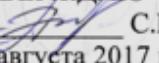


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов
«31» августа 2017 г.

**РАБОЧАЯ ПРОГРАММА
дисциплины**

«Техническая защита информации»

**Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы



/Дешина А.Е./

Заведующий кафедрой
Систем информационной
безопасности



/ А.Г. Остапенко /

Руководитель ОПОП



/ А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (техническая защита информации) на объектах информации и в выделенных помещениях.

1.2. Задачи освоения дисциплины:

- Изучение технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- Изучение технических каналов утечки акустической (речевой) информации;
- Изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- Изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- Освоение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- Освоение основ организации технической защиты информации на объектах информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Техническая защита информации» Б1.Б.25 относится к дисциплинам базовой части блока Б1. Для успешного освоения дисциплины студент должен иметь базовую подготовку по дисциплинам «Физические основы защиты информации», «Физика»

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Техническая защита информации» направлен на формирование следующих компетенций:

ОПК-8-способность к освоению новых образцов программных, технических средств и информационных технологий

ПК-15-способность участвовать в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем

ПК-25-способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и востребование их работ способности привозить в новейшие нештатные ситуации

ПК-26-способность администрировать подсистему информационной безопасности автоматизированной системы

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-8	Знать: способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации Уметь разрабатывать частные политики безопасности компьютерных систем,

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Техническая защита информации» составляет 53.е.

Распределение трудоемкости дисциплины по видам занятий очной формы обучения

Виды учебной работы	Всего часов	Семестры	
		8	8
Аудиторные занятия (всего)	72	72	
В том числе:			
Лекции	36	36	
Практические занятия (ПЗ)	18	18	
Лабораторные работы (ЛР)	18	18	
Самостоятельная работа	72	72	
Часы на контроль	36	36	
Виды промежуточной аттестации - экзамен	+	+	
Общая трудоемкость:			
академические часы	180	180	
зач.ед.	5	5	

	<p>в том числе политики управления доступом и информационными потоками</p> <p>Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений</p>
ПК-15	<p>Знать защитные механизмы и средства обеспечения сетевой безопасности</p> <p>Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы</p> <p>Владеть методами и средствами технической защиты информации</p>
ПК-25	<p>Знать организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации</p> <p>Уметь пользоваться нормативными документами по противодействию технической разведке</p> <p>Владеть методами расчета и инструментального контроля показателей технической защиты информации</p>
ПК-26	<p>Знать порядок организации работ по технической защите конфиденциальной информации на объектах информатизации</p> <p>Уметь планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;</p>

5.СОДЕРЖАНИЕ ДИСЦИПЛИНЫ(МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости типов видов занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ. зан.	Лаб. зан.	СРС	Всего, час
1	Технические каналы утечки информации	<p>Системный подход к защите информации.</p> <p>Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы.</p> <p>Понятие и особенности утечки информации.</p> <p>Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.</p> <p>Распространение сигналов в технических каналах утечки информации</p> <p>Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.</p> <p>Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.</p>	6	4	4	14	28
2	Способы и средства защиты информации от утечки по техническим каналам	<p>Основные концептуальные положения технической защиты информации.</p> <p>Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.</p> <p>Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.</p> <p>Моделирование случайных величин. Законы распределения случайных величин.</p>	10	6	6	22	44

		<p>Статистические оценки и их точность. Алпроксимация результатов статистического моделирования.</p> <p>Основные понятия теории случайных процессов, их классификация и основные характеристики. Марковские процессы с дискретными состояниями. Марковские процессы с дискретными состояниями и непрерывным временем. Стационарные случайные процессы.</p> <p>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 выбору рациональных вариантов защиты. Задачи защиты информации ТКС в условиях конфликта.</p> <p>Понятие конфликта. Способы разрешения конфликта в ТКС.</p> <p>Информационный конфликт (виды, варианты реализации).</p> <p>Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.</p>				
3	Методы и средства контроля эффективности технической защиты информации	<p>Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля. Методические рекомендации по оценке эффективности защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых</p>	10	4	4	18 36

