Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 05.10.2023 10:31:18
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет машиностроения

УТВЕРЖДАЮ

Декан

_____ /Е.В. Сафонов/

«27» апреля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Кодирование и шифрование информации в радиоэлектронных системах

Специальность
11.05.01 Радиоэлектронные системы и комплексы

Профиль
Радиоэлектронные системы передачи информации

Квалификация
Инженер

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

Доцент кафедры «Автоматика и управление»,
к.т.н.  А.А. Филимонова/

Согласовано:
Заведующий кафедрой «Автоматика и управление»,
д.т.н., профессор  /А.А. Радионов/

Руководитель образовательной программы
д.т.н., профессор  /А.А. Радионов/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 5
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 6
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 10
3.4 Тематика семинарских/практических и лабораторных занятий 12
3.5 Тематика курсовых проектов (курсовых работ) 13
4 Учебно-методическое и информационное обеспечение 13
4.1 Нормативные документы и ГОСТы 13
4.2 Основная литература 13
4.3 Дополнительная литература 13
4.4 Электронные образовательные ресурсы 14
4.5 Лицензионное и свободно распространяемое программное обеспечение 14
4.6 Современные профессиональные базы данных и информационные справочные системы 14
5 Материально-техническое обеспечение 14
6 Методические рекомендации 14
6.1 Методические рекомендации для преподавателя по организации обучения 14
6.2 Методические указания для обучающихся по освоению дисциплины 15
7 Фонд оценочных средств 16
7.1 Методы контроля и оценивания результатов обучения 16
7.2 Шкала и критерии оценивания результатов обучения 18
7.3 Оценочные средства 24

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью дисциплины является изучение основных закономерностей передачи информации в цифровых телекоммуникационных системах.

Задачей изучения дисциплины является формирование у студентов компетенций, позволяющих самостоятельно проводить математический анализ физических процессов в аналоговых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчивости телекоммуникационных систем и сетей.

Обучение по дисциплине «Кодирование и шифрование информации в радиоэлектронных системах» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции	Наименование показателя оценивания
ПК-7. Способен решать задачи оптимизации существующих и новых технических решений в условиях априорной неопределенности с применением пакетов прикладных программ	ИПК-7.1 Понимает методы оптимизации существующих и новых технических решений в условиях априорной неопределенности; ИПК-7.2 Применяет современный математический аппарат для решения задачи оптимизации; ИПК-7.3 Использует методы оптимизации проектируемых радиоэлектронных систем и комплексов.	**Знать:** технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в системах связи, действующие нормативные требования и государственные стандарты; теорию классических шифров; **Уметь:** решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов; проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи; составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих

		кодирования и шифрование информации. **Владеть:** навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи; навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)». Дисциплина непосредственно связана со следующими дисциплинами и практиками ООП:

Автоматизированные системы контроля и управления радиоэлектронными средствами
Высшая математика
Интеллектуальный анализ данных
Информационная безопасность
Информационные технологии
Компьютерные и промышленные интерфейсы и сети
Основы теории радиосистем передачи информации
Проектирование радиотехнических систем
Радиоавтоматика
Системы глобального позиционирования
Численные методы в электронной технике

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа).

3.1 Виды учебной работы и трудоемкость

№ п/п	Вид учебной работы	Количество часов	Семестры
			9
1	**Аудиторные занятия**	**72**	**72**
	В том числе:		
1.1	Лекции	36	36
1.2	Семинарские/практические занятия	18	18
1.3	Лабораторные занятия	18	18
2	**Самостоятельная работа**	**72**	**72**
	В том числе:		
2.1	Подготовка к лекциям	20	20
2.2	Подготовка к контрольным работам	20	20
2.3	Подготовка к лабораторным работам	20	20
2.4	Подготовка к экзамену по дисциплине	12	12
3	**Промежуточная аттестация**		
	Зачет/диф.зачет/экзамен	-	Экзамен
	Итого	**144**	**144**

