. Объем и содержание дисциплины

Специальность	10.05.04 Информационно-аналитические системы безопасности (специализация: Информационная безопасность финансовых и экономических структур)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	9
Объем дисциплины (з.е.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	144
Проведение лекционных занятий	36
Проведение практических занятий, семинаров	36
Проведение лабораторных работ, занятий по иностранному языку	72
Самостоятельная работа (ак.час.)	72
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (4)
Формы промежуточной аттестации	Экзамен (9 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

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, 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 съема 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 информационных 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 оптических 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 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.

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 к ним

1) История развития оптических систем передачи информации. Принципы построения волоконно-оптических сетей. Оптические кабели. Пассивные компоненты ВОЛС. Активные компоненты ВОЛС. Проектирование ВОЛС. Основы технической эксплуатации ВОЛС.
2) Основные и вспомогательные технические средства и системы, их классификация и характеристика. Виды побочных опасных электромагнитных излучений. Паразитные связи и наводки опасных сигналов. Технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации. Защита информации от несанкционированного доступа в технических каналах утечки информации.

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.

Критическая информационная инфраструктура. Понятие и способы защиты
1) Понятие критической информационной инфраструктуры (КИИ);
2) Основные требования к объектам КИИ, нормативы защищенности;
3) Критерии определения требуемого уровня защиты для объекта КИИ;
3) Требования к объекту КИИ, в котором располагается объект информатизации;
4) Взаимодействие с объектами ГОССОПКА;
5) Требования к организационно-распорядительной документации подготавливаемой при аттестации объекта информатизации объекта КИИ;
6) Порядок и методика проведения аттестации средств вычислительной техники объекта КИИ.

Персональные данные. Защита информационных систем обработки персональных данных
1) Понятие границы контролируемой зоны, охраняемой территории;
2) Нормативно-методическая документация ФСТЭК России по обработке персональных данных;
3) Нормативно-распорядительная документация, разрабатываемая для информационной системы обрабатывающего персональные данные (ИСПДн);
3) Требования к помещению, в котором располагается объект информатизации (ИСПДн);
4) Методика инструментального контроля электромагнитных и магнитных полей создаваемых средствами вычислительной техники, проверка коммуникаций сети электропитания для ИСПДн;
5) Технические средства активной защиты, обеспечивающие выполнение требований безопасности информации;
6) Методика расчета защищенности СВТ от утечки информации по техническим каналам;
7) Требования к организационно-распорядительной документации подготавливаемой при аттестации ИСПДн;

Итоговое контрольное мероприятие
Итоговая теоретическая контрольная работа. Студенты должны продемонстрировать знание основных принципов организации инженерно-технической защиты объекта. Представить и защитить учебно-практическую работу
по аттестации объекта информатизации.

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. Инженерно-техническая защита информации:учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности/А. А. Торокин.-Москва:Гелиос АРВ,2005, ISBN 5-85438-140-0.-960.-Библиогр.: с. 934-949

Дополнительная:

1. Технические средства обеспечения информационной безопасности.учебное пособие/Министерство образования и науки Российской Федерации; сост. А. П. Зайцев.-Томск:Томский межвузовский центр дистанционного образования,2004.Ч. 1.Технические каналы утечки информации/Томский университет автоматизированных систем управления и радиоэлектроники (ТУСУР), Кафедра КИБЭВС.-2004.-199

2. Технические средства обеспечения информационной безопасности.учебное пособие/Министерство образования и науки Российской Федерации; сост. А. П. Зайцев.-Томск:Томский межвузовский центр дистанционного образования,2004.Ч. 2.Средства защиты информации от утечки по техническим каналам/Томский государственный университет систем управления и радиоэлектроники (ТУСУР), Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС).-2004.-279

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

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

При освоении дисциплины использование ресурсов сети Интернет не предусмотрено.

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:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).

Перечень используемого программного обеспечения:
- операционная система "ALT Linux"
- офисный пакет приложений "Libre office";
- программа просмотра интернет контента (браузер)
Специализированное программное обеспечение Лаборатории радиотехнических средств защиты информации.

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

Аудитория для лекционных занятий - Специализированный учебный кабинет «Лекционный кабинет» (защищённое помещение по конфиденциальной информации), оборудованный: специализированная мебель, телевизор, маркерная доска.

Аудитория для семинарских (практических) занятий, групповых (индивидуальных) консультаций, текущего контроля и промежуточной аттестации оборудованная: специализированная мебель, компьютер/ноутбук, проектор, экран/телевизор, меловая или маркерная доска.

Аудитория для лабораторных занятий - Лаборатория радиотехнических средств защиты информации, оборудованная: специализированная мебель, лабораторное оборудование, проектор, экран, персональные компьютеры, маркерная доска, специализированное оборудование и программное обеспечение.

