РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита информации

(наименование дисциплины (модуля) по УП)

Закреплена за кафедрой: **систем информационной безопасности**

Направление подготовки (специальности): **10.05.03 Информационная безопасность автоматизированных систем**

Профиль: **Обеспечение информационной безопасности распределенных информационных систем**

(название профиля по УП)

Часов по УП: 144; Часов по РПД: 144;
Часов по УП (без учета часов на экзамены): 108; Часов по РПД: 108;
Часов на интерактивные формы (ИФ) обучения по УП: -
Часов на интерактивные формы (ИФ) обучения по РПД: -
Часов на самостоятельную работу по УП: 36 (33,3%);
Часов на самостоятельную работу по РПД: **36 (33,3%);**
Общая трудоемкость в ЗЕТ: 4;
Виды контроля в семестрах (на курсах): Экзамены-1; зачеты – 0; курсовые проекты – 0; курсовые работы – 0;
Форма обучения: очная**;**
Срок обучения: нормативный**.**

Распределение часов дисциплины по семестрам

Вид занятий	**№ семестров, число учебных недель в семестрах**																	
	12/ 18		3 / 18		4 / 18		5 / 18		6 / 18		7 / 20		8 / 18		9 / 18		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции															36	36	36	36
Лабораторные															18	18	18	18
Практические															18	18	18	18
Ауд. занятия															72	72	72	72
Сам. работа															36	36	36	36
Итого															108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**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	**Для достижения цели ставятся задачи:**
1.2.1	Изучение технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
1.2.2	Изучение технических каналов утечки акустической (речевой) информации;
1.2.3	Изучение способов и средств защиты информации, обрабатываемой техническими средствами;
1.2.4	Изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
1.2.5	Освоение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
1.2.6	Освоение основ организации технической защиты информации на объектах информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Цикл (раздел) ООП: С.3	код дисциплины в УП: С3.Б.5
2.1 Требования к предварительной подготовке обучающегося	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике и математике в пределах программы средней школы, а также дисциплины младших курсов, такие как	
С2.Б.2	Математический анализ
С2.Б.4	Теория вероятностей и математическая статистика
С2.В.ОД.1	Информационные операции и атаки в распределенных информационных системах
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
С3.Б.15	Разработка и эксплуатация защищенных автоматизированных систем
С3.Б.19	Методы проектирования защищенных распределенных информационных систем
С3.В.ДВ.1	Управление рисками в распределенных информационных системах

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОК-5	Способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства.
ОК-9	Способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания.
ОК-10	Способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности.
ПК-1	Способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения.
ПК-2	Способностью применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач.
ПК-3	Способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации.
ПК-5	способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.
ПК-9	Способностью к эксплуатации современного телекоммуникационного оборудования и приборов.
ПК-10	Способностью применять современные методы исследования с использованием компьютерных технологий
ПК-11	Способностью разрабатывать и исследовать модели автоматизированных систем
ПК-12	Способностью применять современные методы исследования с использованием компьютерной техники.
ПК-13	Способностью проводить математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований.
ПК-19	Способностью проектировать защищённые телекоммуникационные системы и проводить анализ проектных решений по обеспечению безопасности телекоммуникационных систем.
ПК-20	Способностью разрабатывать политики информационной безопасности автоматизированных систем.
ПК-33	Способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов телекоммуникационных систем.
ПК-22	Способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы.
Пк-23	Способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
ПК-26	Способностью проводить инструментальный мониторинг защищенности автоматизи-

	рованных систем.
ПК-30	Способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности.
ПК-32	Способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.
ПК-36	Способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы.
ПК-37	Способностью администрировать подсистему информационной безопасности автоматизированной системы.
ПК-38	Способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы.
ПК-40	Способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	технические каналы утечки информации
3.1.2	возможности технических средств перехвата информации
3.1.3	способы и средства защиты информации от утечки по техническим каналам
3.1.4	организацию защиты информации от утечки по техническим каналам на объектах информатизации
3.1.5	основы физической защиты объектов информатизации
3.2	**Уметь:**
3.2.1	пользоваться нормативными документами по противодействию технической разведке
3.2.2	анализировать и оценивать угрозы информационной безопасности объекта
3.3	**Владеть:**
3.3.1	методами и средствами технической защиты информации
3.3.2	методами расчета и инструментального контроля показателей технической защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ П./п	Наименование раздела дисциплины	Семестр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах				
				Лекции	Практические занятия	Лабораторные. работы	СРС	Всего часов
1	Технические каналы утечки информации	8	1-3	6	4	2	4	16
2	Способы и средства защиты информации от утечки по техническим каналам	8	4-9	14	8	8	14	44
3	Методы и средства контроля эффективности технической защиты информации	8	10-13	6	2	4	6	18
4	Организация технической защиты информации	8	14-20	10	4	4	12	30
Итого				36	18	18	36	108

