МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ"

Декан ФРТЭ _____ Небольсин В.А.

«17» декабря 2025 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Защита информации в каналах связи»

Направление подготовки — 11.04.01 «Радиотехника»

Магистерская программа — «Радиотехнические средства обработки и защиты информации в каналах связи»

Квалификация выпускника — магистр

Срок освоения образовательной программы — 2 года

Форма обучения — очная

Год начала подготовки — 2026

Автор программы _____ /Р.П. Краснов/

Заведующий кафедрой радиотехники _____ /А.В. Останков/

Руководитель ОПОП _____ /А.В. Останков/

Воронеж 2026

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Цель преподавания дисциплины – обеспечение студентов базовыми знаниями, навыками и представлениями о современных методах защиты информации в каналах связи, подверженных воздействию помех.

1.2. Задачи освоения дисциплины

Для достижения цели ставятся следующие задачи:

– освоение методов избыточного кодирования информации;

– изучение принципов построения линейных кодов;

– освоение методов расчета помехоустойчивости при применении корректирующих кодов;

– изучение структур кодеров и декодеров различных кодов;

– изучение сигнально-кодовых конструкций систем передачи информации;

– освоение методов передачи информации с обратной связью.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации в каналах связи» относится к дисциплинам обязательной части блока Б1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Защита информации в каналах связи» направлен на формирование следующих компетенций:

УК-2 — Способен управлять проектом на всех этапах его жизненного цикла;

ОПК-3 — Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач.

Код компетенции	Результаты обучения, характеризующие сформированности компетенции
УК-2	**знает** линейные коды, применяемые в системах передачи информации и радиосвязи, методы расчета помехоустойчивости при применении корректирующих кодов
	умеет выбирать корректирующий код для системы передачи информации в соответствии с требуемым качеством ее передачи по каналу связи
	владеет основами терминологии по корректирующему кодированию, методами анализа свойств корректирующих кодов

	различной сложности
Код компетенции	**Результаты обучения, характеризующие сформированности компетенции**
ОПК-3	**знает** алгоритмы коррекции ошибок блоковыми кодами, алгоритмы коррекции ошибок циклическими кодами, алгоритмы коррекции ошибок кодами БЧХ
	умеет применять алгоритмы коррекции ошибок для их использования в аппаратуре передачи данных
	владеет оценкой свойств различных алгоритмов коррекции ошибок

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины «Защита информации в каналах связи» составляет 5 зачетных единиц.

Распределение трудоемкости дисциплины по видам занятий

Виды учебной работы	Всего часов	Семестры	
		2	3
Аудиторные занятия (всего) в том числе:	82	30	52
лекции	44	10	34
лабораторные работы	38	20	18
Самостоятельная работа	71	42	29
Курсовая работа			есть
Часы на контроль	27	—	27
Виды промежуточной аттестации		зачет	экзамен
Общая трудоемкость академические часы з.е.	 180 5	 72 2	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Содержание разделов дисциплины и распределение трудоемкости по видам занятий

№ п/п	Наименование темы	Содержание раздела	Лекции	Практ. зан.	Лаб. зан.	СРС	Всего, час
2 семестр			**10**	**—**	**20**	**42**	**72**
1	Методы защиты информации в каналах связи.	Основные определения и понятия. Виды помех. Методы защиты от радиопомех в каналах связи. Связность оконечного оборудования. Запросы на повторную передачу.	2			8	10
2	Помехозащита радиоприемных устройств. Модели каналов связи	Помехозащита приемников. АРУ типа вперед, по ближним шумам, с поиском провала в спектре помехи, медленная АРУ. Ограничители сигналов.	2			8	10
3	Модели каналов	Дискретный и непрерывный канал. Канал с памятью, канал без памяти. Обобщенная модель двоичного канала. Двоичный симметричный канал. Графы каналов. Канал со стиранием. Гауссвский канал.	2		10	8	20
4	Защита информация при передаче аналоговых сигналов	Частотная и временная инверсия. Техническая реализация аппаратуры. Преобразования с временными или частотными перестановками (скремблированием) с переменными перестановками под управлением криптоблока и комбинированные мозаичные преобразования	2		10	8	20
5	Основы теории информации	Информационные характеристики дискретных источников. Информационная модель канала связи. Теоретическое обоснование оптимального кодирования двоичных источников.	2			10	12
3 семестр			**34**	**—**	**18**	**29**	**81**
6	Эффективность систем передачи. Помехоустойчивость основных видов корректирующих кодов.	Помехоустойчивость сигналов цифровой модуляции. Показатели эффективности телекоммуникационных систем. Помехоустойчивость блочных кодов. Основные характеристики методов коррекции ошибок. Помехоустойчивость кодов БЧХ. Помехоустойчивость сверточных кодов. Помехоустойчивость каскадных кодов.	4			2	6
7	Классификация	Модели систем передачи информа-	2		2	2	6

