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 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределенных компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____/А.Е. Дешина/

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 подготов

1.2.Задачиосвоениядисциплины:

- Изучение технических каналов утечки информации, обрабатываемой средств
- Изучение технических каналов утечки акустической (речевой) информации;
- Изучение способов и средств защиты информации, обрабатываемой техничес
- Изучение способов и средств защиты выделенных (защищаемых) помещений
- Освоение методов и средств контроля эффективности защиты информации от
- Освоение основ организации технической защиты информации на объектах и

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Техническаязащитаинформации»Б1.Б.25относитсякдисциплинам «Физика»

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИП

Процессизучениядисциплины«Техническаязащитаинформации»направленнаф

ОПК-1-способностьюанализироватьфизическиеявленияипроцессыприрешении

ПК-3-способностьюпроводитьанализбезопасностикомпьютерныхсистемнасоот

ПК-6-способностьюучаствоватьвразработкепроектнойитехническойдокумента

ПК-18-способностьюпроизводитьустановку,наладку,тестированиеиобслужива ябазамиданных,компьютерныесети,системыантивирусной защиты,средствакриптогра

ПК-19-способностьюпроизводитьпроверкитехническогосостоянияипрофилакт

Компетенция	
ОПК-1	Знать: спос
	Уметь раз
	Владеть н
ПК-3	Знать защ
	Уметь при
	Владеть м
ПК-6	Знать орга аттестации
	Уметь пол
	Владеть м
ПК-18	Знать поряд
	Уметь план
	Владеть на
ПК-19	Знать спосо
	Уметь пров
	Владеть на

Общаятрудоемкостьдисциплины«Техническаязащитаинформации»составляет4

Распределениетрудоемкостидисциплиныповидамзанятий
очнаяформаобучения

Видыучебнойработ
Аудиторныезанятия (всего)
В томчисле:
Лекции
Лабораторныеработы (ЛР)
Самостоятельнаяработа
Виды промежуточной аттестации - зачет с оценкой
Общая трудоемкость: академические часы зач.ед.

№ п/п	Наименованиетемы	
1	Техническиеканалыутечкиинформации	Системный по Характеристик информации. П Понятие и особ Структура, кла Распространен Распростране оптических си
2	Способы и средства защиты информации от утечки по техническим каналам	Основные кон Цели и задачи инженерно-тех Особенности и Демаскирующ Моделировани моделирования Основные поня дискретными с Моделировани Основные этап безопасности и Задачи защиты Понятие конфл Информацион Стратегии про информации, в
3	Методы и средства контроля эффективности технической защиты информации	Контроль эффе

		Виды контроля Виды техничес Методические Способы оценк информации в I и II.
4	Организациятехническойзащитыинформации	Государственна Основные зада документы по Физические ос Классификаци Классификация Методы инжен Классификаци структурное ск Математическа
Итого	**54**	

5.2Переченьлабораторныхработ

Неделя семестра	Наименование практическойработы	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

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ОПК-1	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-3	Знать защитные механизмы и средства обеспечения сетевой безопасности	Знание защитных механизмов и средств обеспечения сетевой безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Умение применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами и средствами технической защиты информации	укажитекритерий	Выполнение работ в срок, предусмотренный	Невыполнение работ в срок, предусмотренны

			в рабочих программах	й в рабочих программах
ПК-6	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	Знание правил организации 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	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь пользоваться нормативными документами по противодействию технической разведке	Умение пользоваться нормативными документами по противодействию технической разведке	Выполнение работ в срок, предусмотренный в рабочих программах	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-18	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 навыками установки и наладки технических средств защиты информации	Владение навыками установки и наладки технических средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-19	Знать способы проверки технического состояния средств защиты информации	Знание способов проверки технического состояния средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь проверять текущее состояние технических средств защиты информации	Умение проверять текущее состояние технических средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками профилактической проверки технических средств защиты информации	Владение навыками профилактической проверки технических средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв10семестредляочнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-1	Знать: способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Тест	Выполнение тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачине решены
	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	Задачине решены
ПК-3	Знать защитные механизмы и средства обеспечения сетевой безопасности	Тест	Выполнение тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачине решены
	Владеть методами и средствами технической защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные	Продемонстрированверный ход решения всех, но не получен верный ответ	Продемонстрированверный ход решения в большинстве задач	Задачине решены

			ответы	во всех задачах		
ПК-6	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 тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь пользоваться нормативными документами по противодействию технической разведке	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачине 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	Задачине решены
ПК-18	Знать порядок организации работ по технической защите конфиденциальной информации на объектах информатизации	Тест	Выполнение тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 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	Задачине решены
	Владеть навыками установки и наладки технических средств защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрированверный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрированверный ход решения в большинстве задач	Задачине решены

ПК-19	Знать способы проверки технического состояния средств защиты информации	Тест	Выполнение тестана 90- 100%	Выполнениетестана 80-90%	Выполнениетестана 70-80%	В тесте менее 70% правильных ответов
	Уметь проверять текущее состояние технических средств защиты 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	Задачине решены
	Владеть навыками профилактической проверки технических средств защиты	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	Задачине 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

7.2.4Примерныйпереченьвопросовдляподготовкикзачету 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 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

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.

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Зачет с оценкой проводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопрсвтестеоценивается1баллом,задачаоцениваетсяв10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)ди	Кодконтролируем	Наименованиеоценочног

	сциплины	ойкомпетенции	осредства
1	Техническиеканалыутечкиинформации	ОПК-1, ПК-3, ПК-6, ПК-18, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
2	Способы и средства защиты информации от утечки по техническим каналам	ОПК-1, ПК-3, ПК-6, ПК-18, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
3	Методы и средства контроля эффективности технической защиты информации	ОПК-1, ПК-3, ПК-6, ПК-18, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
4	Организациятехническойзащитыинформации	ОПК-1, ПК-3, ПК-6, ПК-18, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

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 "Воронежскийгосударственныйтехническийуниверситет", 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.

8.2Переченьинформационныхтехнологий,используемыхприосуществленииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Техническаязащитаинформации»читаютсялекции,проводятсялабораторныеработы.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Видучебныхзанятий	Деятельностьстудента
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.
Лабораторнаяработа	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.
Самостоятельнаяработа	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 промежуточнойаттестации.
Подготовка к промежуточнойаттестации	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 с оценкой три дня эффективнее всего

	использовать для повторения и систематизации материала.