

**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

«Физические основы защиты информации»

Специальность 10.05.02 Информационная безопасность
телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью
телекоммуникационных систем и сетей"

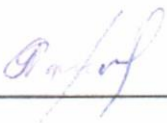
Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы

 /Пахомова А.С./

**Заведующий кафедрой
Систем информационной
безопасности**

 /Остапенко А.Г./

Руководитель ОПОП

 /Остапенко А.Г./

Воронеж 2021

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 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 части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

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

ПК-9.2 – Способен участвовать в работах по проектированию и созданию систем защиты информации на объектах информатизации на основе изучения физических основ формирования технических каналов утечки информации

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-9.2	Знать физические основы возникновения технических каналов утечки информации
	Уметь оценивать эффективность защиты информации от утечки по техническим каналам
	Владеть навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Физические основы защиты информации» составляет 12 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		4	5
Аудиторные занятия (всего)	144	72	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	72	36	36
Самостоятельная работа	252	144	108
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость:			
академические часы	432	216	216
зач.ед.	12	6	6

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 ТКUI. Физические принципы аппаратуры перехвата сигналов, регистрации, измерения параметров сигналов в различных физических полях	12	12	42	66
2	Методические основы построения моделей технических каналов утечки информации	Система показателей оценки опасности ТКUI. Формирование параметрических описаний информативных сигналов, среды распространения и аппаратуры приема сигналов. Показатели оценки опасности ТКUI	12	12	42	66
3	Модель утечки информации по радиоканалу	Структура ТКUI по радиоканалу. Параметры защищаемого радиосигнала. Особенности распространения радиоволн разных диапазонов. Расчет мощности сигнала в точке приема	12	12	42	66
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	42	66
5	Модель утечки информации по оптико-электронным каналам	Структура ТКUI по телевизионному каналу. Параметры защищаемого изображения. Особенности распространения электромагнитных волн оптического диапазона. Расчет освещенности изображения. Разновидности оптико-электронных каналов утечки информации	12	12	42	66
6	Методические основы обоснования эффективности защиты утечки информации по оптико-электронным каналам	Расчет воспринимаемого отношения сигнал/шум. Расчет вероятности обнаружения изображения. Понятие линейного разрешения на местности.	12	12	42	66

		Критерий Джонсона. Методы и средства защиты информации от утечки по оптико-электронным каналам				
Итого			72	72	252	396

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».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-9.2	Знать физические основы возникновения технических каналов утечки информации	Дает определение ТКУИ, перечисляет и характеризует классы ТКУИ, понимает информационные показатели оценки опасности ТКУИ, определяет понятие нормированного показателя	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	Сопоставляет защищаемые характеристики с физическими принципами формирования ТКУИ, проводит расчеты информационных показателей возможностей с учетом условий утечки информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	Умеет рассчитывать требуемые уровни снижения излучаемых сигналов и обосновывать характеристики средств защиты	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/четырёхбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-9.2	Знать физические основы возникновения технических каналов утечки информации	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 навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	Решение прикладных практических задач	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.
ПК-9.2	Знать физические основы возникновения технических каналов утечки информации	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 навыками обоснования требований к способам и средствам защиты информации от утечки по техническим каналам	Решение прикладных 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

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 (минимум 10 вопросов для тестирования с вариантами ответов)

1. Диапазон работы радиоаппаратуры
А) 10 КГц – 100 ГГц; б) 20 МГц – 1 ГГц
2. Диапазон работы оптической аппаратуры
А) 0,4 мкм – 0,7 мкм; б) 0,4 нм – 0,7 нм
3. Диапазон работы телевизионной аппаратуры
А) 0,4 мкм – 0,7 мкм; б) 0,4 мкм – 1,1 мкм
4. Диапазон работы инфракрасной аппаратуры
А) 3 мкм – 5 мкм; б) 0,4 мкм – 14 мкм
5. Диапазон работы аппаратуры ночного видения
А) 0,4 мкм – 1,2 мкм; б) 1,1 мкм – 14 мкм
6. Единицы измерения спектральной плотности потока мощности
А) дБ/Вт Гц^{-1/2}; б) Гц/м²
7. Единицы измерения световой экспозиции
А) лк x c; б) Вт /м²
8. Единицы измерения отношения сигнал/шум

А)Вт/Гц; б) безразмерная величина

9. Единицы измерения эффективной площади антенны

А) м²/град; б) м²

10. Единицы измерения длины волны

А)м; б)Гц

7.2.2 Примерный перечень заданий для решения стандартных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Для оценки опасности технического средства добывания информации по радиоканалу используется значение коэффициента прозрачности атмосферы?
А) Да; Б) Нет
2. Для расчета отношения сигнал/шум на входе радиоприемника используется значение нормированного показателя?
А) Да; б) нет.
3. К основным информационным показателям оценки возможностей технических средств добывания информации относится отношение сигнал/шум?.
А)Да; б) нет.
4. Характеристика «отношение сигнал/шум» используется для расчета вероятности обнаружения? .
А) Да; б) Нет.
5. Критерий «идеального наблюдателя» учитывает разную плату за ошибки разного рода?.
6. Является площадь объекта параметром объекта, используемым при оценке возможностей его обнаружения по радиоканалу?.
А)Да; б) нет.
9. Эффективная площадь антенны используется при оценке возможностей обнаружения объектов по радиоканалу?.
А)Да;б)Нет.
13. Активные радиопомехи используются для защиты от средств добывания информации по радиоканалу?.
А) Да; б) нет.