	криптографических алгоритмов и шифров. Методы криптоанализа и типы атак.	ции с криптографической защитой. Классификация криптографических механизмов. Методы криптоанализа и типы атак. Классические шифры					
8	Криптографические методы с открытым ключом. Система Диффи-Хеллмана. Шифры Шамиля и Эль-Гамаля. Шифр RSA.	Криптосистемы с открытым ключом. Система Диффи–Хеллмана с открытым ключом. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA.	4			2	6
9	Криптографические хэш-функции Стандарты хэш-функций. Имитовставка.	Хэш-функции. Построение хеш-функций на базе блоковых шифров. Метод Меркла — Дамгарда. Криптографически стойкая хэш-функция. ГОСТ 28147-89. Имитовставка. Протокол SSL/TLS.	2			2	4
10	Электронная цифровая подпись. Подпись на базе шифра Эль-Гамаля, RSA	Электронная подпись RSA. Электронная подпись на базе шифра Эль-Гамаля. Стандарты на электронную (цифровую) подпись. ГОСТ Р34.10-94, FIPS 186.	2		8	3	13
11	Стойкость криптосистем. Теоретические пределы скрытности. Системы с совершенной секретностью	Стойкость криптосистем. Шифр Вернама. Расстояние единственности шифра с секретным ключом. Идеальные криптосистемы. Строго идеальный шифр.	2			3	5
12	Блочные алгоритмы шифрования данных.	Стандарт шифрования DES, ГОСТ 28147-89, RC6, AES. Режимы функционирования блочных шифров.	4			3	7
13	Потоковые шифры.	Потоковые шифры. Шифр RC4. Генераторы псевдослучайных последовательностей.	4			3	7
14	Криптосистемы на эллиптических кривых. Инфраструктура открытых ключей.	Эллиптические кривые. Шифр Эль-Гамаля на эллиптической кривой. ГОСТ Р34.10-2001. Инфраструктура открытых ключей. Иерархия сертификатов.	4			3	7
15	Принципы разнесенного приема	Системы SISO, SIMO, MISO, MIMO. Математическая модель системы MIMO. Пропускная способность системы MIMO. Пропускная способность систем SIMO и MISO	2		8	2	12
16	Пространственно-временное блочное кодиро-	Схема Аламути. Ортогональные пространственно-временные блочные коды. Квазиортогональные	2			2	4

	вание. Схема Аламути.	пространственно-временные блочные коды. Неортогональные пространственно-временные блочные коды.					
17	Системы MIMO, использующие информацию о состоянии канала связи.	Методы получения передатчиком информации о состоянии канала связи. Динамическая модель информации о состоянии канала связи. Линейное прекодирование. Нелинейное прекодирование. Алгоритм Косты.	2			2	4
		Итого	**44**	**—**	**38**	**71**	**153**

5.2. Перечень лабораторных работ

1. Моделирование цифровой системы передачи
2. Исследование аддитивного скремблера
3. Получение шифра методами подстановки и перестановки.
4. Получение электронной цифровой подписи
5. Проверка электронной цифровой подписи
6. Система связи с разнесенным приемом

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

В соответствии с учебным планом освоение дисциплины «Защита информации в каналах связи» предусматривает выполнение курсовой работы в третьем семестре.