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов	В том числе, в интерактивной форме (ИФ)
Технические каналы утечки информации		**6**	
1	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. *Самостоятельное изучение*. Основные параметры системы защиты информации.	2	
2	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. *Самостоятельное изучение.* Характеристика и возможности оптических, акустических радиоэлектронных и материально-вещественных каналов утечки информации.	2	
3	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. *Самостоятельное изучение.* Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.	2	

Способы и средства защиты информации от утечки по техническим каналам		**14**	
	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. *Самостоятельное изучение*. Показатели эффективности инженерно-технической защиты информации.	2	
	Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. *Самостоятельное изучение.* Понятие о текущей и эталонной признаковой модели.	2	
	Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования. *Самостоятельное изучение*. Оценка качества статистической модели.	2	
	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. *Самостоятельное изучение*. Основные положения теории нестационарных моментов марковских сетей.	**2**	
	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. *Самостоятельное изучение* Способы оптимизации мер инженерно-технической защиты информации.	2	
	Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС. *Самостоятельное изучение.* Основные понятия рефлексивных игр.	2	
	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. *Самостоятельное изучение*. Разрешение конфликта в условиях рефлексивных игр. Разработка матрицы конфликтного взаимодействия для типовых ТКС.	2	
Методы и средства контроля эффективности технической защиты информации		**6**	
	Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от	2	

	утечки по техническим каналам. Виды технического контроля. *Самостоятельное изучение*. Особенности инструментального контроля эффективности инженерно-технической защиты информации.		
	Показатели эффективности функционирования средств защиты информации в ТКС.	2	
	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. *Самостоятельное изучение*. Оценка дальности перехвата сигналов.	2	
Организация технической защиты информации		**10**	
	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. *Самостоятельное изучение.* Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств.	2	
	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. *Самостоятельное изучение*. Методический подход к оценке эффективности защиты информации от технических разведок.	2	
	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. *Самостоятельное изучение* Комплексное применение методов защиты.	2	
	Математическая модель канала утечки информации применительно к техническим разведкам. *Самостоятельное изучение*. Математическая модель канала акустической утечки информации.	2	
	Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов защиты. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления. Комплекс технических средств охраны. *Самостоятельное изучение* Автоматизация процессов охраны.	2	
Итого за 8-ой семестр		**36**	
Всего		**36**	

4.2 Практические занятия

Неделя семестра	Наименование практической работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
8-ой семестр		**18**	**-**	
Технические каналы утечки информации		**4**		
1	Оценка пропускной способности канала утечки информации.	2		отчет
3	Оценка дальности передачи информации по каналу утечки.	2		отчет
Способы и средства защиты информации от утечки по техническим каналам		**8**		
5	Разработка алгоритма функционирования для типовой подсистемы защиты информации для типовых ТКС.	2		отчет
7	Законы распределения случайных величин. Статистические оценки и их точность.	2		отчет
9	Разработка матрицы конфликтного взаимодействия для типовых ТКС.	2		отчет
12	Формулировка стратегий защиты для типовой ТКС. Разработка тактик и стратегии защиты, контроля для типовой ТКС с учетом целевого назначения ТКС.	2		отчет
Методы и средства контроля эффективности технической защиты информации		**2**		
15	Расчет эффективности защиты информации в ТКС.	2		
Организация технической защиты информации		**4**		
16	Методы и средств защиты информации от технических разведок.	2		
17	Разработка математической модели канала утечки информации применительно к радиотехнической разведке.	2		
Итого за 8-ой семестр		**18**		

4.3. Лабораторные работы

Неделя семестра	Наименование практической работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
8-ой семестр		**18**	**-**	
Технические каналы утечки информации		**2**		
1	Оценка дальности и пропускной способности передачи информации по каналу утечки.	2		отчет
Способы и средства защиты информации от утечки по техническим каналам		**8**		
	Аппроксимация результатов статистического моделирования.	2		отчет

16	Разработка матрицы конфликтного взаимодействия для типовых ТКС.	2		отчет
19	Разработка тактик защиты, контроля для типовой ТКС с учетом целевого назначения ТКС.	4		отчет
Методы и средства контроля эффективности технической защиты информации		**4**		
	Расчет эффективности защиты информации в ТКС.	2		отчет
	Способы оценки размеров зон I и II. Оценка дальности перехвата сигналов.	2		отчет
Организация технической защиты информации		**4**		
	Разработка математической модели канала утечки информации применительно к радиотехнической и акустической разведкам.	4		отчет
Итого за 8-ой семестр		**18**		