7.2.3 Примерный перечень заданий для решения прикладных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Алгоритм оценки опасности технического средства добывания информации содержит блок вычисления характеристик аппаратуры приема информативного излучения?.
А)Да; б) нет.
2. Алгоритм обоснования эффективности защиты объекта от технического средства добывания информации содержит блок вычисления порога принятия решения аппаратурой приема сигналов?.
А)Да; б) нет.
3. Основные информационные показатели оценки возможностей технических средств добывания информации содержат линейное разрешение на

местности? .

А)Да; б) нет.

6. Основные параметры объекта, используемые при оценке возможностей его обнаружения по радиоканалу, содержат ширину спектра сигнала?.

А)Да; б) нет.

7. Основные параметры объекта, используемые при оценке возможностей его обнаружения по инфракрасному каналу, содержат ширину спектра теплового излучения?.

А)Да; б) нет.

13. Основные способы защиты от аппаратуры добывания информации, работающей в радиодиапазоне, содержат уничтожение приемной аппаратуры?.

А)Да; б) нет.

14. Основные способы защиты от оптико-электронной аппаратуры добывания информации содержат маскировочное окрашивание?.

А)Да; б) нет.

15. Основные способы защиты от радиолокационной аппаратуры.

А)Да; б) нет.

16. К оптико-электронной аппаратуре добывания информации относится лазерная аппаратура?.

А)Да; б) нет.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Укажите вопросы для зачета

1. Алгоритм оценки опасности технического средства добывания информации.

2. Алгоритм обоснования эффективности защиты объекта от технического средства разведки.

3. Основные показатели оценки возможностей технических средств разведки.

4. Понятие «отношение сигнал/шум» и его использование в задачах защиты информации технических средств разведки.

5. Основные критерии принятия решений в условиях неопределенности, используемые при расчете вероятности обнаружения объекта.

6. Основные параметры объекта, используемые при оценке возможностей его обнаружения радио-и радиотехнической разведкой.

7. Основные параметры объекта, используемые при оценке возможностей его обнаружения инфракрасной видовой разведкой.

8. Основные параметры объекта, используемые при оценке возможностей его обнаружения радиолокационной видовой разведкой.

9. Основные характеристики аппаратуры радио-и радиотехнической разведки, используемые при оценке возможностей обнаружения объектов защиты.

10. Основные характеристики аппаратуры телевизионной разведки, используемые при оценке возможностей обнаружения объектов защиты.

7.2.5 Примерный перечень заданий для решения прикладных задач

Укажите вопросы для экзамена

1. Средства космической разведки, виды орбит космических аппаратов.
2. Понятие полосы обзора и полосы захвата. Основные расчетные соотношения.
3. Космическая радио и радиотехническая разведка. Основные средства и особенности их применения.
4. Космическая видовая разведка. Основные средства и особенности их применения.
5. Воздушная разведка, носители, оборудование, способы применения.
6. Наземная разведка. Особенности ведения наземной радиолокационной параметрической и радиотехнической разведок.
7. Морская разведка. Классификация гидроакустической разведки.
8. Показатели оценки возможностей технических разведок.
9. Понятие технического канала утечки информации применительно к радиотехнической разведке. Характеристика элементов канала.
10. Расчет отношения сигнал/шум в точке приема радиоизлучения.
11. Апостериорная вероятность. Понятие функции правдоподобия.
12. Понятие технического канала утечки информации применительно к телевизионной разведке. Характеристика элементов канала.
13. Критерий оптимизации приема сигнала. Оптимальный порог обнаружения.
14. Классификация методов и средств защиты информации от Р и РТР.
15. Нормы защиты. Методический подход к оценке эффективности защиты информации от Р и РТР.
16. Алгоритм расчета требуемого уровня дополнительного ослабления

радиосигнала для обеспечения его защищенности от радиотехнической разведки.

17. Характеристика освещенности объекта и фона. Особенности прохождения сигнала (мира) через линейное звено. Понятие частотно-контрастной характеристики.
18. Расчет отношения сигнал/шум в элементе разрешения для ТВР.
19. Расчет воспринимаемого отношения сигнал/шум для ТВР.
20. Варианты описания технических каналов утечки информации для ИКР в зависимости от поддиапазона ведения разведки. Выражения для расчета отношения сигнал/шум в элементе разрешения для различных вариантов.
21. Понятие технического канала утечки информации применительно к радиолокационной видовой разведке. Характеристика элементов канала.
22. Принципы формирования радиолокационных изображений. Расчет мощности сигнала, принятого РЛС.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: 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-9	Тест, контрольная работа, защита

			лабораторных работ, защита реферата, требования к курсовому проекту....
2	Методические основы построения моделей технических каналов утечки информации	ОПК-9	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	Модель утечки информации по радиоканалу	ОПК-9	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-9	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	Модель утечки информации по оптико-электронным каналам	ОПК-9	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	Методические основы обоснования эффективности защиты утечки информации по оптико-электронным каналам	ПК-9	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 методикивыставления 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 [Электронный ресурс] . - 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/>

**9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ
ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**
Средства отображения иллюстративных материалов

**10. 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.

Практические занятия направлены на приобретение практических навыков расчета _____. Занятия проводятся путем решения конкретных задач в аудитории.

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 удастся 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.