Примерная тематика курсовой работы:

«Проектирование цифровой системы передачи».

Задачи, решаемые при выполнении курсовой работы:

1. Привести структурную схему системы передачи данных.
2. Выполнить расчет параметров кодера и декодера примитивного кода.
3. Выполнить расчет АЦП и ЦАП..
4. Осуществить расчет информационных характеристик источника сообщений.
5. Выполнить расчет помехоустойчивости демодулятора.
6. Выбрать тип корректирующего кода и рассчитать помехоустойчивость системы передачи данных.
7. Выполнить сравнение эффективности систем передачи сообщений
8. Заключение и выводы по курсовой работе.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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» и «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
УК-2	**знает** линейные коды, применяемые в системах передачи информации и радиосвязи, методы расчета помехоустойчивости при применении корректирующих кодов	Знание учебного материала и готовность к его обсуждению и применению в рамках выполнения заданий на лабораторных занятиях	Готовность представить аргументированные рассуждения в области корректирующего кодирования	Неспособность представить аргументированные рассуждения, относящиеся к корректирующему кодированию
	умеет выбрать корректирующий код для системы передачи информации в соответствии с требуемым качеством ее передачи по каналу связи	Решение стандартных практических задач в соответствии с индивидуальным вариантом задания на лабораторных занятиях	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеет основами терминологии по корректирующему кодированию, методами анализа свойств корректирующих кодов различной сложности	Выполнение исследовательских задач по корректирующему кодированию на лабораторных занятиях	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-3	**знает** алгоритмы коррекции ошибок блоковыми кодами, алгоритмы коррекции ошибок циклическими кодами, алгоритмы коррекции ошибок кодами БЧХ	Знание учебного материала и готовность к его обсуждению и применению в рамках выполнения заданий на лабораторных занятиях	Готовность представить аргументированные рассуждения в области алгоритмов коррекции ошибок	Неспособность представить аргументированные рассуждения по изучавшимся корректирующим кодам
	умеет применять алгоритмы коррекции ошибок для их использования в аппаратуре передачи данных	Выполнение стандартных исследовательских задач в соответствии с индивидуальным вариантом задания на лабораторных занятиях	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 во втором семестре для очной формы обучения по двухбалльной системе:

«зачтено» или

«не зачтено».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
УК-2	**знает** линейные коды, применяемые в системах передачи информации и радиосвязи, методы расчета помехоустойчивости при применении корректирующих кодов	Знание учебного материала и готовность к его изложению на зачете	Студент демонстрирует понимание учебного материала, ярко выраженную способность самостоятельно использовать знания, умения и навыки при решении практических задач на зачете	Студент демонстрирует незначительное понимание материала, непонимание заданий. Попытки самостоятельного решения практических задач оказываются у него малорезультативными
	умеет выбрать корректирующий код для системы передачи информации в соответствии с требуемым качеством ее передачи по каналу связи	Умение использовать расчеты помехоустойчивости корректирующих кодов на зачете		
	владеет основами терминологии по корректирующему кодированию, методами анализа свойств корректирующих кодов различной сложности	Применение анализа свойств корректирующих кодов различной сложности на зачете		
ОПК-3	**знает** алгоритмы коррекции ошибок блоковыми кодами, алгоритмы коррекции ошибок циклическими кодами, алгоритмы коррекции ошибок кодами БЧХ	Знание учебного материала и готовность к его изложению на зачете	Студент демонстрирует полное понимание учебного материала, ярко выраженную способность самостоятельно использовать знания, умения и навыки при решении практических задач на зачете	Студент демонстрирует незначительное понимание материала, непонимание заданий. Попытки самостоятельного решения практических задач оказываются у него малорезультативными
	умеет применять алгоритмы коррекции ошибок для их использования в аппаратуре передачи данных	Умение анализировать алгоритмы коррекции ошибок на зачете		
	владеет оценкой свойств различных алгоритмов коррекции ошибок	Применение методов определения помехоустойчивости алгоритмов коррекции ошибок на зачете		

Результаты промежуточного контроля знаний оцениваются в третьем семестре для очной формы обучения по четырехбалльной системе:

«отлично»,

«хорошо»,

«удовлетворительно»,

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
УК-2	**знает** линейные коды, применяемые в системах передачи информации и радиосвязи, методы расчета помехоустойчивости при применении корректирующих кодов	Знание учебного материала и готовность к его изложению на экзамене	Студент демонстрирует полное понимание учебного материала, ярко выраженную способность	Студент демонстрирует понимание большей части учебного материала, способность при незначительной по-	Студент демонстрирует частичное понимание материала, способность при получении сторонней помощи	Студент демонстрирует незначительное понимание материала, непонимание заданий. Попытки
	умеет выбрать корректирующий код для си-	Умение использовать расчеты поме-				

	стемы передачи информации в соответствии с требуемым качеством ее передачи по каналу связи	хоустойчивости корректирующих кодов на экзамене	самостоятельно использовать знания, умения и навыки при решении практических задач на экзамене	мощи использовать знания, умения и навыки при решении практических задач на экзамене	к выполнению лабораторных занятий. Попытки самостоятельного решения практических задач демонстрируют нестабильность результатов	самостоятельного решения практических задач оказываются у него малорезультативными
	владеет основами терминологии по корректирующему кодированию, методами анализа свойств корректирующих кодов различной сложности на экзамене	Применение анализа свойств корректирующих кодов различной сложности на экзамене				
ОПК-3	**знает** алгоритмы коррекции ошибок блоковыми кодами, алгоритмы коррекции ошибок циклическими кодами, алгоритмы коррекции ошибок кодами БЧХ	Знание учебного материала и готовность к его изложению на экзамене	Студент демонстрирует полное понимание учебного материала, ярко выраженную способность самостоятельно использовать знания, умения и навыки при решении практических задач на экзамене	Студент демонстрирует понимание большей части учебного материала, способность при незначительной помощи использовать знания, умения и навыки при решении практических задач на экзамене	Студент демонстрирует частичное понимание материала, способность, при получении сторонней помощи, к выполнению лабораторных занятий.	Студент демонстрирует незначительное понимание материала, непонимание заданий. Попытки самостоятельного решения практических задач оказываются у него малорезультативными
	умеет применять алгоритмы коррекции ошибок для их использования в аппаратуре передачи данных	Умение анализировать алгоритмы коррекции ошибок на экзамене				
	владеет оценкой свойств различных алгоритмов коррекции ошибок	Применение методов определения помехоустойчивости алгоритмов коррекции ошибок на экзамене				

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. Что такое блоковый корректирующий код?

а) ... это кодовая комбинация, обладающая избыточностью;

б) ... это кодовая комбинация длиной n с k и r символами;

в) ... это набор разрешенных кодовых комбинаций с определенным кодовым расстоянием d, позволяющим исправлять t ошибок;

г) ... это последовательности информационных символов следующих друг за другом.

2. Дайте определение кодового расстояния d блокового кода. Как величина d может быть определена из набора разрешенных комбинаций кода?

а) кодовым расстоянием d блокового кода называется разность сумм единиц в двух кодовых комбинациях следующих друг за другом;

б) кодовым расстоянием d блокового кода называется величина, позволяющая вычислить все разрешенные кодовые комбинации;

в) кодовым расстоянием d блокового кода называется минимальное хемминговое расстояние, наблюдаемое среди разрешенных кодовых комбинаций кода;

г) кодовым расстоянием d блокового кода называется минимальное хемминговое расстояние самой длинной разрешенной кодовой комбинации.

3. Что такое производящая (образующая) матрица блокового кода и как она строится?

а) производящая (образующая) матрица блокового кода это матрица с минимальным количеством нулей в ее столбцах;

б) производящая (образующая) матрица блокового кода это матрица с минимальным количеством строк с одной единицей;

в) производящая (образующая) матрица блокового кода это матрица с минимальным количеством строк, представляющих собой разрешенные кодовые комбинации корректирующего кода;

г) производящая (образующая) матрица блокового кода это матрица, представляющая собой набор разрешенных кодовых комбинаций корректирующего кода, у которых информационные части состоят из полного набора k строк единичной матрицы и по которому можно построить все разрешенные кодовые комбинации.

