МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

«Физические основы защиты информации»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Специализация Обеспечение информационной безопасности распределенных информационных систем
Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Бабурин А.В./
Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины овладение теоретическими основами защиты информации от ее утечки по техническим каналам

1.2. Задачи освоения дисциплины

- ознакомление с физическими основами возникновения технических каналов утечки информации;
- освоение методических основ оценки эффективности защиты информации от утечки по техническим каналам;
- освоение методов и средств защиты информации от утечки по техническим каналам

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Физические основы защиты информации» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Физические основы защиты информации» направлен на формирование следующих компетенций:

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

ПК-13 - способностью участвовать в проектировании средств защиты информации автоматизированной системы

ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-8	знать новые образцы программных, технических средств и информационных технологий
	уметь принимать участие в освоении новых образцов программных, технических средств и информационных технологий
	владеть навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам
ПК-13	знать принципы проектирования защищенных информационных систем, методы и средства обеспечения целостности, конфиденциальности и доступности данных на основе изучения физических основ защиты информации

	уметь выбирать и настраивать соответствующие технологии и средства защиты для последующей интеграции средства защиты в существующую инфраструктуру.
	владеть проектированием средств защиты информации автоматизированной системы
ПК-15	знать принципы сертификации средств защиты информации автоматизированных систем
	уметь оценивать эффективность защиты информации от утечки по техническим каналам
	владеть способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Физические основы защиты информации» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		4	5
Аудиторные занятия (всего)	108	54	54
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	36	18	18
Самостоятельная работа	72	54	18
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 108 3	 108 3

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	Прак зан.	СРС	Всего, час
1	Физические принципы возникновения технических каналов утечки информации	Понятие технического демаскирующего признака. Определение ТКУИ. Физические принципы аппаратуры перехвата сигналов, регистрации, измерения параметров сигналов в различных физических полях	12	12	12	36
2	Методические основы построения моделей	Система показателей оценки опасности ТКУИ. Формирование параметрических описаний	12	12	12	36

	технических каналов утечки информации	информативных сигналов, среды распространения и аппаратуры приема сигналов. Показатели оценки опасности ТКУИ				
3	Модель утечки информации по радиоканалу	Структура ТКУИ по радиоканалу. Параметры защищаемого радиосигнала. Особенности распространения радиоволн разных диапазонов. Расчет мощности сигнала в точке приема	12	12	12	36
4	Методический подход к обоснованию эффективности защиты информации от ее утечки по радиоканалу	Понятие оптимального приемника. Критерии идеального наблюдателя и Неймана-Пирсона. Структурная схема оптимального приемника. Понятие порога принятия решения	12	12	12	36
5	Модель утечки информации по оптико-электронным каналам	Структура ТКУИ по телевизионному каналу. Параметры защищаемого изображения. Особенности распространения электромагнитных волн оптического диапазона. Расчет освещенности изображения. Разновидности оптико-электронных каналов утечки информации	12	12	12	36
6	Методические основы обоснования эффективности защиты утечки информации п оптико-электронным каналам	Расчет воспринимаемого отношения сигнал/шум. Расчет вероятности обнаружения изображения. Понятие линейного разрешения на местности. Критерий Джонсона. Методы! и средства защиты информации от утечки по оптико-электронным каналам	12	12	12	36
		Итого	**72**	**72**	**72**	**216**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

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-8	знать новые образцы программных, технических средств и информационных технологий	знать новые образцы программных, технических средств и информационных технологий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь принимать участие в освоении новых образцов	уметь принимать участие в освоении новых образцов программных, технических	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный в

