МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.

_____ "___" _____ 20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Техническая защита информации Б3.Б.7

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Математические и программные средства защиты информации
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Сулимов А.И.

Рецензент(ы):

Ишмухаметов Ш.Т.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Шерстюков О. Н.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 911217

Казань
2017

Содержание

Программу дисциплины разработал(а)(и) младший научный сотрудник, б/с Сулимов А.И. НИЛ СВЧ проектирование и радиотелекоммуникации Институт физики , Amir.Sulimov@kpfu.ru

1. Цели освоения дисциплины

Целью дисциплины "Техническая защита информации" является формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения применять специальные знания для решения конкретных научно-практических задач. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.Б.7 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, 7 семестр.

Задачи дисциплины - дать знания по:

- концепции инженерно-технической защиты информации;
- теоретическим основам инженерно-технической защиты информации;
- физическим основам инженерно-технической защиты информации;
- техническим средствам добывания и методам противодействия им;
- организационным основам инженерно-технической защиты информации;
- методическому обеспечению инженерно-технической защиты информации.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-2 (общекультурные компетенции)	способность осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
ОК-7 (общекультурные компетенции)	способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства
ПК-1 (профессиональные компетенции)	способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности
ПК-11 (профессиональные компетенции)	способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации
ПК-14 (профессиональные компетенции)	способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-21 (профессиональные компетенции)	способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов
ПК-23 (профессиональные компетенции)	способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности
ПК-25 (профессиональные компетенции)	способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью
ПК-27 (профессиональные компетенции)	способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
ПК-3 (профессиональные компетенции)	способность использовать нормативные правовые документы в своей профессиональной деятельности
ПК-4 (профессиональные компетенции)	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
ПК-6 (профессиональные компетенции)	способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов

В результате освоения дисциплины студент:

1. должен знать:

- виды, источники и носители защищаемой информации;
- основные угрозы безопасности информации;
- концепцию инженерно-технической защиты информации;
- методы оценки угрозы инженерно-технического добывания информации;
- основные принципы организации и методы реализации технической защиты информации;
- основные руководящие и нормативные документы в сфере инженерно-технической защите информации;
- методику организации инженерно-технической защиты информации;

2. должен уметь:

- различать виды защищаемой информации, идентифицировать её источники и носители;
- выявлять основные угрозы безопасности информации и оценивать их степень;
- использовать основные принципы и методы инженерно-технической защиты информации;
- использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации;

3. должен владеть:

- методами аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем передачи, хранения и обработки информации;
- методами инженерного расчета размеров контролируемой зоны;
- навыками работы с профессиональными аппаратными средствами инженерно-технической защиты информации.

4. должен демонстрировать способность и готовность:
- применять полученные знания в своей дальнейшей профессиональной деятельности

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) 180 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 7 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Концепция технической защиты информации	7	1-2	4	2	0	Устный опрос
2.	Тема 2. Утечка информации по техническим каналам	7	3-4	4	0	6	Устный опрос
3.	Тема 3. Основные принципы технической защиты информации	7	5-6	4	4	4	Устный опрос
4.	Тема 4. Организационные основы технической защиты информации	7	7	2	2	0	Устный опрос
5.	Тема 5. Технические средства добывания информации	7	8-9	4	2	4	Устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов	7	10-11	6	2	0	Устный опрос
7.	Тема 7. Методы противодействия утечке и добыванию информации	7	12-13	4	2	4	Устный опрос
8.	Тема 8. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	7	14-15	4	2	0	Устный опрос
9.	Тема 9. Моделирование процессов технической защиты информации	7	16-17	4	2	0	Контрольная работа Устный опрос
.	Тема . Итоговая форма контроля	7		0	0	0	Экзамен
	Итого			36	18	18	

4.2 Содержание дисциплины

Тема 1. Концепция технической защиты информации

лекционное занятие (4 часа(ов)):

