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 Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Дешина А.Е./

Заведующий кафедрой Систем информационной безопасности _____ /А.Г. Остапенко/

Руководитель ОПОП _____ /А.Г. Остапенко/

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

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.Задачиосвоениядисциплины:

- 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.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Техническаязащитаинформации» Б1.Б.25относитсякдисциплинамбазовойчастиблокаБ1 . Для успешного освоения дисциплины студент должен иметь базовую подготовку по дисциплинам «Физические основы защиты информации», «Физика»

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Техническаязащитаинформации»направленнаформированиеследующихкомпетенций:

ОПК-8-способностьюкосвоениюновыхобразцовпрограммных,техническихсредствиинформационныхтехнологий

ПК-15-способностьюучаствоватьвпроведенииэкспериментально-исследовательскихработприсертификациисредствзащитыинформацииавтоматизированныхсистем

ПК-25-способностьюобеспечитьэффективноеприменениесредствзащитыинформационно-технологическихресурсовавтоматизированнойсистемыивосстановлениеихработоспособностипривозникновенииинештатныхситуаций

ПК-26-способностьюадминистрироватьподсистемуинформационнойбезопасностиавтоматизированнойсистемы

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
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, в том числе политики управления доступом и информационными

	потоками
	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений
ПК-15	Знать защитные механизмы и средства обеспечения сетевой безопасности
	Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы
	Владеть методами и средствами технической защиты информации
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
	Уметь пользоваться нормативными документами по противодействию технической разведке
	Владеть методами расчета и инструментального контроля показателей технической защиты информации
ПК-26	Знать порядок организации работ по технической защите конфиденциальной информации на объектах информатизации
	Уметь планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Техническаязащитаинформации»составляет8з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всего часов	Семестры 9
Аудиторныезанятия (всего)	100	100
В томчисле:		
Лекции	40	40
Лабораторныеработы (ЛР)	60	60
Самостоятельнаяработа	152	152
Часынаконтроль	36	36
Видыпромежуточнойаттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 288 8	 288 8

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостип

овидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Техническиеканалыутечкиинформации	Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Распространение сигналов в технических каналах утечки информации Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.	10	10	34	64
2	Способы и средства защиты информации от утечки по техническим ка-налам	Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Моделирование случайных величин. Законы распределения случайных величин.	12	20	36	64

		Статистические оценки и их точность. Аппроксимация результатов статистического моделирования. 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. 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. Понятие конфликта. Способы разрешения конфликта в ТКС. Информационный конфликт (виды, варианты реализации). 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.				
3	Методы и средства контроля эффективности технической защиты ин-формации	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	12	16	46	62

		технического контроля. Методические рекомендации по оценке эффективности защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых 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	Организациятехнической защитыинформации	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.	6	14	36	62
Итого			**40**	**60**	**152**	**252**

5.2Переченьлабораторныхработ

Неделя	Наименованиепрактическойработы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
10-ый семестр		**54**	**-**	
Техническиеканалыутечкиинформации		**8**		
1	Оценка дальности и пропускной способности передачи информации по каналу утечки.	8		отчет
Способы и средства защиты информации от утечки по техническимканалам		**12**		
	Аппроксимациярезультатовстатистическогомоделирования.	4		отчет
	Разработка матрицы конфликтного взаимодействия для типовых ТКС.	4		отчет
	Разработка тактик защиты, контроля для типовой ТКС с учетом целевого назначения ТКС.	4		отчет
Методы и средства контроля эффективности технической защиты информации		**10**		
	Расчет эффективности защиты информации в ТКС.	4		отчет
	Способы оценки размеров зон I и II. Оценка дальности перехвата сигналов.	6		отчет
Организациятехническойзащитыинформации		**6**		
	Разработка математической модели канала утечки информации применительно к радиотехнической и акустической разведкам.	6		отчет
Итогоза 10-й семестр		**36**		

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматривается выполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции	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 защитныхмеханизмов и средствв обеспечения сетевой	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,	Знание организации работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны,	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации		
	Уметь пользоваться нормативными документами по противодействию технической разведке	Умение пользоваться нормативными документами по противодействию технической разведке	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ 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	Невыполнение работ 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	Невыполнение работ 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	Невыполнение работ 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	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этапромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9семестредлячнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**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	Выполнение тестана 90-100%	Выполнение тестана 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 информационными	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные	Продемонстрирован верный ход решения всех, но не получен	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	потоками		ответы	верный ответ во всех задачах		
	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 решены
ПК-15	Знать защитные механизмы и средства обеспечения сетевой безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 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	Решение стандартных практических задач	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 решены
	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 задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
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	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	Уметь пользоваться нормативными документами по противодействию технической разведке	Решение стандартных практических задач	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 решены
	Владеть методами расчета и инструментального контроля показателей	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и	Продемонстрирован верный ход решения	Продемонстрирован верный ход решения в большинстве	Задачи решены

	технической защиты информации		получены верные ответы	всех, но не получен верный ответ во всех задачах	задач	
ПК-26	Знать порядок организации работ по технической защите конфиденциальной информации на объектах информатизации	Тест	Выполнение тестана 90-100%	Выполнение тестана 80-90%	Выполниетестана 70- 80%	В тесте менее 70% правильных ответов
	Уметь планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;	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 решены
	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 решены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Чем отличаются ОТСС от ВТСС?
   А) не могут использоваться для обработки открытой информации
   В) потребляемой мощностью
   С) наличием принятых мер по защите информации
   Д) большей скоростью обработки информации
2. Акустоэлектрические преобразователи могут быть:
   А) индуктивные, емкостные, пьезоэлектрические
   В) индуктивные, емкостные, резистивные
   С) емкостные, электродинамические, электромагнитные
   Д) индуктивные, пьезоэлектрические, электродинамические
3. Микрофоны по принципу электромеханического преобразования делятся на:
   А) электродинамические, электростатические, релейные, электромагнитные
   В) электродинамические, пьезо-микрофоны, электромагнитные
   С) электродинамические, релейные, конденсаторные, электростатические
   Д) электродинамические, электромагнитные, электростатические
4. Разведка по виду носителя технического средства разведки классифицируется:
   А) воздушная, наземная
   В) воздушная, морская, сухопутная
   С) воздушная, наземная, космическая
   Д) космическая, воздушная, наземная, морская