	программных, технических средств и информационных технологий	средств и информационных технологий	рабочих программах	рабочих программах
	владеть навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	владеть навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-13	знать принципы проектирования защищенных информационных систем, методы и средства обеспечения целостности, конфиденциальности и доступности данных на основе изучения физических основ защиты информации	знать принципы проектирования защищенных информационных систем, методы и средства обеспечения целостности, конфиденциальности и доступности данных на основе изучения физических основ защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выбирать и настраивать соответствующие технологии и средства защиты для последующей интеграции средства защиты в существующую инфраструктуру.	уметь выбирать и настраивать соответствующие технологии и средства защиты для последующей интеграции средства защиты в существующую инфраструктуру.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть проектированием средств защиты информации автоматизированной системы	владеть проектированием средств защиты информации автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-15	знать принципы сертификации средств защиты информации автоматизированных систем	знать принципы сертификации средств защиты информации автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь оценивать эффективность защиты информации от утечки по техническим каналам	уметь оценивать эффективность защиты информации от утечки по техническим каналам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	владеть способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	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 4, 5 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-8	знать новые образцы программных, технических средств и информационных технологий	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь принимать участие в освоении новых образцов программных, технических средств и информационных технологий	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-13	знать принципы проектирования защищенных информационных систем, методы и средства обеспечения целостности, конфиденциальности и доступности данных на основе изучения физических основ защиты информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь выбирать и настраивать соответствующие технологии и средства защиты для последующей интеграции средства защиты в существующую инфраструктуру.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть проектированием средств защиты информации автоматизированной системы	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-15	знать принципы сертификации средств защиты информации автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	уметь оценивать эффективность защиты информации от утечки по техническим каналам	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-8	знать новые образцы программных, технических средств и информационных технологий	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь принимать участие в освоении новых образцов программных, технических средств и информационных технологий	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 навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	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
ПК-13	знать принципы проектирования защищенных информационных систем, методы и средства обеспечения целостности, конфиденциальности и доступности данных на основе изучения физических основ защиты информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	уметь выбирать и настраивать соответствующие технологии и средства защиты для последующей интеграции средства защиты в существующую инфраструктуру.	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 проектированием средств защиты информации автоматизированной системы	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
ПК-15	знать принципы сертификации средств защиты информации автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь оценивать эффективность защиты информации от утечки 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 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	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.Какой из следующих методов относится к физическим методам защиты информации?

a) Шифрование данных

b) Использование экранированных помещений

c) Аутентификация пользователей

Правильный ответ: b

2.Что такое электромагнитная совместимость (ЭМС) в контексте защиты информации?

a) Способность устройства работать в условиях электромагнитных помех

b) Метод шифрования данных

c) Процесс аутентификации пользователей

Правильный ответ: a

3.Какой из следующих методов используется для защиты информации от несанкционированного доступа через электромагнитные излучения?

a) Криптографические методы

b) Экранирование

c) Биометрическая аутентификация

Правильный ответ: b

4.Что такое TEMPEST?

a) Метод шифрования данных

b) Стандарт по защите информации от утечек через побочные электромагнитные излучения

c) Протокол сетевой безопасности

Правильный ответ: b

5.Какой из следующих методов используется для защиты информации от подслушивания через акустические каналы?

a) Использование звукоизоляционных материалов

b) Шифрование данных

c) Биометрическая аутентификация

Правильный ответ: a

6.Что такое физическая изоляция в контексте защиты информации?

a) Метод шифрования данных

b) Разделение информационных систем на отдельные физические компоненты для предотвращения несанкционированного доступа

c) Процесс аутентификации пользователей

Правильный ответ: b

7.Какой из следующих методов используется для защиты информации от несанкционированного доступа через оптические каналы?

a) Использование оптических фильтров

b) Шифрование данных

c) Биометрическая аутентификация

Правильный ответ: a

8.Что такое защита от несанкционированного доступа (ЗНД) в контексте физической безопасности?

a) Метод шифрования данных

b) Комплекс мер, направленных на предотвращение физического доступа к информационным системам

c) Процесс аутентификации пользователей

Правильный ответ: b

9.Какой из следующих методов используется для защиты информации от утечек через вибрационные каналы?

a) Использование виброизоляционных материалов

b) Шифрование данных

c) Биометрическая аутентификация

Правильный ответ: a

10.Что такое защита от электромагнитных импульсов (ЭМИ)?

a) Метод шифрования данных

b) Комплекс мер, направленных на защиту информационных систем от воздействия электромагнитных импульсов

c) Процесс аутентификации пользователей

Правильный ответ: b

7.2.2 Примерный перечень заданий для решения стандартных задач

1.Какой метод следует использовать для защиты информации от утечек через электромагнитные излучения?