		признаков объектов наблюдения. Способы оценки безопасности речевой информации в помещении. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств. Способы оценки размеров зон I и II.					
4	Организация технической защиты информации	Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средств защиты информации от технических разведок. Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственное, энергетическое и структурное скрытие информации и ее носителей. Дезинформирование, как метод скрытия. Математическая модель канала утечки информации применительно к техническим разведкам.	10	4	4	18	36
Итого			36	18	18	72	144

5.2 Перечень лабораторных работ

Неделя семестра	Наименование практической работы	Объем часов	В том числе в интерак- тивной форме (ИФ)
	8-ый семестр	18	-
	Технические каналы утечки информации	4	
1	Оценка дальности и пропускной способности передачи информации по каналу утечки.	4	
	Способы и средства защиты информации от утечки по техническим каналам	6	
	Аппроксимация результатов статистического моделирования.	4	
	Разработка тактик защиты, контроля для типовой ТКС с учетом целевого назначения ТКС.	2	
	Методы и средства контроля эффективности технической защиты информации	4	
	Расчет эффективности защиты информации в ТКС.	4	
	Организация технической защиты информации	4	
	Разработка математической модели канала утечки информации применительно к радиотехнической и акустической разведкам.	4	
	Итог за 8-й семестр	18	

6.ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ(РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом посвоению единой дисциплины не предусматривается выполнение курсового проекта (работы) или контрольной работы.

7.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей критериев оценивания компетенций на различных этапах формирования, описание шкалы оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«неаттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Неаттестован
ОПК-8	Знать: способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знание способов и средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Умение разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений	Владение навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-15	Знать защитные механизмы и средства обеспечения сетевой безопасности	Знание защитных механизмов и средств обеспечения сетевой безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Умение применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами и средствами технической защиты информации	Владение методами и средствами технической защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-25	Знать организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов	Знание организации работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов	Выполнение работ в срок, предусмотренный в рабочих	Невыполнение работ в срок, предусмотренный в рабочих

	обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	информатизации и сертификации средств защиты информации	программах	рабочих программах
	Уметь пользоваться нормативными документами по противодействию технической разведке	Умение пользоваться нормативными документами по противодействию технической разведке	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполненые работы в срок, предусмотренный в рабочих программах
	Владеть методами расчета и инструментального контроля показателей технической защиты информации	Владение методами расчета и инструментального контроля показателей технической защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполненные работы в срок, предусмотренный в рабочих программах
ПК-26	Знать порядок организации работ по технической защите конфиденциальной информации на объектах информатизации	Знание порядка организации работ по технической защите конфиденциальной информации на объектах информатизации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполненные работы в срок, предусмотренный в рабочих программах
	Уметь планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;	Умение планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполненные работы в срок, предусмотренный в рабочих программах
	Владеть методами расчета и инструментального контроля показателей технической защиты информации	Владение методами расчета и инструментального контроля показателей технической защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполненные работы в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9 семестре дипломной формой обучения по четырембалльной системе:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.

ОПК-8	Знать: способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Тест	Выполнениетестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационным потоками	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
ПК-15	Знать защитные механизмы и средства обеспечения сетевой безопасности	Тест	Выполнениетестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
	Владеть методами и средствами технической защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены

				задачах		
ПК-25	Знать организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	Тест	Выполнениетестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь пользоваться нормативными документами по противодействию технической разведке	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
	Владеть методами расчета и инструментального контроля показателей технической защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
ПК-26	Знать порядок организации работ по технической защите конфиденциальной информации на объектах информатизации	Тест	Выполнениетестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь планировать, организовывать и	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход	Продемонстрирован верный ход решения в	Задачи нерешены