5. Когда возникает паразитная гальваническая связь?
   А) в результате воздействия магнитного поля
   В) в результате воздействия электрического поля
   С) через общее активное сопротивление
   Д) все ответы верны
6. Пассивное скрытие заключается в:
   А) исключении или значительном затруднении обнаружения объектов
   В) ослаблении до необходимого уровня демаскирующих признаков объектов
   С) верно А и В
   Д) все ответы неверны
7. Акустическое давление измеряется в:
   А) кг/ м²
   В) Па
   С) ВТ/ м²
   Д) Н/ м²
8. Источниками опасных сигналов могут быть:
   А) акустоэлектрические преобразователи
   В) 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
   В) от электропроводности экрана и сопротивления заземления
   С) верно А и В
   Д) все ответы неверны
10. Разрешающая способность ПЗС определяется:
   А) размером диагонали матрицы
   В) габаритами объекта наблюдения
   С) количеством ячеек, размещающихся в поле изображения
   Д) величиной напряжения питания

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1. Нормативное значение коэффициента звукоизоляции для обеспечения защиты речевой конфиденциальной информации для смежных помещений, не оборудованных системами звукоусиления, равно:
   А) 50 дБ
   В) 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
   В) 340 м/с
   С) 100 м/с
   Д) 200 м/с
3. Среднегеометрическая частота октавной полосы частот рассчитывается по формуле:
   А) $f_{ср} = \sqrt{f_н f_в}$
   В)$f_{ср} = \sqrt{f_в - f_н}$

С) $f_{ср} = 0{,}5\sqrt{f_в f_н}$

Д) $f_{ср} = \sqrt{f_в / f_н}$

4. Освещенность поверхности Земли звездным светом составляет:

А) 0,01 лк

В) 0,001 лк

С) 0,1 лк

Д) 1 лк

5. Диапазон длин волн в видимом диапазоне составляет:

А) 0,45-0,7 мкм

В) 0,2-0,6 мкм

С) 0,4-0,76 мкм

Д) 0,3-0,65 мкм

6. Чувствительность микрофона определяется по формуле:

А) E=U/p

В) E=Up

С) E=Rp

Д) E=U/R

7. Назначение прибора ST-031 «Пиранья»:

А) для проверки эффективности электромагнитного экранирования

В) многофункциональный поисковой прибор

С) для создания акустических тест-сигналов

Д) для уничтожения радиозакладок

8. В каком диапазоне находится слышимый речевой сигнал?

А) 300 Гц- 2 кГц

В) 300 Гц- 2,5 кГц

С) 200 Гц- 6 кГц

Д) 200 Гц- 4 кГц

9. Удельная мощность звуковых колебаний определяется по формуле:

А) $P_{уд} = Fv/S$

В) $P_{уд} = P/S$

С) все ответы верны

Д) все ответы неверны

10. Уровень слухового ощущения определяется по формуле:

А) E= $10\lg\frac{I_0}{I_{пс}}$

В) E= $\lg\frac{I_0}{I_{пс}}$

С) E= $10\lg\frac{I}{I_0}$

Д) E= $10\lg\frac{I}{I_{пс}}$

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

(минимум10вопросовдлятестированиясвариантамиответов)

7.2.4Примерныйпереченьвопросовдляподготовкикэкзамену

Контрольно-измерительныематериалытекущегоконтроля

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 характеристикислучайных 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 разведка

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, выделяемы 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. Основныеорганизационные и техническиемерыпозащитеинформации

32. Классификация средств технических разведок по виду носителя. Типовыезадачитехническихразведок.
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, какметодскрытия.
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. Моделизлоумышленника.
47. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления.
48. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.
49. Комплекстехническихсредствохраны.

7.2.7Паспортоценочныхматериалов

№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,определяющиепроцедурыоцениванияознаний

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестиров ометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсист яоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттеста

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсисте оценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестац

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

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

Дополнительная литература:

1. Методические указания к лабораторным работам по дисциплине "Техничес обучения [Электронный ресурс] / Каф. систем информационной безопасност
2. Методические указания к самостоятельным работам по дисциплине «Техн 090303 «Информационная безопасность автоматизированных систем» очной ВПО "Воронежскийгосударственныйтехническийуниверситет", 2014. - 1 фа
3. Технические средства обеспечения информационной безопасности [Электро

8.2Переченьинформационныхтехнологий,используемыхприосуществлени »,современныхпрофессиональныхбазданныхиинформационныхсправочныхсист

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 дл
Дисплейный класс, оснащенный компьютерными программами для проведени

10.М

Подисциплине«Техническаязащитаинформации»читаютсялекции,проводятсял
Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболее
Лабораторныеработывыполняютсяналабораторномоборудованиивсоответстви

Видучебныхзанятий	
Лекция	Написание конспекта лекций: кратк энциклопедий, словарей, справочни в материале, необходимо сформули
Лабораторнаяработа	Лабораторные работы позволяют н необходимо: следует разобрать лек
Самостоятельнаяработа	Самостоятельная работа студентов - работа с текстами: учебниками, сп - выполнение домашних заданий и - работа над темами для самостояте - участие в работе студенческих нау - подготовка к промежуточнойаттес
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттес эффективнее всего использовать дл