МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита информации от утечки по техническим каналам»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Дешина А.Е,/

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

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2021

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 «Защита информации от утечки по техническим каналам» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Защита информации от утечки по техническим каналам» направлен на формирование следующих компетенций:

ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и

нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-9	знать порядок организации работ по защите информации от утечки по техническим каналам
	уметь планировать, организовывать и контролировать выполнение мероприятий по защите информации от утечки по техническим каналам
	владеть навыками установки и наладки средств защиты информации от утечки по техническим каналам
ОПК-6	знать организацию работы и нормативно-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 утечки информации по техническим каналам
	владеть методами расчета и инструментального контроля показателей технической защиты информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита информации от утечки по техническим каналам» составляет 8 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		7	8
Аудиторные занятия (всего)	180	108	72
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	108	72	36
Самостоятельная работа	72	36	36
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 288 8	 144 4	 144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Технические каналы утечки 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.	12	18	12	42
2	Средства обнаружения каналов утечки информации	Индикаторы электромагнитных излучений. Радиочастотомеры. Сканирующие приемники, селективные вольтметры, анализаторы спектра. Автоматизированные поисковые комплексы Характеристики индикаторов электромагнитных излучений, Радиочастотомеров, сканирующих приемников, селективных вольтметров, анализаторов спектра Характеристики нелинейных локаторов и селективных металлодетекторов	12	18	12	42
3	Организация инженерно-технической защиты информации	Организационно-методические основы защиты информации. Общие требования к защите информации. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации Методика принятия решения на защиту от утечки информации в организации. Алгоритм принятия решения. Разработка вариантов и выбор оптимального решения	12	18	12	42
4	Методы и средства защиты информации от утечки по техническим каналам	Организация защиты речевой информации. Пассивные средства защиты выделекнных помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации. Рекомендации про выбору систем виброакустической защиты. Подавление диктофонов. Нейтрализация радиомикрофонов. Защита электросети. Защита оконечного оборудования слаботочных линий. Защита абонентского участка телефонных линий. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН. Критерий защищенности средств вычислительной техники. Нормированные уровни помех в каналах утечки. Методика проведения специальных исследований технических средств ЭВТ. Метод расчета	12	18	12	42

		радиуса зоны II (R2) технических средств ЭВТ. Организация защиты ПЭВМ от несанкционированного доступа				
5	Мероприятия по выявлению каналов утечки информации	Специальные проверки. Порядок проведения специальной проверки технических средств Подготовка к проведению специальных обследований. Выполнение поисковых мероприятий. Подготовка отчетных материалов 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.	12	18	12	42
6	Методы и средства контроля эффективности защиты информации по техническим каналам утечки	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 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.	12	18	12	42
		Итого	**72**	**108**	**72**	**252**

5.2 Перечень лабораторных работ

	Наименование практической работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
Технические каналы утечки информации		**18**		
	Оценка дальности и пропускной способности передачи информации по каналу утечки.	6		отчет
	Многофункциональный поисковый прибор ST-031 «Пиранья»	6		отчет
	Исследование детектора	6		отчет

	электромагнитного поля ST107			
Средства обнаружения каналов утечки информации		**18**		
	Аппроксимация результатов статистического моделирования.	6		отчет
	Разработка матрицы конфликтного взаимодействия для типовых ТКС.	6		отчет
	Разработка тактик защиты, контроля для типовой ТКС с учетом целевого назначения ТКС.	6		отчет
Организация инженерно-технической защиты информации		**18**		
Разработка математической модели канала утечки информации применительно к радиотехнической и акустической разведкам.		8		отчет
Организация аттестации выделенного помещения по требованиям безопасности информации		10		отчет
Методы и средства защиты информации		**18**		
Методология защиты информации от утечки за счет ПЭМИН		8		отчет
Системы вибрационной и акустической защиты		10		отчет
Мероприятия по выявлению каналов утечки информации		**18**		
Исследования в области акустоэлектрических преобразований (АЭП)		8		отчет
Исследования в области в области ВЧ-навязывания		10		отчет
Методы и средства контроля эффективности технической защиты информации		**18**		
	Расчет эффективности защиты информации в ТКС.	8		отчет
	Способы оценки размеров зон I и II.	10		отчет

