Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»

_____ Бурлов В.Г.

Утверждаю
Председатель УМС _____И.И. Палкин

Рекомендована решением
Учебно-методического совета
18 мая 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры
17 мая 2018 г., протокол № 5
Зав. кафедрой _____ Бурлов В.Г.

Авторы-разработчики:
_____Смирнов П.И
_____Алейникова О.В.

Санкт-Петербург 2018

1. Цели освоения дисциплины

Цели дисциплины «Техника защиты информации» – формирование базовых знаний и практических навыков по защиты информации от утечки по техническим каналам.

.

.**Задачи** изучения дисциплины: привить студентам навыки использования средств и методов защиты информации от утечки на объектах информатизации. Дать базовые знания об устройстве и принципах действия средств защиты информации. Научить студента формулировать задачи по защите информации. Обучить специалиста основам организации технической защиты информации на объектах информатизации и в выделенных помещениях

2. Место дисциплины в структуре ОП

Дисциплина «Техника защиты информации» для направления подготовки 10.05.02 – информационная безопасность телекоммуникационных систем относиться к дисциплинам базовой части блока дисциплин (модулей) (Б.3) профессионального цикла.

Для освоения данной дисциплины, необходимо обладать базовыми знаниями (общее среднее образование), а также освоить учебный материал предшествующих дисциплин: «Математика», «Физики», «Теория вероятностей и математическая статистика», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Основы информационный безопасности», «Организационно-правовое обеспечение».

Параллельно с дисциплиной «Техника защиты информации» изучаются дисциплины: «Защита программных средств защищенных ТКС», «Управление информационной безопасностью ТКС», «Защищенные корпоративные сети», «Интеллектуальные информационные системы», «Радиоразведка и радиопротиводействие», «Радиомониторинг».

Знания и практики, полученные обучаемыми по дисциплине «Техника защиты информации», непосредственно используются при написании выпускной работы студента и в практической профессиональной деятельности, связанной с защитой информации от утечки по техническим каналам.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ПК-14	способностью выявлять тенденции развития информационной безопасности телекоммуникационных систем
ПК-19	способностью проектировать защищённые телекоммуникационные системы и проводить анализ проектных решений по обеспечению безопасности телекоммуникационных систем
ПК-20	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду
ПК-24	способностью оценивать эффективность систем защиты информации в телекоммуникационных системах
ПК-25	способностью осуществлять аудит уровня защищенности и аттестацию телекоммуникационных систем
ПК-35	способностью проводить мониторинг, техническую диагностику

	средств защиты и оценку эффективности информационной безопасности защищенных телекоммуникационных систем

В результате освоения компетенций в рамках дисциплины обучающийся должен:

Знать:

- - возможности технических средств перехвата информации;
- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- основы физической защиты объектов информатизации;

Уметь:

- пользоваться нормативными документами по противодействию технической разведке;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять навыки по технической защите информации на объектах информатизации;

Владеть навыками:

- методами и средствами технической защиты информации;
- методами расчета и инструментального контроля показателей технической защиты информации;
- рационального выбора средств и методов защиты информации объектов информатизации.

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении	Способен изложить основное содержание современных	Знает основное содержание современных научных идей в	Может дать критический анализ современным

		рабочей области анализа	научных идей в рабочей области анализа	рабочей области анализа, способен их сопоставить	проблемам в заданной области анализа

4. Структура и содержание дисциплины

Общая трудоемкость (объем) дисциплины (модуля) составляет 4 зачетные единицы (ЗЕ*), 144 академических часа.

4.1. Структура дисциплины

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Семинар Лаборат. Практич.	Самост. работа			
1	Основы защиты информации	**10**	2	2	2	Ответ на экзамене. Отчеты по лабораторным работам	5/2	ПК-14
2	Техническая разведка	**10**	7	2	8	Ответ на экзамене Отчеты по лабораторным работам	10	ПК-19, ПК-20
3	Технические каналы утечки информации.	**10**	7	2	8	Ответ на экзамене. Отчеты по лабораторным работам	10	ПК-19, ПК-20
4	Средства выявления технических каналов утечки информации.	**10**	8	2	8	Ответ на экзамене. Отчеты по лабораторным работам	11/2	ПК-24, ПК-35
5	Защита информации от утечки по техническим каналам.	**10**	8	24	9	Ответ на экзамене Отчеты по лабораторным работам	28/12	ПК-19, ПК-25, ПК-20

	ИТОГО		32	32	35		16	

4.2. Содержание разделов дисциплины

4.2.1. Основы защиты информации.

Информация как объект защиты. Информационная безопасность Российской Федерации. Направления защиты информации. Система защиты информации. Основные мероприятия по защите информации. Мероприятия по контролю эффективности защиты информации

4.2.2. Техническая разведка.

Классификация технической разведки. Возможности видов технических разведок. Обработка разведывательной информации. Оценка возможностей технической разведки по добыванию информации. Характеристика разведывательного сообщества США

.