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. Индикаторы и критерии их оценивания

ОПК.11

Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Может анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	**Неудовлетворител** Не знает основные требования по информационной безопасности. Не умеет использовать информационные технологии выявления уязвимостей АС в своей профессиональной деятельности с учетом требований информационной безопасности. Не владеет методиками анализа программных и аппаратных методов защиты от несанкционированного доступа к информации с учетом требований информационной безопасности. **Удовлетворительн** Знает основные требования по информационной безопасности. Не умеет использовать информационные технологии выявления уязвимостей АС в своей профессиональной деятельности с учетом требований информационной безопасности. Не владеет методиками анализа программных и аппаратных методов защиты от несанкционированного доступа к информации с учетом требований информационной безопасности. **Хорошо** Знает основные требования по информационной безопасности. Умеет использовать информационные технологии выявления уязвимостей АС в своей профессиональной деятельности с учетом требований информационной безопасности. Не владеет методиками анализа

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо программных и аппаратных методов защиты от несанкционированного доступа к информации с учетом требований информационной безопасности. **Отлично** Знает основные требования по информационной безопасности. Умеет использовать информационные технологии выявления уязвимостей АС в своей профессиональной деятельности с учетом требований информационной безопасности. Владеет методиками анализа программных и аппаратных методов защиты от несанкционированного доступа к информации с учетом требований информационной безопасности.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : для ИАСБ

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 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
	Нормативные документы, регламентирующие инженерно-техническую защиту информации **Письменное контрольное мероприятие**	Умеет применять методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации
	Технические каналы утечки информации, способы перехвата информационных сигналов **Письменное контрольное мероприятие**	Знает методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Аттестация защищаемых помещений по требованиям безопасности информации **Письменное контрольное мероприятие**	Может анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Аттестация средств вычислительной техники по требованиям безопасности информации **Письменное контрольное мероприятие**	Знает технические каналы утечки информации, возникающие при обработке информации ограниченного доступа в автоматизированных системах.Умеет анализировать взаимосвязь возникновения потенциальных каналов утечки информации с архитектурно-техническими и схемотехническими решениями, реализованными в автоматизированных системах.Может грамотно обосновать применение различных средств и методов защиты информации в автоматизированных системах
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Знает средства и методы защиты информации в компьютерных системах и сетях, защиты информации от утечки по техническим каналам.Умеет решать профессиональные задачи при реализации средств и методов защиты информации в различных системах. Может грамотно анализировать различные автоматизированные системы обработки информации и выявлять возможные уязвимости.

Спецификация мероприятий текущего контроля

Нормативные документы, регламентирующие инженерно-техническую защиту информации

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает виды защищаемой информации, источники опасных сигналов. Органы разведки и технические средства дистанционного съема информации Имеет четкое представление о Перечне сведений конфиденциального характера, Федеральных законах: - об информации, информационных технологиях и защите информации; - о коммерческой тайне; - персональных данных; - об утверждении перечня сведений конфиденциального характера; Знает основные положения Специальных требований и рекомендаций по защите информации конфиденциального характера; Может уверенно оперировать понятиями Временной методики оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам и Временной методики оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах.	11.8
Знает в общих чертах виды защищаемой информации, источники опасных сигналов. Органы разведки и технические средства дистанционного съема информацииЗнает перечень сведений конфиденциального характера, Федеральные законы: - об информации, информационных технологиях и защите информации; - о коммерческой тайне; - персональных данных; - об утверждении перечня сведений конфиденциального характера; Имеет общее представление о Специальных требованиях и рекомендациях по защите информации конфиденциального характера;Может в общих чертах рассказать о временной методике оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам и временной методике оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах.	8.2

Технические каналы утечки информации, способы перехвата информационных сигналов

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **10**

Показатели оценивания	Баллы
Знает все характеристики каналов утечки информации. Имеет представление о структуре технических каналов утечки информации. Понимает отличия технического канала утечки информации от канала связи.Знает виды технических каналов утечки информации. Может подробно рассказать о способах комплексного использования злоумышленниками технических каналов утечки информации Имеет представление о технических средствах измерения сигналов, способы и методики работы Понимает принципы конструкции и работы, виды и характеристики анализаторов спектра; Знает особенности конструкции и эксплуатации программно-аппаратных измерительных	11.8