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Виды контроля	Объем часов
8 семестр		**Экзамен**	**28**
1	Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.	проверка домашнего задания	4
3	Показатели эффективности инженерно-технической защиты информации.	проверка домашнего задания	2
5	Способы оптимизации мер инженерно-технической защиты информации.	проверка домашнего задания	2
8	Разрешение конфликта в условиях рефлексивных игр. Разработка матрицы конфликтного взаимодействия для типовых ТКС.	проверка домашнего задания, допуск к выполнению лабораторной работы	4
10	Особенности инструментального контроля эффективности инженерно-технической защиты информации.	проверка домашнего задания	4
12	Оценка дальности перехвата сигналов.	проверка домашнего задания	2
15	Методический подход к оценке эффективности защиты информации от технических разведок.	проверка домашнего задания	4
18	Математическая модель канала акустической утечки информации.	проверка домашнего задания	4

4.5. Темы курсовых работ

Не предусмотрены

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	**Информационные лекции** не предусмотрены.
5.2	**Практические занятия**: совместное обсуждение вопросов лекций, домашних контрольных заданий.
5.3	**Лабораторные работы** не предусмотрены.
5.4	**самостоятельная работа студентов**: – изучение теоретического материала, – подготовка к лекциям и практическим занятиям, – работа с учебно-методической литературой, – оформление конспектов лекций, подготовка отчетов, – подготовка к текущему контролю успеваемости и к экзамену;
5.5	**консультации** по всем вопросам учебной программы.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1	**Контрольные вопросы и задания**
6.1.1	Используемые формы текущего контроля: – отчет и защита выполненных практических и лабораторных работ.
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля знаний. Фонд включает вопросы к экзаменам. Фонд оценочных средств представлен в учебно-методическом комплексе дисциплины.
6.2	**Другие виды контроля**
	Не предусмотрены.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1 Рекомендуемая литература

№ п/п	**Авторы, составители**	Заглавие	Годы издания. Вид издания	Обеспеченность
7.1.1. Основная литература				
7.1.1.1	Вентцель Е.С., Овчаров Л.А.	Теория случайных процессов и ее инженерные приложения. - М. : Наука, 1991. - 384с.	1991 печат.	0,07
7.1.1.2	Язов Ю.К.	Технология проектирования систем защиты информации в информационно-телекоммуникационных системах [Электронный ресурс]: учеб. пособие / Ю. К. Язов. - Электрон.дан. (1 файл). - Воронеж : ВГТУ, 2004. 30.00.	2004 Электронный ресурс	
7.1.1.3	Владимиров И.В.	Основы системных исследований телекоммуникаций систем в аспекте обеспечения информационной безопасности [Электронный ресурс] : учеб. пособие / И. В. Владимиров. - - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 дискета. - 30-00.	2012 печат.	
7.1.1.4	Минаев В.А.	Основы информационной безопасности / В.А. Минаев, С.В. Скрыль, А.П. Фисун, В.Е. Потанин, С.В. Дворянкин. - Воронеж: Воронежский институт МВД России, 2001. - 464с.	2001 печатн.	
7.1.2. Дополнительная литература				
7.1.2.1	Дьяконов В.В., Круглов В.А.	MATLAB: Анализ, идентификация и моделирование систем: Специальный справочник / - СПб. : Питер, 2002. - 448с.	2002 печатн.	
7.1.2.2	Кудрявцев Е.М.	GPSS World. Основы имитационного моделирования различных систем. "ДМК Пресс", 317 с. (ЭБС «Лань»)	2008 печатн.	
7.1.2.3	Бугров Ю.Г., Остапенко Г.А.; Радько Н.М.	Моделирование атак сети массового обслуживания [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл : 1248 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет"	2007 Эл.рес	

7.1.3 Программное обеспечение и интернет ресурсы	
7.1.3.1	Методические указания к выполнению лабораторных работ **представлены на сайте:** Интернет ресурсы: http://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ) http://e.lanbook.com/ (ЭБС Лань) http://znanium.com/ (ЭБС Знаниум) http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))
7.1.3.2	**Компьютерные практические работы**: – система компьютерной математики MATLAB. – интегрированная среда языка имитационного моделирования GPSS PS – инструментальная система имитационного моделирования AnyLogic PLE

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	**Специализированная лекционная аудитория**, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Приложение 1

Контрольно-измерительные материалы для проведения текущего контроля и промежуточной и итоговой аттестации по дисциплине «Техническая защита информации»

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.

Продолжение приложения 1

Контрольно-измерительные материалы итогового контроля

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.

Продолжение приложения 1

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. Комплекс технических средств охраны.