Системный подход к защите информации. Характеристика инженерно-технической защиты информации. Основные параметры системы защиты информации. Основные концептуальные положения инженерно-технической защиты информации.Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Методика проведения аттестация технических средств защиты информации. Оценка эффективности технической защиты информации"

Тема 2. Утечка информации по техническим каналам

лекционное занятие (4 часа(ов)):

Информации как предмет защиты. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Источники опасных сигналов. Основные и вспомогательные технические средства и системы, их классификация и характеристика. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований. Виды побочных опасных электромагнитных излучений. Паразитные связи и наводки опасных сигналов. Характеристика технической разведки. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации. Технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

лабораторная работа (6 часа(ов)):

Лабораторная работа по теме "Обнаружение опасных сигналов закладных устройств в проводных и электросетевых линиях". Лабораторная работа по теме "Обнаружение опасных сигналов оптических закладных устройств, работающих в ИК-диапозоне"

Тема 3. Основные принципы технической защиты информации

лекционное занятие (4 часа(ов)):

Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

практическое занятие (4 часа(ов)):

Практическое занятие по теме: "Статистический анализ загрузки заданного радиодиапазона, обнаружение и локализация радиозакладных устройств в защищаемом помещении"

лабораторная работа (4 часа(ов)):

Лабораторная работа по теме "Методы инженерно-технической защиты информации". Лабораторная работа по теме "Поиск и обнаружение радиозакладных устройств с помощью универсальных зондовых приборов".

Тема 4. Организационные основы технической защиты информации

лекционное занятие (2 часа(ов)):

Государственная система защиты информации. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Контроль эффективности инженерно-технической защиты информации.Требования по защите информации от утечки по техническим каналам Виды технического контроля.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Поиск и подбор нормативной-правовой технической документации при разработке системы технической защиты информации"

Тема 5. Технические средства добывания информации

лекционное занятие (4 часа(ов)):

Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.Средства инженерной защиты и технической охраны. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Поиск и локализация закладных устройств по их демаскирующим признакам"

лабораторная работа (4 часа(ов)):

Лабораторная работа по теме "Обнаружение и локализация средств электроники методами нелинейной радиолокации"

Тема 6. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов

лекционное занятие (6 часа(ов)):

Распространение сигналов в технических каналах утечки информации. Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Оценка протяжённости технических каналов утечки информации".

Тема 7. Методы противодействия утечке и добыванию информации

лекционное занятие (4 часа(ов)):

Средства предотвращения утечки информации по техническим каналам.Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции и звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Расчёт параметров активных и пассивных технических средств противодействия утечке информации".

лабораторная работа (4 часа(ов)):

Лабораторные занятия по теме "Постановка помех для противодействия техническим средствам добывания информации"

Тема 8. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

лекционное занятие (4 часа(ов)):

Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утеку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Оценка характерных радиусов (R1 и R2) распространения побочных электромагнитных излучений и наводок от технических средств обработки информации".

Тема 9. Моделирование процессов технической защиты информации

лекционное занятие (4 часа(ов)):

Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по оценке эффективности защиты информации. Оценка эффективности защиты видовых признаков объектов наблюдения. Оценка дальности перехвата опасных сигналов.

практическое занятие (2 часа(ов)):

Практическое занятие по теме: "Оптимизация параметров средств инженерно-технической защиты информации".

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1	Тема 1. Концепция					

технической защиты информации

7	1-2	подготовка к

устному опросу

8	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Утечка информации по техническим каналам	7	3-4	подготовка к устному опросу	8	устный опрос
3.	Тема 3. Основные принципы технической защиты информации	7	5-6	подготовка к устному опросу	8	устный опрос
4.	Тема 4. Организационные основы технической защиты информации	7	7	подготовка к устному опросу	4	устный опрос
5.	Тема 5. Технические средства добывания информации	7	8-9	подготовка к устному опросу	8	устный опрос
6.	Тема 6. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов	7	10-11	подготовка к устному опросу	12	устный опрос
7.	Тема 7. Методы противодействия утечке и добыванию информации	7	12-13	подготовка к устному опросу	8	устный опрос
8.	Тема 8. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	7	14-15	подготовка к устному опросу	8	устный опрос
9.	Тема 9. Моделирование процессов технической защиты информации	7	16-17	подготовка к контрольной точке	4	контрольная точка
				подготовка к устному опросу	4	устный опрос
	Итого				72	