4.2.3. Технические каналы утечки информации.

Обобщенная модель технического канала утечки информации. Опасные сигналы. Классификация технических каналов утечки информации. Побочные электромагнитные излучения и зоны пространственной защиты информации. Демаскирующие признаки объектов защиты.

4.2.4. Средства выявления технических каналов утечки информации.

Индикаторы электромагнитного поля. Сканирующие радиоприемники. Автоматизированные комплексы радиоконтроля. Комплексы оценки защищенности технических средств по каналу ПЭМИН. Комплексы оценки защищенности информации от утечки по акустическому и виброакустическому каналам. Многофункциональный комплект для выявления каналов утечки информации «Пиранья». Нелинейные локаторы. Металлодетекторы. Портативные рентгено-телевизионные установки. Досмотровые эндоскопы

4.2.5. Защита информации от утечки по техническим каналам.

Экранирование электромагнитных полей. Заземление технических средств. Фильтрация информационных сигналов. Маскирование информационных сигналов ПЭМИН. Маскирование акустических речевых сигналов

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тема занятия	Форма проведения	Формируемые компетенции
1	1	Постановка задачи защиты информации от утечки по техническим каналам	Лабораторная	ПК-14
2	2	Методы и средства бесконтактного съема информации с проводной линии	Лабораторная	ПК-19, ПК-20
3	3	Средства перехвата акустической информации	Лабораторная	ПК-19, ПК-20
4	4	Стандарты и методы измерения	Лабораторная	ПК-24, ПК-35

5	5	Изучение принципов работы скремблера	Лабораторная	ПК-19, ПК-25, ПК-20
6	5	Технические средства для обеспечения энергетической скрытности	Лабораторная	ПК-19, ПК-25, ПК-20
7	5	Звукоизоляция помещений	Лабораторная	ПК-19, ПК-25, ПК-20
8	5	Защита линий связи от утечки информации по акустическим и электрическим каналам	Лабораторная	ПК-19, ПК-25, ПК-20
10	5		Лабораторная	ПК-19, ПК-25, ПК-20

5. Учебно-методическое обеспечение самостоятельной работы студент и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль производится путем проверки и защиты отчетов лабораторных работ.

5.2. Методические указания по организации самостоятельной работы

Во время самостоятельной работы студенты знакомятся с существующими методами исследования технических каналов утечки информации и характеристик технических средств защиты информации от ее утечки по техническим каналам, читают методические указания по выполнению лабораторных работ, читают дополнительный материал в виде лекционных занятий, работают с методическими указаниями по написанию курсовой работы.

В перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Техника защиты информации» входит:

1. Методические указания по выполнению лабораторных работ.
2. Дополнительный лекционный материал

Контроль исполнения самостоятельных работ осуществляется преподавателем с участием студентов в форме обсуждения выполненных заданий и работ.

Источники для самостоятельной подготовки:

1. Технические средства и методы защиты информации от утечки по техническим каналам на объектах информатизации: учебное пособие. А.Е. Давыдов, Р.В. Максимов, О.К. Савицкий. – СПб.: Изд-во Политехн. ун-та, 2012. – 192 с.

5.3. Промежуточный контроль: зачет, экзамен, курсовая работа

Перечень вопросов для промежуточной аттестации (экзамен):

1) Защищенность систем передачи информации. Мешающие воздействия. Определение. Виды мешающих воздействий.
2) Защищенность систем передачи информации. Направленные действия противника (НДП). Определение. Виды НДП.

3)Технический канал утечки информации (ТКУИ). Определение. Классификация ТКУИ. Причины и источники образования ТКУИ. Постановка задачи защиты информации от утечки по техническим каналам.

4) Виды, источники и носители защищаемой информации в телекоммуникационных системах. Классификация каналов передачи информации.

5) Скрытие речевой информации в аналоговых каналах связи. Обобщенная структурная схема скремблера. Основные характеристики скремблеров. Сравнительный анализ скремблеров различных видов.

6) Временные скремблеры. Принцип работы. Виды. Структура.

7) Частотные скремблеры. Принципы работы. Виды. Структура.

8) Энергетическая, структурная и информационная скрытность. Постановка задачи обеспечения энергетической скрытности. Энергетический обнаружитель.

9) Энергетическая скрытность. Повышение энергетической скрытности СПИ при использовании прикрывающих сигналов.

10) .Энергетическая скрытность. Повышение энергетической скрытности СПИ при использовании широкополосных сигналов.

11) Энергетическая скрытность. Повышение энергетической скрытности СПИ при использовании принципа передачи сигналов с трансформацией временного масштаба.

12) Энергетическая скрытность. Активные технические средства для обеспечения энергетической скрытности. Классификация. Краткая характеристика.

13) Энергетическая, структурная и информационная скрытность. Постановка задачи обеспечения структурной скрытности. Цифровые маскираторы. Обобщенная структурная схема.

14) Структурная скрытность. Маскиратор на основе генератора М-ПСП.