4. Проверочная матрица блокового кода – это матрица, ...

а) из которой можно определить номер ошибки в кодовом слове;

б) у которой нет строк единичной матрицы;

в) которая имеет r строк и n столбцов и строится на основе производящей матрицы, причем правая ее часть представляет собой единичную матрицу размерностью r, а левая часть определяется столбцами правой части образующей матрицы, которые становятся ее r строками;

г) из которой можно определить количество нулей в кодовом слове.

5. Транспонированная проверочная матрица блокового кода строится из ...

а) проверочной матрицы путем перестановки ее частей;

б) образующей матрицы путем перестановки ее частей;

в) его проверочной матрицы таким образом, чтобы ее столбцы стали строками транспонированной матрицы;

г) проверочной матрицы путем перестановки в ней нулей и единиц.

6. Какое существует соотношение между производящей и транспонированной матрицами блокового кода?

а) произведение производящей матрицы блокового кода на его транспонированную матрицу образует матрицу- произведение r x k, все строки у которой состоят из одних нулей;

б) произведение производящей матрицы блокового кода на его транспонированную матрицу образует матрицу, состоящую из одних нулей;

в) произведение производящей матрицы блокового кода на его транспонированную матрицу образует единичную матрицу;

г) произведение производящей матрицы блокового кода на его транспонированную матрицу образует последовательность единиц длиной n.

7. Как определить синдром блокового кода? Для определения синдрома блокового кода необходимо ...

а) подсчитать число единиц в принятой разрешенной кодовой комбинации;

б) перемножить разрешенную кодовую комбинацию на транспонированную матрицу блокового кода;

в) перемножить разрешенную кодовую комбинацию на образующую матрицу блокового кода;

г) перемножить разрешенную кодовую комбинацию на проверочные символы блокового кода.

8. Что характеризует синдром и какое его основное свойство используется при декодировании блокового кода?

а) синдром указывает на число единиц и нулей в кодовом слове;

б) синдром характеризует, какое количество ошибок произошло в кодовом слове под воздействием помех;

в) синдром характеризует, есть ли ошибки в кодовом слове, если он равен нулю, то ошибок нет, если он не равен нулю, то в кодовом слове есть ошибки, а сам он равен сумме тех строк транспонированной проверочной матрицы, номера которых совпадают с номерами ошибок в кодовом слове;

г) синдром характеризует, сколько единиц содержит кодовое слово.

9. Как осуществляется кодирование блоковыми корректирующими кодами?

а) для процедуры кодирования блоковыми корректирующими кодами необходимо к информационным символам кодовой комбинации добавить последовательность, состоящую из единиц, взятых от информационной комбинации;

б) для процедуры кодирования блоковыми корректирующими кодами необходимо к информационным символам кодовой комбинации добавить последовательность, состоящую из нулей, взятых от информационной комбинации;

в) для процедуры кодирования блоковыми корректирующими кодами необходимо к информационным символам кодовой комбинации добавить последовательность, полученную в результате умножения информационной комбинации на образующую матрицу блокового кода;

г) для процедуры кодирования блоковыми корректирующими кодами необходимо к информационным символам кодовой комбинации добавить последовательность, полученную в результате деления информационной комбинации на проверочную матрицу блокового кода.

10. Что такое декодирование блоковых корректирующих кодов?

а) декодирование блоковых корректирующих кодов это процедура выделения информационных символов из проверочных символов;

б) декодирование блоковых корректирующих кодов это процедура выделения информационных символов из разрешенной кодовой комбинации;

в) декодирование блоковых корректирующих кодов это процедура выделения информационных символов из результата деления разрешенной кодовой комбинации на проверочные символы;

г) декодирование блоковых корректирующих кодов это процедура, заключающаяся в определении наличия ошибок в кодовом слове и последующего их исправления.

7.2.2. Примерный перечень заданий для решения стандартных задач

Программой не предусмотрено.

7.2.3. Примерный перечень заданий для решения прикладных задач

Программой не предусмотрено.