5. Образовательные технологии, включая интерактивные формы обучения

Занятия проводятся в форме лекций и лабораторных работ. Материалы лекций демонстрируются с помощью мультимедийного оборудования, допускаются дискуссии, обсуждения, совместные решения типичных задач, связанных с практической деятельностью в рамках рассматриваемой темы. Лабораторные работы посвящены формированию основных практических навыков по дисциплине и призваны сформировать у студентов навыки самостоятельного решения задач. Часть заданий по лабораторным работам выполняется с использованием профессиональных технических средств инженерно-технической защиты информации, другая часть выполняется с привлечением персонального компьютера. Контроль осуществляется в форме проверки домашних заданий и контрольных работ, а также обсуждения отчётов по результатам выполнения лабораторных работ.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Концепция технической защиты информации

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Что собой представляет техническая защита информации? 2) Каковы принципиальные отличия технической защиты информации от прочих методов обеспечения информационной безопасности? 3) Каковы цели и задачи технической защиты информации? 4) На каком структурном уровне организации информационных систем работает техническая защита информации (согласно модели OSI)? 5) Что представляет собой информация и носитель защищаемой информации? 6) Что собой представляет инженерно-техническое добывание информации? 7) Какие виды инженерно-технического добывания информации вам известны? 8) Что собой представляет системный подход к защите информации? 9) Какие характеристики и показатели эффективности инженерно-технической защиты информации вам известны? 10) Назовите основные параметры системы технической защиты информации? 11) Назовите основные направления инженерно-технической защиты информации?

Тема 2. Утечка информации по техническим каналам

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Что собой представляет утечка информации? 2) Что собой представляет технический канал утечки информации? 3) Основные классификации технических каналов утечки информации? 4) Какие разновидности технических каналов утечки речевой информации вам известны? 5) В чём состоит принципиальное отличие технических каналов утечки от других каналов передачи информации? 6) Каковы основные характеристики технических каналов утечки информации? 7) Что такое "опасные сигналы"? 8) Что такое "демаскирующие признаки объектов наблюдения"? 9) Какие разновидности демаскирующих признаков вам известны? 10) Какие демаскирующие признаки сигналов вам известны? 11) Какие источники опасных сигналов вы можете назвать? 12) Что такое "вспомогательные технические средства и системы"? 13) Что собой представляют акустоэлектрические преобразования и как они способствуют утечке информации? 14) Какие технические каналы утечки вы можете идентифицировать в типичном офисном помещении? 15) Какие типы технических каналов утечки (оптических, акустических, радиоэлектронных, материально-вещественных и т.д.) представляют наибольшую угрозу информационной безопасности?

Тема 3. Основные принципы технической защиты информации

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Какие направления инженерно-технической защиты информации вам известны? 2) Какова классификация методов инженерно-технической защиты информации? 3) Какова итоговая цель (в терминах конкретных характеристик технических каналов утечки) всех методов инженерно-технической защиты информации? 4) Что собой представляют активные методы технической защиты информации? 5) Каковы недостатки активных методов технической защиты информации 6) Что собой представляют пассивные методы технической защиты информации? 7) Каковы недостатки пассивных методов технической защиты информации? 8) Каковы основные принципы технической охраны объектов? 9) Какие методы скрытия информации и ее носителей вам известны? 10) Что собой представляет звукоизоляция и чем она отличается от звукопоглощения? 11) Каково минимально необходимое отношение (сигнал/шум) для предотвращение утечки информации по техническим каналам различной физической природы? 12) Какие типы генерируемых помех вам известны?