3.2 Тематический план изучения дисциплины

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	**Раздел 1. Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность**	**14**	**4**	**2**	**2**	**0**	**6**
1.1	Тема 1. Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSK, GMSK и численный анализ вероятности символьной ошибки		2	2	0	0	2
1.2	Тема 2. Модемы спутниковых систем связи M-QAM, M-PSK, 16-APSK, 32-APSK, и численный анализ вероятности символьной ошибки.		2	0	2	0	4
2	**Раздел 2. Пропускная способность канала связи. Кодирование источника**	**16**	**4**	**4**	**2**	**0**	**6**
2.1	Тема 1. Пропускная способность канала связи. Объем сигнала и емкость канала связи, условия их		2	0	0	0	2

	согласования. Кодирование источника						
2.2	Тема 2. Методы эффективного кодирования. Фрактальное кодирование изображений. Вейвлет-преобразования сигналов и изображений		2	4	2	0	4
3	**Раздел 3. Помехоустойчивое кодирование в телекоммуникационных системах**	**24**	**4**	**4**	**4**	**0**	**12**
3.1	Тема 1. Коды Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона. Циклические избыточные коды CRC (Cyclic redundancycheck).		2	2	2	0	2
3.2	Тема 2. Сверточные коды. Декодирование сверточных кодов по методу Витерби.		0	2	0	0	4
3.3	Тема 3. Турбокодирование. Сверточные турбокоды. Декодирование турбокодов. Характеристики по мехоустойчивости сверточных турбокодов.		0	0	2	0	2
3.4	Тема 4. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов.		2	0	0	0	4
4	**Раздел 4. Сигнально-кодовые конструкции в телекоммуникационных системах**	**12**	**2**	**0**	**4**	**0**	**6**
4.1	Тема 1. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (TCM) и их анализ.		2	0	0	0	2
4.2	Тема 2. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO		0	0	4	0	4
5	**Раздел 5. Классические шифры**	**14**	**6**	**0**	**0**	**0**	**8**
5.1	Тема 1. Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифров замены.		2	0	0	0	2
5.2	Тема 2. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря.		2	0	0	0	4

	Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шифр Хилла.						
5.3	Тема 3. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.		2	0	0	0	2
6	**Раздел 6. Шифрование с секретным ключом**	**22**	**6**	**2**	**4**	**0**	**10**
6.1	Тема 1. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифрования данных DES.		2	0	0	0	4
6.2	Тема 2. Блочный криптоалгоритм стандарт AES. Методы оценки качества алгритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров.		2	0	0	0	2
6.3	Тема 3. Поточные режимы блочных шифров. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обрат ной связью по переносу.		2	2	4	0	4
7	**Раздел 7. Шифрование с открытым ключом**	**10**	**2**	**2**	**0**	**0**	**6**
7.1	Тема 1. Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипосистемы. Алгебраическая обобщенная модель шифра. Односторонние функции.		0	2	0	0	2

	Факторизация. Дискретный логарифм.						
7.2	Тема 2. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации крипто систем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).		2	0	0	0	4
8	**Раздел 8. Криптографические протоколы в сетях передачи данных**	**20**	**4**	**2**	**2**	**0**	**12**
8.1	Тема 1. Сети шифрованной связи. Организация сетей конфиденциальной связи. Основные термины и понятия. Угрозы сетям. Протоколы распределения ключей и их характеристики. Компрометация абонентов сети; способы построения протоколов-шифрованной связи и методы их решения. Повторное использование ключей в сетях шифрованной связи.		2	0	0	0	2
8.2	Тема 2. Подходы к снижению вероятности повторного использования. Современные тенденции развития средств и методов криптографической защиты информации. Программно-аппаратная реализация современных криптографических средств. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем. PGP кодирование и шифрование с открытым ключом. Общие сведения.		0	2	2	0	4
8.3	Тема 3. Безопасность сети передачи данных на транспортном уровне SSL и TLS.		2	0	0	0	2
8.4	Тема 4. Криптографические протоколы, протоколы		0	0	0	0	4

	распределения ключей, парольные системы разграничения доступа. Способы восстановления шифрованной связи после компрометации. Подходы к локализации негативных последствий компрометации. Сети связи с открытым распределением ключей. Проблемы синхронизации в сетях.						
9	**Раздел 9. Шифрование в современных системах связи**	**12**	**4**	**2**	**0**	**0**	**6**
9.1	Тема 1. Безопасность GSM сетей. Алгоритм шифрования A5/1. Системные сообщения GSM. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы и стандарты защиты беспроводных сетей LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности.		2	2	0	0	2
9.2	Тема 2. Иерархия ключей в E-UTRAN. Генерирование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в EUTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование технологии шифрования в сетях LTE.		2	0	0	0	4
	Итого	**144**	**36**	**18**	**18**	**0**	**72**

3.3 Содержание дисциплины

Раздел 1. Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность

Тема 1. Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSK, GMSK и численный анализ вероятности символьной ошибки

Тема 2. Модемы спутниковых систем связи M-QAM, M-PSK, 16-APSK, 32-APSK, и численный анализ вероятности символьной ошибки.