15) Структурная скрытность. Маскиратор на основе нелинейной маскирующей последовательности.

16) Защита информации от утечки по акустическим каналам. Классификация акустических каналов утечки информации. Структура акустического канала утечки информации.

17) Защита информации от утечки по акустическим каналам. Физические преобразователи акустической информации.

18) Защита информации от утечки по акустическим каналам. Методы перехвата акустической информации.

19) Средства перехвата акустической информации. Активные радиозакладные устройства. Структура. Характеристики. Принципиальная схема простейшего радимикрофона.

20) Средства перехвата акустической информации. Полуактивные радиозакладные устройства. Структура. Характеристики.

21) Методы и средства защиты акустической информации. Акустические генераторы шума. Принципиальная схема генератора «белого» шума.

22) Методы и средства защиты акустической информации. Средства виброакустической, ультразвуковой защиты. Типовые характеристики. Технические средства защиты от радиозакладок.

23) Методы и средства защиты акустической информации. Звукоизоляция помещений.

24) Электрические каналы утечки информации. Классификация, краткая характеристика.
25) Электрические каналы утечки информации. Паразитные емкостные, индуктивные связи. Паразитные обратные связи через источники питания. Ассиметричная и симметричная наводка.
26) Электрические каналы утечки информации. Утечка информации по цепям заземления.
27) Электрические каналы утечки информации. Связь через ближнее электрическое и магнитное поля. Связь через общее полное сопротивление.
28) Методы и средства бесконтактного съема информации с проводной линии.
29) Защита линий связи от утечки информации по электрическим каналам. Экранирование.
30) Защита линий связи от утечки информации по электрическим каналам. Приборы для постановки активной заградительной помехи.
31) Защита линий связи от утечки информации по электрическим каналам. Методы контроля проводных линий.
32) Защита линий связи от утечки информации по электрическим каналам. Типовые схемы защиты телефонных аппаратов.
33) Экранирование помещений. Эффективность экранов. Материалы для изготовления экрана. Требования к изготовлению экранов.
34) Технические каналы утечки информации при эксплуатации ЭВМ. Классификация, краткая характеристика.
35) Технические каналы утечки информации при эксплуатации ЭВМ. Методы обеспечения защиты информации от утечки через побочные электромагнитные излучения.
36) Технические каналы утечки информации при эксплуатации ЭВМ. Стандарты и методы измерения побочных электромагнитных излучений.

Образец билета:

Экзаменационный билет № 1

1)Защищенность систем передачи информации. Мешающие воздействия. Определение. Виды мешающих воздействий.
2)Технические каналы утечки информации при эксплуатации ЭВМ. Стандарты и методы измерения побочных электромагнитных излучений.

Заведующий кафедрой _____ Бескид П.П.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А.. Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. – М.: НПЦ «Аналитика», 2010

3. Правовые, руководящие, нормативные, нормативно-методические и методические документы, регламентирующие деятельность в области информационной безопасности.

б) дополнительная литература:

1. Меньшаков Ю.К. Теоретические основы технических разведок.- М.: МГТУ им. Н.Э.Баумана, 2008.
2. Анимов В.П., Коровин И.В., Рыбальченко В.И. Блокировка акустоэлектрических преобразователей в электронных технических средствах и системах общего применения: сборник рекомендаций «Z9». – М.: Гелиос АРВ, 2010.
3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки по информации техническим каналам: учеб. пособие. – М.: Горячая линия – Телеком, 2005.
4. Меньшаков Ю.К. Виды и средства иностранных технических разведок. /Под ред. М.П. Сычева. – М.: Изд.- во МГТУ им. Н.Э. Баумана, 2009.

в) программное обеспечение и Интернет-ресурсы:

www.intuit.ru – Национальный открытый университет

http://inf1.info/ - Планета Информатики

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Те	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторном занятии.
Лабораторные	На лабораторных занятиях выполняются лабораторные работы по овладению методами экспериментальных исследований технических каналов утечки информации и характеристик технических средств защиты информации от ее утечки по техническим каналам, изученные во время лекций. Как правило, на каждом занятии студент должен показать результаты выполнения лабораторной преподавателю.
Внеаудиторная работа	представляет собой вид занятий, которые каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает самостоятельное изучение разделов дисциплины.
Подготовка к зачёту/экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные	Перечень программного обеспечения и

	технологии	информационных справочных систем
Основы защиты информации	Лабораторные работы Технология объяснительно-иллюстративного обучения	MS Office 2007
Техническая разведка	Лабораторные работы	MS Office 2007 Internet Explorer
Технические каналы утечки информации.	Лабораторные работы	MS Office 2007
Средства выявления технических каналов утечки информации.	Лабораторные работы	MS Office 2007
Защита информации от утечки по техническим каналам.	Лабораторные работы	MS Office 2007

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий используются обычные, и в некоторых случаях, мультимедийные аудитории. Лабораторные занятия проводятся в компьютерном классе с ЛВС, связанной Интернетом.