	контролировать выполнение мероприятий по технической защите конфиденциальной информации;			решения всех, но не получен верный ответ во всех задачах	большинство задач	
	владеть методами расчета и инструментального контроля показателей технической защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков или опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Чем отличаются ОТСС от ВТСС?
 - не могут использоваться для обработки открытой информации
 - потребляемой мощностью
 - наличием принятых мер по защите информации
 - большой скоростью обработки информации
2. Акустоэлектрические преобразователи могут быть:
 - индуктивные, емкостные, пьезоэлектрические
 - индуктивные, емкостные, резистивные
 - емкостные, электродинамические, электромагнитные
 - индуктивные, пьезоэлектрические, электродинамические
3. Микрофоны по принципу электромеханического преобразования делятся на:
 - электродинамические, электростатические, релейные, электромагнитные
 - электродинамические, пьезо-микрофоны, электромагнитные
 - электродинамические, релейные, конденсаторные, электростатические
 - электродинамические, электромагнитные, электростатические
4. Разведка по виду носителя технического средства разведки классифицируется:
 - воздушная, наземная
 - воздушная, морская, сухопутная
 - воздушная, наземная, космическая
 - космическая, воздушная, наземная, морская
5. Когда возникает паразитная гальваническая связь?
 - в результате воздействия магнитного поля
 - в результате воздействия электрического поля
 - через общее активное сопротивление
 - все ответы верны
6. Пассивное скрытие заключается в:
 - исключении или значительном затруднении обнаружения объектов
 - ослаблении до необходимого уровня демаскирующих признаков объектов
 - верно А и В

- Д) все ответы неверны
7. Акустическое давление измеряется в:
- А) кг/ м²
 Б) Па
 С) ВТ/ м²
 Д) Н/ м²
8. Источниками опасных сигналов могут быть:
- А) акустоэлектрические преобразователи
 Б) излучатели высокочастотных и низкочастотных сигналов
 С) паразитные связи и наводки
 Д) все ответы верны
9. От чего зависит эффективность электрического экранирования?
- А) от толщины экрана и его магнитных свойств
 Б) от электропроводности экрана и сопротивления заземления
 С) верно А и В
 Д) все ответы неверны
10. Разрешающая способность ПЗС определяется:
- А) размером диагонали матрицы
 Б) габаритами объекта наблюдения
 С) количеством ячеек, размещающихся в поле изображения
 Д) величиной напряжения питания

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Нормативное значение коэффициента звукоизоляции для обеспечения защиты речевой конфиденциальной информации для смежных помещений, не оборудованных системами звукоусиления, равно:
- А) 50 дБ
 Б) 46 дБ
 С) 36 дБ
 Д) 26 дБ
2. Скорость звука в воздухе при нормальном атмосферном давлении и температуре 20°С равна:
- А) 270 м/с
 Б) 340 м/с
 С) 100 м/с
 Д) 200 м/с
3. Среднегеометрическая частота октавной полосы частот рассчитывается по формуле:
- А) $f_{cp} = \sqrt{f_h f_b}$
 Б) $f_{cp} = \sqrt{f_b - f_h}$
 С) $f_{cp} = 0,5\sqrt{f_b f_h}$
 Д) $f_{cp} = \sqrt{f_b / f_h}$
4. Освещенность поверхности Земли звездным светом составляет:
- А) 0,01 лк
 Б) 0,001 лк
 С) 0,1 лк
 Д) 1 лк
5. Диапазон длин волн в видимом диапазоне составляет:

- A) 0,45-0,7 мкм
 B) 0,2-0,6 мкм
 C) 0,4-0,76 мкм
 D) 0,3-0,65 мкм
6. Чувствительность микрофона определяется по формуле:
 A) $E=U/p$
 B) $E=Up$
 C) $E=Rp$
 D) $E=U/R$
7. Назначение прибора ST-031 «Пиранья»:
 A) для проверки эффективности электромагнитного экранирования
 B) многофункциональный поисковой прибор
 C) для создания акустических тест-сигналов
 D) для уничтожения радиозакладок
8. В каком диапазоне находится слышимый речевой сигнал?
 A) 300 Гц- 2 кГц
 B) 300 Гц- 2,5 кГц
 C) 200 Гц- 6 кГц
 D) 200 Гц- 4 кГц
9. Удельная мощность звуковых колебаний определяется по формуле:
 A) $P_{уд} = Fv/S$
 B) $P_{уд} = P/S$
 C) все ответы верны
 D) все ответы неверны
10. Уровень слухового ощущения определяется по формуле:
 A) $E = 10 \lg \frac{I_0}{I_{nc}}$
 B) $E = \lg \frac{I_0}{I_{nc}}$
 C) $E = 10 \lg \frac{I}{I_0}$
 D) $E = 10 \lg \frac{I}{I_{nc}}$