a) Шифрование данных

b) Экранирование помещений

c) Биометрическая аутентификация

Правильный ответ: b

2.Какой из следующих методов наиболее эффективен для защиты информации от подслушивания через акустические каналы?

a) Использование звукоизоляционных материалов

b) Шифрование данных

c) Аутентификация пользователей

Правильный ответ: a

3.Какой метод используется для защиты информации от несанкционированного доступа через оптические каналы?

a) Использование оптических фильтров

b) Шифрование данных

c) Биометрическая аутентификация

Правильный ответ: a

4.Какой из следующих методов применяется для защиты информации от утечек через вибрационные каналы?

a) Использование виброизоляционных материалов

b) Шифрование данных

c) Аутентификация пользователей

Правильный ответ: a

5.Какой метод следует использовать для защиты информации от электромагнитных импульсов (ЭМИ)?

a) Шифрование данных

b) Экранирование и заземление оборудования

c) Биометрическая аутентификация

Правильный ответ: b

6.Какой из следующих методов используется для предотвращения несанкционированного физического доступа к информационным системам?

a) Шифрование данных

b) Установка систем контроля доступа (СКУД)

c) Биометрическая аутентификация

Правильный ответ: b

7.Какой метод наиболее эффективен для защиты информации от утечек через электромагнитные поля?

a) Использование экранированных кабелей

b) Шифрование данных

c) Аутентификация пользователей

Правильный ответ: a

8.Какой из следующих методов используется для защиты информации от утечек через акустические вибрации?

a) Использование виброизоляционных материалов

b) Шифрование данных

c) Биометрическая аутентификация

Правильный ответ: a

9.Какой метод следует использовать для защиты информации от утечек через оптические волокна?

a) Использование оптических фильтров и защитных кожухов

b) Шифрование данных

c) Аутентификация пользователей

Правильный ответ: a

10.Какой из следующих методов применяется для защиты информации от утечек через электромагнитные излучения, возникающие при работе электронных устройств?

a) Использование экранированных помещений и заземления

b) Шифрование данных

c) Биометрическая аутентификация

Правильный ответ: a

7.2.3 Примерный перечень заданий для решения прикладных задач

1.Какой метод следует использовать для защиты серверной комнаты от электромагнитных излучений?

a) Установка биометрической системы доступа

b) Экранирование стен и потолка

c) Шифрование данных на серверах

Правильный ответ: b

2.Какой из следующих методов наиболее эффективен для предотвращения подслушивания переговоров в конференц-зале?

a) Использование звукоизоляционных панелей

b) Установка видеонаблюдения

c) Шифрование голосовых данных

Правильный ответ: a

3.Какой метод используется для защиты информации, передаваемой по оптоволоконным линиям связи, от перехвата?

a) Использование оптических фильтров и защитных кожухов

b) Установка антивирусного ПО

c) Биометрическая аутентификация пользователей

Правильный ответ: a

4.Какой из следующих методов применяется для защиты информации от утечек через вибрационные каналы в здании?

a) Использование виброизоляционных материалов в стенах и полах

b) Установка системы контроля доступа

c) Шифрование данных на рабочих станциях

Правильный ответ: a

5.Какой метод следует использовать для защиты информации в дата-центре от электромагнитных импульсов (ЭМИ)?

a) Экранирование и заземление оборудования

b) Установка систем контроля доступа

c) Шифрование данных на серверах

Правильный ответ: a

6.Какой из следующих методов используется для предотвращения несанкционированного физического доступа к критическим информационным системам?

a) Установка систем контроля доступа (СКУД)

b) Шифрование данных на серверах

c) Использование звукоизоляционных материалов

Правильный ответ: a

7.Какой метод наиболее эффективен для защиты информации от утечек через электромагнитные поля, создаваемые компьютерными мониторами?

a) Использование экранированных кабелей и фильтров

b) Установка антивирусного ПО

c) Биометрическая аутентификация пользователей

Правильный ответ: a

8.Какой из следующих методов используется для защиты информации от утечек через акустические вибрации в офисных помещениях?