Раздел 2. Пропускная способность канала связи. Кодирование источника

Тема 1. Пропускная способность канала связи. Объем сигнала и емкость канала связи, условия их согласования. Кодирование источника

Тема 2. Методы эффективного кодирования. Фрактальное кодирование изображений. Вейвлет-преобразования сигналов и изображений

Раздел 3. Помехоустойчивое кодирование в телекоммуникационных системах

Тема 1. Коды Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона. Циклические избыточные коды CRC (Cyclic redundancycheck).

Тема 2. Сверточные коды. Декодирование сверточных кодов по методу Витерби.

Тема 3. Турбокодирование. Сверточные турбокоды. Декодирование турбокодов. Характеристики по мехоустойчивости сверточных турбокодов.

Тема 4. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов.

Раздел 4. Сигнально-кодовые конструкции в телекоммуникационных системах

Тема 1. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (TCM) и их анализ.

Тема 2. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO

Раздел 5. Классические шифры

Тема 1. Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифров замены.

Тема 2. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шифр Хилла.

Тема 3. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.

Раздел 6. Шифрование с секретным ключом

Тема 1. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифрования данных DES.

Тема 2. Блочный криптоалгоритм стандарт AES. Методы оценки качества алгритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров.

Тема 3. Поточные режимы блочных шифров. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обрат ной связью по переносу.

Раздел 7. Шифрование с открытым ключом

Тема 1. Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипосистемы. Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм.

Тема 2. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации крипто систем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).

Раздел 8. Криптографические протоколы в сетях передачи данных

Тема 1. Сети шифрованной связи. Организация сетей конфиденциальной связи. Основные термины и понятия. Угрозы сетям. Протоколы распределения ключей и их характеристики. Компрометация абонентов сети; способы построения протоколов-шифрованной связи и методы их решения. Повторное использование ключей в сетях шифрованной связи.

Тема 2. Подходы к снижению вероятности повторного использования. Современные тенденции развития средств и методов криптографической защиты информации. Программно-аппаратная реализация современных криптографических средств. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной

криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем. PGP кодирование и шифрование с открытым ключом. Общие сведения.

Тема 3. Безопасность сети передачи данных на транспортном уровне SSL и TLS.

Тема 4. Криптографические протоколы, протоколы распределения ключей, парольные системы разграничения доступа. Способы восстановления шифрованной связи после компрометации. Подходы к локализации негативных последствий компрометации. Сети связи с открытым распределением ключей. Проблемы синхронизации в сетях.

Раздел 9. Шифрование в современных системах связи

Тема 1. Безопасность GSM сетей. Алгоритм шифрования A5/1. Системные сообщения GSM. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы и стандарты защиты беспроводных сетей LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности.

Тема 2. Иерархия ключей в E-UTRAN. Генерирование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в EUTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование технологии шифрования в сетях LTE**.**

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Практическая работа 1. Модемы сотовой связи FSK, MSKGMSK и численный анализ вероятности символьной ошибки.

Практическая работа 2. Исследование кодирования источника дискретных сообщений методами Шеннона- Фано.

Практическая работа 3. Исследование алгоритмов Лемпеля- Зива.

Практическая работа 4. Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.

Практическая работа 5. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо.

Практическая работа 6. Алгоритмы практической реализации криптосистем с секретным ключом.

Практическая работа 7. Алгоритмы практической реализации криптосистем с открытым ключом.

Практическая работа 8. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных.

Практическая работа 9. Безопасность GSM сетей.

3.4.2 Лабораторные занятия

Лабораторная работа 1. Модемы спутниковых систем связи M-QAM, M-PSK, 16-APSK, 16-APSK и численный анализ вероятности символьной ошибки.