Тема 4. Организационные основы технической защиты информации

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Какова структура государственной системы защиты информации? 2) Какие государственные ведомства курируют область технической защиты информации? 3) Какие руководящие, нормативные и методические документы по технической защите информации вам известны? 4) Что собой представляет сертификация контролируемого помещения? 5) Что такое "специальное обследование"? 6) Какова методика обследования контролируемого помещения на предмет наличия технических каналов утечки? 7) Какова методика обследования контролируемого помещения на предмет наличия устройств несанкционированного съёма информации? 8) Какие виды технического контроля эффективности защиты информации вам известны? 9) Где следует искать актуальный перечень сертифицированных технических средств защиты информации? 10) Какие организации г. Казани, имеющие лицензию на оказание услуг в области сертификации по технической защите информации, вам известны?

Тема 5. Технические средства добывания информации

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Что собой представляет "закладное устройство"? 2) Какие способы классификации закладных устройств вам известны? 3) Какие виды закладных устройств, различающихся по типу технического канала утечки информации, вам известны? 4) Какие типы закладных устройств, различающихся по типу источника питания, вам известны? 5) Какие типы закладных устройств, различающихся по регулярности режима работы, вам известны? 6) С какими техническими ограничениями сталкивается злоумышленник при разработке закладного устройства? 7) Каковы типичные значения основных технических характеристик наиболее распространённых закладных устройств? 8) Как оценить радиус действия закладного устройства? 9) Какие методы камуфляжа закладных устройств вам известны? 10) Какие демаскирующие признаки наиболее распространённых закладных устройств вам известны? 11) Как идентифицировать закамуфлированное закладное устройство по его демаскирующим признакам? 12) Каковы преимущества и недостатки закладных устройств, работающих в инфракрасном диапазоне? 13) Каковы принципы работы сканирующих радиоприемников и комплексов радиомониторинга? 14) Какие разновидности комплексов радиоконтроля и радиомониторинга вам известны? 15) Какие средства управления доступом вам известны?

Тема 6. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) На чём основана обобщённая методика оценки протяжённости технического канала утечки информации? 2) Что такое "разборчивость речи"? 3) Какие показатели разборчивости речи вам известны? 4) Какова методика расчёта показателей разборчивости речи? 5) Какова методика субъективной оценки разборчивости речи? 6) Какие методы подавления опасных акустических сигналов вам известны? 7) Каковы основные закономерности ослабления радиосигналов при их распространении? 8) Каковы основные закономерности распространения акустических волн? 9) Каковы основные закономерности распространения виброакустических возмущений в твёрдых телах? 10) Как оценить эффективность средств противодействия акустической утечке информации? 11) Как оценить дальность утечки информации по воздуховодным и вентиляционным конструкциям? 12) Как оценить угрозу утечки информации в телефонных линиях связи при её добывании по методу высокочастотного навязывания? 13) Как оценить угрозу утечки информации по оптикоэлектронному (лазерному) каналу?

Тема 7. Методы противодействия утечке и добыванию информации

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Какие методы противодействия радиоэлектронным каналам утечки вам известны? 2) Какие методы противодействия акустоэлектрическим каналам утечки вам известны? 3) Какие методы противодействия виброакустическим каналам утечки вам известны и в чём состоит их особенность? 4) Какие методы противодействия оптикоэлектронным каналам утечки вам известны? 5) Какие методы противодействия электрическим каналам утечки вам известны? 6) Какие методы противодействия перехвату телефонных переговоров вам известны? 7) Какие физические характеристики среды распространения сигналов влияют на дальность технических каналов утечки различной природы? 8) Какие типы средств зашумления вам известны? 9) Каковы основные принципы построения генераторов пространственного зашумления? 10) Каковы основные принципы построения генераторов линейного зашумления? 11) Каковы основные принципы построения генераторов виброакустической помехи? 12) Какие методы локализации закладных устройств вам известны? 13) В чём состоит принцип "акустозавязки" и в чём его недостатки? 14) В чём состоит принцип акустической триангуляции? 15) Что такое "прицельная помеха"?