a) Использование виброизоляционных материалов в стенах и полах

b) Установка системы контроля доступа

c) Шифрование данных на рабочих станциях

Правильный ответ: a

9.Какой метод следует использовать для защиты информации от утечек через оптические волокна в корпоративной сети?

a) Использование оптических фильтров и защитных кожухов

b) Установка антивирусного ПО

c) Биометрическая аутентификация пользователей

Правильный ответ: a

10.Какой из следующих методов применяется для защиты информации от утечек через электромагнитные излучения, возникающие при работе электронных устройств в офисе?

a) Использование экранированных помещений и заземления

b) Шифрование данных на серверах

c) Биометрическая аутентификация пользователей

Правильный ответ: a

7.2.4 Примерный перечень вопросов для подготовки к зачету

Понятие технического демаскирующего признака. Определение ТКУИ. Физические принципы аппаратуры перехвата сигналов, регистрации, измерения параметров сигналов в различных физических полях

Система показателей оценки опасности ТКУИ. Формирование параметрических описаний информативных сигналов, среды распространения и аппаратуры приема сигналов. Показатели оценки опасности ТКУИ

Структура ТКУИ по радиоканалу. Параметры защищаемого радиосигнала. Особенности распространения радиоволн разных диапазонов. Расчет мощности сигнала в точке приема.

Понятие оптимального приемника. Критерии идеального наблюдателя и Неймана-Пирсона. Структурная схема оптимального приемника. Понятие порога принятия решения

7.2.5 Примерный перечень заданий для решения прикладных задач

Понятие технического демаскирующего признака. Определение ТКУИ. Физические принципы аппаратуры перехвата сигналов, регистрации, измерения параметров сигналов в различных физических полях

Система показателей оценки опасности ТКУИ. Формирование параметрических описаний информативных сигналов, среды распространения и аппаратуры приема сигналов. Показатели оценки опасности ТКУИ

Структура ТКУИ по радиоканалу. Параметры защищаемого радиосигнала. Особенности распространения радиоволн разных диапазонов. Расчет мощности сигнала в точке приема.

Понятие оптимального приемника. Критерии идеального наблюдателя и Неймана-Пирсона. Структурная схема оптимального приемника. Понятие порога принятия решения.

Структура ТКУИ по телевизионному каналу. Параметры защищаемого изображения.

Особенности распространения электромагнитных волн оптического диапазона. Расчет освещенности изображения. Разновидности оптико-электронных каналов утечки информации

Расчет воспринимаемого отношения сигнал/шум. Расчет вероятности обнаружения изображения. Понятие линейного разрешения на местности. Критерий Джонсона. Методы и средства защиты информации от утечки по оптико-электронным каналам

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	Физические принципы возникновения технических каналов утечки информации	ОПК-8, ПК-13, ПК -15	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Методические основы построения моделей технических каналов утечки информации	ОПК-8, ПК-13, ПК -15	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Модель утечки информации по радиоканалу	ОПК-8, ПК-13, ПК -15	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Методический подход к обоснованию эффективности защиты информации от ее утечки по радиоканалу	ОПК-8, ПК-13, ПК -15	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Модель утечки информации по оптико-электронным каналам	ОПК-8, ПК-13, ПК -15	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

6	Методические основы обоснования эффективности защиты утечки информации п оптико-электронным каналам	ОПК-8, ПК-13, ПК -15	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

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

Физические основы защиты информации [Электронныйресурс]

. - Электрон. текстовые, граф. дан. (5,34 Мб). - Воронеж :

ФГБОУ ВПО "Воронежский государственный технический университет", 2015. -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:

Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru

Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org

База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia

Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories

База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls

База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/

Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news

Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/

SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: http://securitypolicy.ru/

SearchInform - Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/

Информационная безопасность предприятия. Электрон. дан. - Режим доступа: Ekrost.ru

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

По дисциплине «Физические основы защиты информации» читаются лекции, проводятся практические занятия.

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

Вид учебных занятий	Деятельность студента
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.

Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
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.