Лабораторная работа 2-3. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо. Циклические избыточные коды CRC (Cyclic redundancycheck). Сверточные коды. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби.

Лабораторная работа 4-5. Турбокодирование. Сверточные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов. Низкоплотностные коды. Алгоритмы декодирования низкоплотных кодов. Исследование каскадных кодов.

Лабораторная работа 6-7. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (ТСМ) и их анализ. Исследование сигнально-кодовой конструкции на базе системы

с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM- MIMO.

Лабораторная работа 8-9. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифрования данных DES. Блочный криптоалгоритм стандарт AES. Российский блочный шифр ГОСТ в поточном режиме. Блочный шифр AES в поточном режиме.

3.5 Тематика курсовых проектов (курсовых работ)

Не предусмотрены

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Не предусмотрены

4.2 Основная литература

1. Голиков, А. М. Кодирование и шифрование информации в системах связи. Часть 1. Кодирование : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2016. — 327 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110240.

2. Голиков, А. М. Кодирование и шифрование информации в системах связи. Часть 2. Шифрование : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2016. — 490 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110225.

3. Голиков, А. М. Кодирование в телекоммуникационных системах : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2016. — 338 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110246.

4. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-47181-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/338018.

4.3 Дополнительная литература

1. Голиков, А. М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика : учебное пособие для вузов / А. М. Голиков. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 452 с. — ISBN 978-5-8114-9233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189336.

2. Исследование методов кодирования и шифрования : учебное пособие / А. П. Алексеев, М. И. Макаров, О. В. Сирант, С. С. Яковлева ; под редакцией А. П. Алексеева. — Самара : ПГУТИ, 2018. — 102 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182252.

3. Трифонов, П. В. Основы помехоустойчивого кодирования : учебное пособие / П. В. Трифонов. — Санкт-Петербург : НИУ ИТМО, 2022. — 231 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/283868.

4.4 Электронные образовательные ресурсы

Не предусмотрены

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Microsoft-Office
2. Microsoft-Windows
3. Math Works-MATLAB, Simulink

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Единое окно доступа к образовательным ресурсам Федеральный портал http://window.edu.ru
2. Компьютерные информационно-правовые системы «Консультант» http://www.consultant.ru, «Гарант» http://www.garant.ru
3. Официальный интернет-портал правовой информации http://pravo.gov.ru.
4. Научная электронная библиотека http://www.elibrary.ru
5. Российская государственная библиотека http://www.rsl.ru
6. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru/index.php

5 Материально-техническое обеспечение

1. Компьютерный класс с предустановленным программным обеспечением, указанным в п. 4.5, мультимедийное оборудование (проектор, персональный компьютер преподавателя).
2. Аудитория для лекционных, практических занятий. Оборудование и аппаратура: аудиторная доска, возможность использования мультимедийного комплекса.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

На первом занятии по дисциплине необходимо ознакомить студентов с порядком ее изучения (темами курса, формами занятий, текущего и промежуточного контроля), раскрыть место и роль дисциплины в системе наук, ее практическое значение, довести до студентов требования к форме отчетности и применения видов контроля. Выдаются задания для подготовки к практическим и семинарским занятиям.

При подготовке к лабораторным и практическим работам по перечню объявленных тем преподавателю необходимо уточнить план их проведения, продумать формулировки и содержание учебных вопросов, выносимых на обсуждение, ознакомиться с перечнем тематических вопросов.

В ходе работы во вступительном слове раскрыть практическую значимость темы работы, определить порядок ее проведения, время на обсуждение каждого учебного вопроса.

Применяя фронтальный опрос дать возможность выступить всем студентам, присутствующим на занятии.

В заключительной части работы следует подвести ее итоги: дать оценку выступлений каждого студента и учебной группы в целом. Раскрыть положительные стороны и недостатки проведенной лабораторной работы. Ответить на вопросы студентов. Выдать задания для самостоятельной работы по подготовке к следующему занятию.

Методика преподавания дисциплины «Кодирование и шифрование информации в радиоэлектронных системах» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся:

– подготовка к выполнению и защита практических и лабораторных работ с помощью специализированного программного обеспечения;

– защита и индивидуальное обсуждение выполняемых этапов расчетно-графических работ;

– технологии анализа ситуаций для активного обучения, которые позволяют студентам соединить теорию и практику, представить примеры принимаемых решений и их последствий, демонстрировать различные позиции, формировать навыки оценки альтернативных вариантов в вероятностных условиях.