Тема 8. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Что собой представляют "побочные электромагнитные излучения" (ПЭМИ) и какова их физическая природа? 2) В чём состоит принципиальное отличие ПЭМИ от радиоканалов передачи информации? 3) Что такое "наводки" и какова их физическая природа? 4) Что такое радиусы R1 и R2? 5) Как выглядит профиль стандартной функции ослабления ПЭМИ и что собой представляют ближняя, промежуточная и дальняя зоны ЭМИ? 6) Какой объект является элементарным излучателем побочных электрических полей? 7) Какой объект является элементарным излучателем побочных магнитных полей? 8) Какие ПЭМИ представляют более высокую угрозу утечки информации: электрические или магнитные? 9) Какова физическая природа ПЭМИ проводных линий? 10) В чём состоит принцип действия кабеля типа "витая пара"? 11) Какие типы паразитных электрических связей вам известны? 12) Какова феноменология утечки информации по цепям электропитания? 13) Какова феноменология утечки информации по цепям заземления? 14) Какие требования предъявляются к цепям заземления с точки зрения эффективности средств информационной безопасности? 15) Какие методы экранирования ПЭМИ вам известны? 16) Каковы основные принципы экранирования электрических полей? 17) Каковы основные принципы экранирования низкочастотных магнитных полей? 18) Что такое "магнитное сопротивление"? 19) Каковы основные принципы экранирования высокочастотных электромагнитных полей? 20) Каковы особенности экранирования проводных и кабельных линий? 21) Какие функциональные узлы персонального компьютера являются наиболее активными источниками ПЭМИ? 22) В чём состоит принцип перехвата ван Эйка? 23) В чём состоит принцип перехвата информации, набираемой на клавиатурных устройствах ввода?

Тема 9. Моделирование процессов технической защиты информации

контрольная точка , примерные вопросы:

Расчётное задание по оценке угрозы утечки информации по техническому каналу и расчёту параметров средств противодействия её техническому добыванию.

устный опрос , примерные вопросы:

Устный опрос проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции. Примеры вопросов для устного опроса по данному разделу: 1) Каковы основные этапы проектирования системы защиты информации? 2) Каковы основные принципы оптимизации системы технической защиты информации? 3) Каковы основные принципы моделирования объектов технической защиты? 4) Каковы основные принципы моделирования технических каналов утечки информации? 5) Каковы основные принципы моделирования каналов технического добывания информации? 6) Какие рекомендации по оценке значений параметров моделирования вы можете дать? 7) Каковы основные этапы алгоритма оценки дальности перехвата опасных сигналов?

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Оценка знаний студента производится в соответствии с рекомендациями балльно-рейтинговой системы. Расчётное задание оценивается в 10 баллов.

В зачётном и/или экзаменационном билете содержатся два вопроса, различающихся по объёму охватываемого материала и степени сложности

соответствующего им раздела дисциплины. Первый вопрос оценивается в 15 баллов, второй вопрос (как правило, более объёмный) - в 25 баллов.

После обсуждения вопросов, содержащихся в билете, студенту предлагается ряд дополнительных вопросов с общей оценкой 10 баллов. Дополнительные

вопросы задаются из перечня основных вопросов к зачёту/экзамену, из программы лабораторного практикума или расчётных заданий. Процесс контроля

выстроен таким образом, чтобы проверить успешность усвоения студентом основных и дополнительных компетенций, перечисленных в разделе 3.

Примеры вопросов для подготовки к зачёту:

1. Основные направления, методы и средства технического противодействия закладным устройствам.

2. Оптико-электронный канал утечки речевой информации. Лазерные микрофоны интерферометрического и дифференциально-интерферометрического принципов действия.