Приложение 2

Экзаменационные билеты девятого семестра

Воронежский государственный технический университет

Билет № 1
По технической защите информации

1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации.
2. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 2
По технической защите информации

1. Представление сил и средств защиты информации в виде системы.
2. Комплекс технических средств охраны.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 3
По технической защите информации

1. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.
2. Модели злоумышленника.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 4
По технической защите информации

1. Распространение акустических сигналов в атмосфере, воде и в твердой среде.

2. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 5
По технической защите информации

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
2. Классификация методов инженерной защиты и технической охраны объектов защиты.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 6
По технической защите информации

1. Принципы защиты информации техническими средствами
2. Инженерные конструкции. Автономные и централизованные системы охраны.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 7
По технической защите информации

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
2. Математическая модель канала утечки информации применительно к техническим разведкам.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 8
По технической защите информации

1. Принципы защиты информации техническими средствами
2. Пространственное скрытие объектов наблюдения и сигналов.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 9
По технической защите информации

1. Основные направления инженерно-технической защиты информации.
Свойства информации, влияющие на ее безопасность.
2. Инженерная защита и техническая охрана объектов.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 10
По технической защите информации

1. Виды, источники и носители защищаемой информации.
2. Пространственное, энергетическое и структурное скрытие информации и ее носителей.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 11
По технической защите информации

1. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
2. Классификация методов и средств защиты информации от технических разведок.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 12
По технической защите информации

1. Моделирование случайных величин и их законы распределения.
2. Классификация методов инженерно-технической защиты информации.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 13
По математике

1. По технической защите информации

1. Статистические оценки и их точность.
2. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 14
По технической защите информации

1. Аппроксимация результатов статистического моделирования

2. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 15
По технической защите информации

1. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.

2. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Билет № 16
По технической защите информации

1. Принципы моделирования объектов защиты.

2. Способы оценки размеров зон I и II.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Билет № 17
По математике

1. По технической защите информации

1. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.

2. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 18
По технической защите информации

1. Задачи защиты информации ТКС в условиях конфликта.

2. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 19
По технической защите информации

1. Понятие конфликта. Способы разрешения конфликта в ТКС.
2. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Воронежский государственный технический университет

Билет № 20
По технической защите информации

1. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия

2. Основные задачи, структура и характеристика государственной системы противодействия технической защите.

Билет рассмотрен и утвержден на заседании кафедры

Зав. кафедрой проф. А.Г. Остапенко

Приложение 3

Карта обеспеченности рекомендуемой литературой

№ п/п	Авторы, составители	Заглавие	Год издания. Вид издания.	Обеспеченность
1. Основная литература				
Л1.1	Вентцель Е.С., Овчаров Л.А.	Теория случайных процессов и ее инженерные приложения. - М. : Наука, 1991. - 384с.	1991 печат.	
Л1.2	Язов Ю.К.	Технология проектирования систем защиты информации в информационно-телекоммуникационных системах [Электронный ресурс]: учеб. пособие / Ю. К. Язов. - Электрон.дан. (1 файл). - Воронеж : ВГТУ, 2004. 30.00.	2004 Электронный ресурс	
Л1.3	Минаев В.А.	Основы информационной безопасности / В.А. Минаев, С.В. Скрыль, А.П. Фисун, В.Е. Потанин, С.В. Дворянкин. - Воронеж: Воронежский институт МВД России, 2001. - 464с.	2001 печатн.	
Л1.4	Владимиров И.В.	Основы системных исследований телекоммуникаций систем в аспекте обеспечения информационной безопасности [Электронный ресурс] : учеб. пособие / И. В. Владимиров. - - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006.	2012 печатн.	
2. Дополнительная литература				
Л2.1	Каркоцкий В.Л.	Методические указания по выполнению практических работ по дисциплине "Технические средства и методы защиты информации" для студентов очной формы обучения специальностей 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" и 090106 "Информационная безопасность телекоммуникационных систем" [Электронный ресурс] / Каф. систем информационной безопасности; Сост. В.Л.Каркоцкий. - Электрон. текстовые, граф. дан. (147 Кб). - Воронеж : ВГТУ, 2005.	2005 Электронный ресурс	
Л2.2	Дуров В.П.	Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие / В. П. Дуров. - Электрон. дан. (1 файл :6681088 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006	2006 Электронный ресурс	
Л2.3	Гончаров И.В.	Основы применения технических средств информационной безопасности [Электронный ресурс] : Методические указания к практическим занятиям по дисциплине "Технические средства и методы защиты информации" для студентов специальности 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" очной формы обучения / каф. систем информационной безопасности; сост. Гончаров И.В. - Электрон. текстовые, граф. дан. (539 Кб). -	2007 Электронный ресурс	

		Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007.		
3. Методические разработки				
Л3.1				
Л3.2				

Зав. кафедрой _____ / А.Г. Остапенко /

Директор НТБ _____ / Т.И. Буковшина /