Обучение по дисциплине ведется с применением традиционных потоково-групповых информационно-телекоммуникационных технологий. При осуществлении образовательного процесса по дисциплине используются следующие информационно-телекоммуникационные технологии: презентации с применением проектора и программы PowerPoint.

6.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов направлена на решение следующих задач:

Самостоятельная работа является одним из видов учебных занятий. Цель самостоятельной работы – практическое самостоятельное получение студентами навыков работы в программе математического моделирования, рассматриваемых в процессе изучения дисциплины.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Задачи самостоятельной работы студента:

- развитие навыков самостоятельной учебной работы;
- освоение содержания дисциплины;
- углубление содержания и осознание основных понятий дисциплины;
- использование материала, собранного и полученного в ходе самостоятельных занятий для эффективной подготовки к экзамену.

Виды внеаудиторной самостоятельной работы:

- самостоятельное изучение отдельных тем дисциплины;
- подготовка к лабораторным и практическим занятиям;
- оформление отчетов по выполненным практическим и лабораторным работам и подготовка к их защите;
- подготовка к экзамену.

Для выполнения любого вида самостоятельной работы необходимо пройти следующие этапы:

- определение цели самостоятельной работы;
- конкретизация познавательной задачи;
- самооценка готовности к самостоятельной работе;
- выбор адекватного способа действия, ведущего к решению задачи;
- планирование работы (самостоятельной или с помощью преподавателя) над заданием;
- осуществление в процессе выполнения самостоятельной работы самоконтроля (промежуточного и конечного) результатов работы и корректировка выполнения работы;
- рефлексия;
- презентация работы

7 Фонд оценочных средств

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- лабораторные работы;
- практические работы;
- тестирование;
- контрольные работы;
- экзамен.

Оценочные средства текущего контроля успеваемости включают контрольные задания индивидуально для каждого обучающегося.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	**Наименование компетенции выпускника**
ПК-7	Способен решать задачи оптимизации существующих и новых технических решений в условиях априорной неопределенности с применением пакетов прикладных программ

7.1 Методы контроля и оценивания результатов обучения

Перечень оценочных средств по дисциплине «Кодирование и шифрование информации в радиоэлектронных системах».

№ п/п	Вид контроля результатов обучения	Наименование контроля результатов обучения	Краткая характеристика контроля результатов обучения
1	Текущий	Контрольная работа	Решение контрольной работы осуществляется на последнем занятии изучаемой темы. Студенту выдаются 2 задачи. Контрольная работа выполняется индивидуально каждым студентом. При проверке преподаватель оценивает правильность произведенных

			расчетов, алгоритмов, использования терминологии и выводы.
2	Текущий	Тестирование	Тестирование проводится на последнем занятии изучаемой темы. Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. В рамках тестирования проверяется владение терминологией и знание теоретической базы.
3	Текущий	Практическая работа	Практическая работа выполняется индивидуально каждым студентом. Оформленный отчет студент сдает преподавателю на проверку в заранее установленный срок. При проверке преподаватель оценивает качество оформления, правильность расчетов и выводов. К защите практической работы допускаются студенты, которые выполнили работу, оформили в соответствии с требованиями отчет о практической работе и предоставили его к защите. Каждому студенту задается не менее 3-х вопросов на тему практической работы. Далее проводится защита отчета каждым студентом индивидуально в формате "вопрос-ответ" (задаются 3 вопроса).
	Текущий	Лабораторная работа	Лабораторная работа выполняется индивидуально каждым студентом. Оформленный отчет студент сдает преподавателю на проверку в заранее установленный срок. При проверке преподаватель оценивает качество оформления, правильность расчетов и выводов. К защите лабораторной работы допускаются студенты, которые выполнили работу, оформили в соответствии с требованиями отчет о лабораторной работе и предоставили его к защите. Каждому студенту задается не менее 3-х вопросов на тему лабораторной работы. Далее проводится защита отчета каждым студентом индивидуально в формате "вопрос-ответ" (задаются 3 вопроса).
3	Промежуточный	Экзамен	Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения

			обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Экзамен проводится в устной форме. В аудитории находится преподаватель и не более 5 человек из числа студентов. Во время проведения экзамена его участникам запрещается иметь при себе и использовать средства связи (сотовые телефоны, микрофоны и пр.). Студенту выдается билет с тремя вопросами. Количество дополнительных вопросов – не более двух. Количество дополнительных вопросов зависит от полноты ответа студента. Длительность экзамена 2 часа (120 минут). К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Кодирование и шифрование информации в радиоэлектронных системах».