7.2.4. Примерный перечень вопросов для подготовки к зачету

1. Виды защиты информации. Виды нарушения передачи информации.
2. Виды помех в системах передачи данных.
3. Методы защиты аналоговых и цифровых сигналов в канале связи.
4. Принцип действия АРУ: АРУ «вперед», АРУ по ближним шумам.
5. Принцип действия АРУ: медленная АРУ, АРУ с многократными стробами.
6. Схемы амплитудно-частотной селекции.
7. Модель дискретного канала без памяти, двоичного симметричного канала.
8. Модель гауссовского канала.
9. Принцип частотной и временной инверсии и перестановки.
10. Аппаратура частотной инверсии, частотных перестановок.
11. Аппаратура скремблирования.
12. Дискретный источник информации. Энтропия источника.
13. Энтропия: частная, совместная, частная условная. Связь между ними.
14. Полное количество информации в двоичном симметричном канале.
15. Информационная модель канала связи.
16. Теорема кодирования в канале без помех.
17. Теорема кодирования в канале с помехами.

7.2.5. Примерный перечень вопросов для подготовки к экзамену

1. Помехоустойчивость сигналов цифровой модуляции.
2. Эффективность систем передачи данных.
3. Помехоустойчивость блочных кодов. Энергетический выигрыш

кодирования.

4. Помехоустойчивость кодов БЧХ, сверточных, каскадных кодов.

5. Модель системы передачи информации с криптографической защитой по открытому и защищенному каналу.

6. Модель системы передачи информации с аутентификацией и шифрованием.

7. Виды криптоалгоритмов: симметричные и несимметричные, замены, перестановки, композиционные.

8. Методы криптоанализа и криптоатак.

9. Шифр Цезаря, аддитивный перестановочный шифр, шифр Плейфера.

10. Понятие криптосистемы с открытым ключом, дискретного логарифма.

11. Система Диффи–Хеллмана с открытым ключом.

12. Шифр Шамира.

13. Шифр Эль-Гамаля.

14. Шифр RSA.

15. Понятие хэш-функции. Требования к хэш-функции. Алгоритм построения хэш-функции.

16. Метод построения хэш-функции Меркла — Дамгарда. Стандарт хэшфункций ГОСТ Р 34.11-94.

17. Имитовставки. Типы имитовставок.

18. Электронная подпись RSA. Электронная подпись на базе шифра Эль-Гамаля.

19. Электронная подпись на базе стандарта ГОСТ Р34.10-94.

20. Понятие совершенно секретной криптосистемы. Шифр Вернама.

21. Расстояние единственности шифра с секретным ключом. Строго идеальный шифр.

22. Принципы блочного шифрования. Ячейка Фейстеля. Алгоритм шифрования стандарта DES.

23. Шифр RC6: шифрование и дешифрование блока данных.

24. Шифр AES: функции одного раунда шифрования.

25. Принцип работы потоковых шифров. Шифр RC4.

26. Основные принципы построения шифра на эллиптических кривых.

27. Структура систем SISO, SIMO, MISO, MIMO.

28. Схема Аламути.

29. Ортогональные пространственно-временные блочные коды.

30. Получение и применение информации о состоянии канала связи.

31. Системы с линейным прекодированием.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Основными формами текущего контроля при изучении дисциплины являются индивидуальный устный опрос (УО), тестирование (Т), защита результатов лабораторных исследований (ЗЛ).

При устном опросе и защите результатов лабораторных исследований оценка «отлично» выставляется студенту, корректно ответившему на не менее чем 80% задававшихся ему вопросов; оценка «хорошо» выставляется за успешный ответ не менее чем на 60% вопросов; при ответе, по меньшей мере, на 40% вопросов студент получает оценку «удовлетворительно»; худшие результаты фиксируются как «неудовлетворительные».