3. Понятие о демаскирующих признаках объекта. Демаскирующие признаки сигналов.

4. Механизм (методика, принцип) обнаружения и классификации опасных сигналов.

5. Методы локализации закладных устройств. Метод энергетического зондирования. Метод акустической и радиолокационной триангуляции.

6. Атрибуты и признаки потенциально опасного сигнала закладных устройств.

7. Государственная система (иерархия) в области технических средств защиты информации. Основные руководящие, нормативные и методические документы.

8. Технический контроль эффективности мер по защите информации. Общая методика проведения технического контроля (ПЭМИН, акустических и виброакустических каналов утечки).

Примеры экзаменационного билета:

Билет №1

1. Общая характеристика радиозакладных устройств. Спектральные характеристики сигналов радиозакладных устройств.

2. Применение звукопоглощающих и звукоизолирующих элементов и конструкций. Звукопоглощающие окна и двери. Резонаторные звукопоглотители.

Билет №2

1. Пассивные и активные методы противодействия акустическим каналам утечки информации.

2. Понятие о демаскирующих признаках объекта. Демаскирующие признаки сигналов.

Примеры расчётного задания:

1) Какова должна быть спектральная плотность шумового напряжения SU (в дБ относительно к 1мкВ/(кГц)^1/2) сигнала линейного зашумления,

подаваемого в цепь заземления, чтобы исключить в диапазоне частот от 9 кГц до 30 МГц возможность утечки информации от нагрузки 75 Ом,

находящейся под напряжением 12В? Известно, что в цепи заземления используется два параллельных штыревых заземлителя диаметром

14 мм и протяжённостью 31м. Тип заземляющего грунта - глина.

2) Оценить изменение предельной дальности передачи радиозакладного устройства мощностью 25 мВт до и после осуществления экранирования

контролируемого помещения сеточным экраном из проводящей проволоки. Шаг сетки экрана составляет 1 см, а радиус сечения проволоки 0,8 мм.

Рабочая частота радиозакладного устройства равна 330 МГц. Критическое отношение (сигнал/шум) принять равным SNR* = 5,

а среднеквадратичный уровень фоновых радиоизлучений σn = 2.3 мкВ.

7.1. Основная литература:

1) Аверченков, В. И. Методы и средства инженерно-технической защиты информации[электронный ресурс] : учеб.пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р.Гайнулин, - М.: ФЛИНТА, 2011. - 187 с. - Режим доступа:http://znanium.com/bookread.php?book=453848

2) Аверченков, В. И. Разработка системы технической защиты информации [электронныйресурс] : учеб.пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. - 2-еизд., стереотип. - М.: ФЛИНТА, 2011. - 187 с. - Режим доступа:http://znanium.com/bookread.php?book=453880

3) Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин.- 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: ил. - Режим доступа:http://znanium.com/bookread.php?book=474838

7.2. Дополнительная литература:

1) Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб.пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - М. : ФЛИНТА, 2011. - 184 с. - ISBN 978-5-9765-1272-6. Режим доступа: http://znanium.com/bookread.php?book=453862

2) Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4. Режим доступа: http://znanium.com/bookread.php?book=402686

7.3. Интернет-ресурсы:

Интернет-портал для ИТ-специалистов - http://www.habrahabr.ru/

Интернет-портал обзора рынка технических средств безопасности - http://www.sec.ru/

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал ресурсов по информационной безопасности - http//all-ib.ru

Официальный сайт Федеральной службы по техническому и экспортному контролю - http://www.fstec.ru/

Электронная библиотека по техническим наукам - http://techlibrary.ru

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Техническая защита информации" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Компьютерные классы и мультимедийные аудитории Института Вычислительной математики и Информационных технологий.

Лаборатория "Технические средства защиты информации" Института физики

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 090900.62 "Информационная безопасность" и профилю подготовки Математические и программные средства защиты информации .

Автор(ы):
Сулимов А.И. _____
"__" _____ 201 __ г.

Рецензент(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.