7.2.3 Примерный перечень заданий для решения прикладных задач (минимум 10 вопросов для тестирования с вариантами ответов)

7.2.4 Примерный перечень вопросов для подготовки к экзамену Контрольно-измерительные материалы текущего контроля

1. Какие свойства информации, влияющие на ее безопасность, вы знаете?
2. Определите виды, источники и носители защищаемой информации.
3. Основные направления инженерно-технической защиты информации.
4. Какие основные характеристики технических каналов утечки информации вы знаете?
5. Структура, классификация и основные характеристики технических каналов утечки информации.
6. Перечислите принципы защиты информации техническими средствами.
7. Что такое модель и моделирование?
8. Что такое аналитическая модель системы?

9. Моделирование случайных величин и их законы распределения.
10. Какие числовые характеристики случайных величин вы знаете?
11. Что описывает нижеприведенная формула? Поясните основные ее параметры.

$$f(x) = \frac{1}{\sigma \sqrt{2\pi}} e^{\frac{(x-a)^2}{2\sigma^2}}.$$

12. Какие статистические оценки знаете? Как определить их точность?
13. Аппроксимация результатов статистического моделирования.
14. Что такое адекватная модель?
15. Принципы моделирования объектов защиты.
16. Моделирование угроз безопасности информации.
17. Методические рекомендации по выбору рациональных вариантов защиты.
18. Основные понятия теории случайных процессов.
19. Классификация и основные характеристики случайных процессов.
20. Перечислите задачи защиты информации ТКС в условиях конфликта.
21. Понятие конфликта. Способы разрешения конфликта в ТКС.
22. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС.
23. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.
24. Какие виды контроля эффективности инженерно-технической защиты информации вы знаете?
25. Какие предъявляются требования по защите информации от утечки по техническим каналам?
26. Дайте классификацию методов и средств защиты информации от технических разведок.
27. Математическая модель канала утечки информации применительно к техническим разведкам

1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации.
2. Представление сил и средств защиты информации в виде системы.
3. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.
4. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.
5. Распространение оптических сигналов в атмосфере и в светопроводах.
6. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
7. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.
8. Принципы защиты информации техническими средствами.
9. Основные направления инженерно-технической защиты информации.
10. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации.
11. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
12. Основные теоремы теории вероятностей.
13. Моделирование случайных величин и их законы распределения.
14. Статистические оценки и их точность.
15. Аппроксимация результатов статистического моделирования.

16. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.
17. Принципы моделирования объектов защиты.
18. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.
19. Задачи защиты информации ТКС в условиях конфликта.
20. Понятие конфликта. Способы разрешения конфликта в ТКС.
21. Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия.
22. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС.
23. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.
24. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля.
25. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.
26. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения.
27. Способы оценки безопасности речевой информации в помещении.
28. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.
29. Способы оценки размеров зон I и II.
30. Основные задачи, структура и характеристика государственной системы противодействия технической защите.
31. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации

32. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок.
33. Принципы действия аппаратуры технических разведок.
34. Классификация методов и средств защиты информации от технических разведок.
35. Классификация методов инженерно-технической защиты информации.
36. Инженерная защита и техническая охрана объектов.
37. Пространственное, энергетическое и структурное скрытие информации и ее носителей.
38. Дезинформирование, как метод скрытия.
39. Математическая модель канала утечки информации применительно к техническим разведкам.
40. Пространственное скрытие объектов наблюдения и сигналов.
41. Структурное и энергетическое скрытие объектов наблюдения.
42. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение.
43. Энергетическое скрытие радио и электрических сигналов.
44. Классификация методов инженерной защиты и технической охраны объектов защиты.
45. Инженерные конструкции. Автономные и централизованные системы охраны
46. Модели злоумышленника.
47. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления.
48. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.
49. Комплексты технических средств охраны.