При промежуточном (итоговом) контроле в форме экзамена на оценку «отлично» могут претендовать студенты, демонстрирующие знание теоретического материала, способные ответить по меньшей мере на 80% вопросов преподавателя (в рамках утвержденного комплекта оценочных средств (КОС)) и самостоятельно решать задачи, как минимум, среднего уровня сложности. Оценку «хорошо» заслуживают студенты, демонстрирующие знание наиболее важных положений теоретического материала, способные ответить по меньшей мере 60% вопросов преподавателя (в рамках утвержденного КОС) и самостоятельно решать задачи невысокой сложности, а также решать задачи среднего уровня сложности под руководством преподавателя. Оценку «удовлетворительно» получают студенты, демонстрирующие знание наиболее важных положений теоретического материала, способные ответить, как минимум, на 40% вопросов преподавателя (в рамках КОС), а также решать задачи невысокой сложности под руководством преподавателя. При более низкой результативности студент получает оценку «неудовлетворительно».

При контроле в форме зачета студенты, получившие оценку «зачтено», должны продемонстрировать знание наиболее важных положений теоретического материала, ответить, как минимум, на 50% вопросов преподавателя (в рамках КОС), а также решать задачи невысокой сложности под руководством преподавателя. При более низкой результативности студент получает оценку «не зачтено».

Контроль в форме тестирования проводится по тест - билетам, каждый из которых содержит 10 вопросов. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом. Максимальное количество набранных баллов – 30.

При контроле в форме экзамена:

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 16 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 16 до 20 баллов.

3. Оценка «Хорошо» ставится в случае, если студент набрал от 21 до 25 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 26 до 30 баллов.

При контроле в форме зачета:

1. Оценка «Зачтено» ставится, если студент набрал от 16 до 30 баллов.

2. Оценка «Не зачтено» ставится в случае, если студент набрал менее 16 баллов.

7.2.7. Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Методы защиты информации в каналах связи.	УК-2, ОПК-3	Устный опрос, зачет
2	Помехозащита радиоприемных устройств. Модели каналов связи	УК-2, ОПК-3	Устный опрос, зачет
3	Модели каналов	УК-2, ОПК-3	Устный опрос, зачет
4	Защита информация при передаче аналоговых сигналов	УК-2, ОПК-3	Устный опрос, зачет
5	Основы теории информации	УК-2, ОПК-3	Устный опрос, экзамен
6	Эффективность систем передачи. Помехоустойчивость основных видов корректирующих кодов.	УК-2, ОПК-3	Устный опрос, экзамен
7	Классификация криптографических алгоритмов и шифров. Методы криптоанализа и типы атак.	УК-2, ОПК-3	Устный опрос, экзамен
8	Криптографические методы с открытым ключом. Система Диффи-Хеллмана. Шифры Шамиля и Эль-Гамаля. Шифр RSA.	УК-2, ОПК-3	Устный опрос, зачет
9	Криптографические хэш-функции Стандарты хэш-функций. Имитовставка.	УК-2, ОПК-3	Устный опрос, зачет
10	Электронная цифровая подпись. Подпись на базе шифра Эль-Гамаля, RSA	УК-2, ОПК-3	Устный опрос, зачет
11	Стойкость криптосистем. Теоретические пределы скрытности. Системы с совершенной секретностью	УК-2, ОПК-3	Устный опрос, зачет
12	Блочные алгоритмы шифрования данных.	УК-2, ОПК-3	Устный опрос, зачет
13	Потоковые шифры.	УК-2, ОПК-3	Устный опрос, зачет
14	Криптосистемы на эллиптических кривых. Инфраструктура открытых ключей.	УК-2, ОПК-3	Устный опрос, зачет
15	Принципы разнесенного приема	УК-2, ОПК-3	Устный опрос, зачет
16	Пространственно-временное блочное кодирование. Схема Аламути.	УК-2, ОПК-3	Устный опрос, зачет
17	Системы MIMO, использующие информацию о состоянии канала связи.	УК-2, ОПК-3	Устный опрос, зачет

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

При преподавании дисциплины «Защита информации в каналах связи» в качестве формы оценки знаний студентов используются индивидуальные варианты заданий на лабораторные занятия, а также задания на экзамен на бумажном носителе.

Задания к экзамену/зачету включают 2 теоретических вопроса, относящихся к области знаний, определяемой перечнем вопросов к экзамену (см. п. 7.2.5/7.2.4).