	Оценка дальности перехвата сигналов.			
Итого:		**108**		

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

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

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

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-9	знать порядок организации работ по защите информации от утечки по техническим каналам	знание порядка организации работ по защите информации от утечки по техническим каналам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь планировать, организовывать и контролировать выполнение мероприятий по защите информации от утечки по техническим каналам	умение планировать, организовывать и контролировать выполнение мероприятий по защите информации от утечки по техническим каналам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками установки и наладки средств защиты информации от утечки по техническим каналам	владение навыками установки и наладки средств защиты информации от утечки по техническим каналам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-6	знать организацию работы и нормативно-правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты	знание организации работы и нормативно-правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации		
	уметь пользоваться нормативными документами по противодействию утечки информации по техническим каналам	умение пользоваться нормативными документами по противодействию утечки информации по техническим каналам	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

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7, 8 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ОПК-9	знать порядок организации работ по защите информации от утечки по техническим каналам	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь планировать, организовывать и контролировать выполнение мероприятий по защите информации от утечки по техническим каналам	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками установки и наладки средств защиты информации от утечки по техническим каналам	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ОПК-6	знать организацию работы и нормативно-правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации			
	уметь пользоваться нормативными документами по противодействию утечки информации по техническим каналам	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть методами расчета и инструментального контроля показателей технической защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-9	знать порядок организации работ по защите информации от утечки по техническим каналам	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь планировать, организовывать и контролировать выполнение мероприятий по защите информации от утечки по техническим каналам	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками установки и наладки средств защиты информации от утечки по техническим каналам	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ОПК-6	знать организацию работы и нормативно-правовые акты и стандарты по лицензированию деятельности в	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации					
	уметь пользоваться нормативными документами по противодействию утечки информации по техническим каналам	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 не 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 не решены

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

7.2.1 Примерный перечень заданий для подготовки к тестированию

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

7.2.2 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

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=√(〖f_н f〗_в)

В) f_ср=√(〖f_в-f〗_н)

С) f_ср=0,5√(〖f_в f〗_н)

Д) f_ср=√(〖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= 10lgI_0/I_пс

В) E= lgI_0/I_пс

С) E= 10lgI_ /I_0

Д) E= 10lgI_ /I_пс

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 зачету

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.
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 разведка

7.2.5 Примерный перечень заданий для подготовки к экзамену

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. 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.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Технические каналы утечки информации	ОПК-9, ОПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата
2	Средства обнаружения каналов утечки информации	ОПК-9, ОПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата
3	Организация инженерно-технической защиты информации	ОПК-9, ОПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата
4	Методы и средства защиты информации от утечки по техническим каналам	ОПК-9, ОПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата
5	Мероприятия по выявлению каналов утечки информации	ОПК-9, ОПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата
6	Методы и средства контроля эффективности защиты информации по техническим каналам утечки	ОПК-9, ОПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется

проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Технические средства и методы защиты информации: Учеб. пособие / А. П. Зайцев [и др.]; под ред. А. П. Зайцева и А. А. Шелупанова. - [4-е изд., перераб. и доп.]. - М.: Горячая линия -Телеком, 2009. - 616 с.: ил. - ISBN 978-5-9912-0084-4: 469-00.

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. - 1 файл. - 30-00.

3. Радько Н.М. Защита информации в беспроводных сетях [Электронный ресурс]: Учеб. пособие / Н. М. Радько, А. Н. Мокроусов. - Электрон. текстовые, граф. дан. (835 072 байт). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2010. - 1 файл. - 30-00.

Дополнительная литература:

1. Методические указания к лабораторным работам по дисциплине "Техническая защита информации" для студентов специальностей 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. И. В. Гончаров. - Электрон. текстовые, граф. дан. (679 Кбайт). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

2. Методические указания к самостоятельным работам по дисциплине «Техническая защита информации» для студентов

специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения Воронеж [Электронный ресурс] / Каф. систем информационной безопасности; Сост. А. Е. Дешина. - Электрон. текстовые, граф. дан. (263 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

3. Технические средства обеспечения информационной безопасности [Электронный ресурс]: учеб. пособие / И. В. Гончаров [и др.]. - Электрон. дан. (1 файл). - Воронеж: ВГТУ, 2004. - 1 файл. - 30.00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

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/ (ЭБС IPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Защита информации от утечки по техническим каналам» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных	Деятельность студента

занятий	
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.