7.2.7 Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины
1	Техническиеканалыутечкиинформации
2	Способы и средства защиты информации от утечки по техническим каналам
3	Методы и средства контроля эффективности технической защиты информации
4	Организациятехническойзащитыинформации

7.3. Методическиематериалы, определяющиепроцедурыоцениваниязнаний

Тестированиеосуществляется,либопримоющикомпьютернойсистемытестированиеметодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либопримоющикомпьютернойсистемыоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации

Решениеприкладныхзадачосуществляется,либопримоющикомпьютернойсистемыоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации

1. Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабра

8.1 Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Технические средства и методы защиты информации: Учеб. пособие / А. П. Заинкин, В. П. Дуров, Н. М. Радько. - Воронеж: Воронежский государственный технический университет, 2010. - 1 файл. - 30-00.
2. Дуров В.П. Программно-аппаратная защита информации [Электронный ресурс] / В.П. Дуров. - Воронеж: Воронежский государственный технический университет, 2010. - 1 файл. - 30-00.
3. Радько Н.М. Защита информации в беспроводных сетях [Электронный ресурс] / Н.М. Радько. - Воронеж: Воронежский государственный технический университет, 2010. - 1 файл. - 30-00.

Дополнительная литература:

1. Методические указания к лабораторным работам по дисциплине "Технические средства и методы защиты информации: Учеб. пособие / А. П. Заинкин, В. П. Дуров, Н. М. Радько. - Воронеж: Воронежский государственный технический университет, 2010. - 1 файл. - 30-00.
2. Методические указания к самостоятельным работам по дисциплине «Технические средства и методы защиты информации: Учеб. пособие / А. П. Заинкин, В. П. Дуров, Н. М. Радько. - Воронеж: Воронежский государственный технический университет, 2010. - 1 файл. - 30-00.
3. Технические средства обеспечения информационной безопасности [Электронный ресурс] / А. П. Заинкин, В. П. Дуров, Н. М. Радько. - Воронеж: Воронежский государственный технический университет, 2010. - 1 файл. - 30-00.

8.2 Переченьинформационныхтехнологий,используемыхприосуществленииучебногопроцесса,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем

<http://att.nica.ru>

<http://www.edu.ru/>

<http://window.edu.ru/window/library>

<http://www.intuit.ru/catalog/>

<https://marsohod.org/howtostart/marsohod2>

<http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp>

<https://cchgeu.ru/education/cafedras/kafsib/?docs>

<http://www.eios.vorstu.ru>

<http://e.lanbook.com/> (ЭБС Лань)

<http://IPRbookshop.ru/> (ЭБСIPRbooks)

9МАТЕРИАЛЬНО

Специализированная лекционная аудитория, оснащенная оборудованием для
Дисплейный класс, оснащенный компьютерными программами для проведения

10.МП

Подисциплине «Техническая защита информации» читаются лекции, проводятся лекции.
Основой изучения дисциплины являются лекции, на которых излагаются наиболее
Лабораторные работы выполняются на лабораторном оборудовании в соответствии

Вид учебных занятий	
Лекция	Написание конспекта лекций: краткий энциклопедий, словарей, справочников в материале, необходимо сформулировать вопросы для обсуждения
Лабораторная работа	Лабораторные работы позволяют не только практиковаться в теории, но и необходимо: следует разобрать лекции и выполнить задания
Самостоятельная работа	Самостоятельная работа студентов - работа с текстами: учебниками, статьями - выполнение домашних заданий и - работа над темами для самостоятельной работы - участие в работе студенческих научно-исследовательских - подготовка к промежуточной аттестации
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации эффективнее всего использовать для этого различные методы: чтение литературы, выполнение домашних заданий, участие в семинарах, обсуждение вопросов с преподавателем