При проведении экзамена/зачета разрешается использование:

– конспектов лекций;

– учебной литературы в бумажной форме;

– настольных микрокалькуляторов;

– приложения «Инженерный калькулятор» на ПЭВМ (при проведении зачета в аудитории, содержащей вычислительную технику)

Использование мобильных телефонов, планшетов, ноутбуков и/или иных устройств, предоставляющих беспроводную связь, не допускается.

Время подготовки к ответу по заданию составляет 30…45 мин. Затем осуществляется проверка уровня подготовки в ходе устной беседы с экзаменатором, на которую отводится до 15 минут, и выставляется оценка в соответствии с требованиями из п. 7.1.2.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Перечень учебной литературы, необходимой для освоения дисциплины

1. Матвеев Б.В. Защита информации в телекоммуникационных системах: учеб. пособие. — Воронеж: Изд-во ВГТУ, 2001. — 268 с.

2. Смирнов В. М. - Модемы и кодеки / В. М. Смирнов. – Издательство "Лань", 2026. – 224 с.

URL: https://e.lanbook.com/book/508941

3. Бакулин М.Г., Варукина Л.А., Крейнделин В.Б.Технология MIMO: принципы и алгоритмы/ М.Г. Бакулин, Л.А. Варукина, В.Б. Крейнделин/ – Издательство "Горячая линия-Телеком", 2016. – 244 с. URL: https://e.lanbook.com/book/111007

4. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: Учебное пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак – М.: Издательство "ФЛИНТА", 2017. – 215 с.

URL: https://e.lanbook.com/book/92914

5. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации / Б.Я. Рябко, А.Н. Фионов. – М.: Издательство "Горячая линия-Телеком", 2017. – 230 с

URL: https://e.lanbook.com/book/111097

6. Защита информации в каналах связи [Электронный ресурс] : методические указания к выполнению курсовой работы для студентов направления 11.04.01 «Радиотехника» магистерская программа - «Радиотехнические средства обработки и защиты информации в каналах связи / ФГБОУ ВО "Воронеж. гос. техн. ун-т", Каф. радиотехники; сост. : Р. П. Краснов. - Воронеж : Воронежский государственный технический университет, 2022. - Электрон. текстовые и граф. данные (466 Кб).

7. Защита информации в каналах связи [Электронный ресурс] : методические указания к самостоятельной работе для студентов направления 11.04.01 «Радиотехника» (магистерская программа подготовки «Радиотехнические средства обработки и защиты информации в каналах связи») / ФГБОУ ВО "Воронеж. гос. техн. ун-т", Каф. радиотехники; сост.: Р. П. Краснов. - Воронеж : Воронежский государственный технический университет, 2023. - Электрон. текстовые и граф. данные (265 Кб).

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

Офисный пакет приложений, ПО MATLAB.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Лаборатории кафедры радиотехники, в том числе оснащенные ПК, ресурсы библиотеки ВГТУ, ПК преподавателей и студентов.

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

По дисциплине «Защита информации в каналах связи» читаются лекции, проводятся лабораторные занятия.

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

Лабораторные занятия проводятся в режиме моделирования на персональных компьютерах типовых алгоритмов коррекции ошибок. Они направлены на наглядное изучение взаимосвязи между параметрами радиотехнических устройств, статистическими характеристиками помех, возникающих в каналах связи.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Контроль усвоения материала дисциплины производится устным опросом при защите результатов лабораторных работ. Освоение дисциплины оценивается на экзамене.

При наличии среди обучающихся студентов-инвалидов и лиц с ОВЗ особенности изучения ими дисциплины согласуются с преподавателем в индивидуальном порядке.

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 словарей и 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, практическом или лабораторном занятии.
Лабораторные занятия	Работа с конспектом лекций, просмотр рекомендуемой литературы. Изучение теоретических материалов и подготовка домашних заданий к лабораторным работам. Выполнение исследований; при этом особое внимание следует уделить выявлению взаимосвязей между изменением параметров помех и возможностью кода.
Самостоятельная работа	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 экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, и исследования свойств корректирующих кодов на лабораторных занятиях.