комплексов; Характеристики активных и пассивных антенн для измерения электромагнитных полей; 5) Принципы работы и характеристики генераторов НЧ и ВЧ сигналов. Знает специальные устройства несанкционированного перехвата информации Знает способы и средства подслушивания акустических сигналов; Классификация и характеристики закладных устройств; Типовые варианты камуфлирования закладных устройств; Умеет работать с имеющимися поисковыми техническими средствами	
Знает некоторые технические каналы утечки информации и характеристики каналов утечки информации. Имеет общее представление о структуре технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Типовая структура и основные характеристики ТКУИ. Способы комплексного использования злоумышленниками технических каналов утечки информации Знает некоторые технические средства измерения сигналов, способы и методики работыИмеет представление о специальных устройствах несанкционированного перехвата информации Знает частично способы и средства подслушивания акустических сигналов; Может применить (с подсказками) некоторые технические средств контроля окружающей обстановки.	8.2

Аттестация защищаемых помещений по требованиям безопасности информации

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает на хорошем уровне порядок аттестации защищаемых помещений по требованиям безопасности информацииИмеет четкое понятие ограждающих конструкций защищаемого помещения, границы контролируемой зоны, охраняемой территории, а также о непреднамеренном прослушивание речевой конфиденциальной информации, нормативы защищенности; Уверенно знает Строительные требования и рекомендации по доработке защищаемого помещения до требований безопасности информации и Методику инструментального контроля акустической и виброакустической защищенности защищаемого помещения; Может использовать Методику расчета защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу; Знает требования к организационно-распорядительной документации подготавливаемой при аттестации защищаемого помещения;	11.2
Имеет общее представление об аттестация защищаемых помещений по требованиям безопасности информацииИмеет понятие об ограждающих конструкций защищаемого помещения, границы контролируемой зоны, охраняемой территории; Частично знает Строительные требования и рекомендации по доработке защищаемого помещения до требований безопасности информации; Знает обобщенно Методику инструментального	8.2

контроля акустической и виброакустической защищенности защищаемого помещения и технические средства контроля звукоизоляции ограждающих конструкций защищаемого помещения;Может использовать (с подсказками) Методику расчета защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу; Может подготовить (с некритичными ошибками) организационно-распорядительную документацию подготавливаемой при аттестации защищаемого помещения;	

Аттестация средств вычислительной техники по требованиям безопасности информации

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знает уверенно порядок аттестации средств вычислительной техники по требованиям безопасности информацииЗнает понятие границы контролируемой зоны, охраняемой территории, технические требования к проводным коммуникациям объекта информатизации, нормативы защищенности; Уверенные знания по Методике инструментального контроля электромагнитных и магнитных полей создаваемых средствами вычислительной техники, проверка коммуникаций сети электропитания, Методике инструментального контроля заземления объекта информатизации, Методике расчета защищенности СВТ от утечки информации по техническим каналам; Уверенно знает Требования к организационно-распорядительной документации подготавливаемой при аттестации объекта информатизации и Может разработать порядок и методику проведения аттестации средств вычислительной техники и технических средств размножения документов. Знает Волоконно-оптические линии связи, технические каналы утечки информации и защита от несанкционированного доступа к нимЗнает Способы и средства инженерной защиты и технической охраныЗнает основные положения по критическая информационная инфраструктура. Понятие и способы защитыМожет определить класс и категорию ИСПДн. Защита информационных систем обработки персональных данных	11.8
Знает общий порядок аттестации средств вычислительной техники по требованиям безопасности информацииИмеет представление о понятии границы контролируемой зоны, охраняемой территории, о технических требованиях к проводным коммуникациям объекта информатизации, нормативы защищенности; Знает в общих чертах Методику инструментального контроля электромагнитных и магнитных полей создаваемых средствами вычислительной техники, проверка коммуникаций сети электропитания, Методику инструментального контроля заземления объекта информатизации, Методику расчета защищенности СВТ от утечки информации по техническим каналам;Знает общие	8.2

требования к организационно-распорядительной документации подготавливаемой при аттестации объекта информатизации; Знает приблизительно порядок и методику проведения аттестации средств вычислительной техники и технических средств размножения документов. Знает общие сведения о волоконно-оптические линии связи, технические каналы утечки информации и защита от несанкционированного доступа к ним Имеет представление о способах и средствах инженерной защиты и технической охраны Знает обобщенно о критической информационной инфраструктуре. Понятие и способы защитыУмеет определить класс персональных данных. Защита информационных систем обработки персональных данных	

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
УдовлетворительноЗнает не менее 50% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Умеет (с ошибками) применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Не владеет основными навыками работы со средствами защиты информации.	4.1
НеудовлетворительноЗнает менее 50% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Не умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Не владеет основными навыками работы со средствами защиты информации.	2
ХорошоЗнает не менее 70% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Владеет (с ошибками) основными навыками работы со средствами защиты информации.	2
ОтличноЗнает основные требования при решении учебно-теоретических и практических задач в области защиты информации; Отлично умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Владеет навыками работы со средствами защиты информации	1.9