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю).

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в системах связи, действующие нормативные требования и государственные	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в	Обучающийся демонстрирует неполное соответствие следующих знаний: технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в системах связи,	Обучающийся демонстрирует частичное соответствие следующих знаний: технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в системах связи,	Обучающийся демонстрирует полное соответствие следующих знаний: технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в

стандарты; теорию классических шифров.	системах связи, действующие нормативные требования и государственные стандарты; теорию классических шифров.	действующие нормативные требования и государственные стандарты; теорию классических шифров. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	действующие нормативные требования и государственные стандарты; теорию классических шифров. Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	системах связи, действующие нормативные требования и государственные стандарты; теорию классических шифров. Свободно оперирует приобретенными знаниями.
уметь: решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов; проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи; составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих кодирования и шифрование информации.	Обучающийся не умеет или в недостаточной степени умеет: решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов; проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи; составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих кодирования и шифрование информации.	Обучающийся демонстрирует неполное соответствие следующих умений: решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов; проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи; составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих кодирования и шифрование информации. Допускаются значительные	Обучающийся демонстрирует частичное соответствие следующих умений: решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов; проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи; составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих кодирования и шифрование информации. Умения освоены, но допускаются	Обучающийся демонстрирует полное соответствие следующих умений: решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов; проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи; составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих кодирования и

		ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	шифрование информации. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи; навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи.	Обучающийся не владеет или в недостаточной степени владеет навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи; навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи.	Обучающийся в недостаточной степени владеет: навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи; навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет: навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи; навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет: навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи; навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи. Свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкала оценивания промежуточной аттестации: экзамена.

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности, не испытывает затруднений при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует

	приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует полное отсутствие или недостаточное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент не может оперировать знаниями и умениями при их переносе на новые ситуации.

Шкала оценивания текущего контроля.

Наименование контроля результатов обучения	Шкала оценивания	Описание
Контрольная работа по теме раздела	Отлично - Работа высокого качества, уровень выполнения отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, либо некоторые из выполненных заданий содержат незначительные ошибки Хорошо - Уровень выполнения работы отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным	Защита темы включает решение задач в аудитории в течение одной пары и проходит после изучения соответствующего раздела. Билеты состоят из вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 1,5 часа.

	материалом в основном сформированы, некоторые виды заданий выполнены с ошибками. Удовлетворительно - Теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой заданий не выполнено; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий. Неудовлетворительно - Теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, предусмотренные программой задания не выполнены	
Тестирование по пройденной теме	Тест содержит 20 заданий, правильный ответ на 1 задание соответствует 1 баллу. Время тестирования - 30 минут. Студенту предоставляется две попытки для прохождения теста. Максимальная оценка за тест - 20 баллов. Тест считается успешно пройденным, если студент дал не менее 60% правильных ответов (набрал не менее 12 баллов).	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.
Подготовка и защита отчета по практической работе	Зачтено: набрано 3 и более баллов Незачтено: набрано 2 и менее баллов Расчеты выполнены верно – 1 балл, выводы логичны и	В качестве форм текущего контроля знаний студентов используются отчеты по практическим работам. Отчет по практической работе содержит расчеты, выводы.

	обоснованы – 1 балл, оформление работы соответствует требованиям – 1 балл, правильный ответ на один вопрос (при защите задаётся 2 вопроса) – 1 балл.	Защита отчета по практической работе осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность расчетов и выводов. Студенты не выполнившие практическую работу к защите не допускаются
Выполнение и защита лабораторной работы	Зачтено: набрано 3 и более баллов Незачтено: набрано 2 и менее баллов Расчеты выполнены верно – 1 балл, выводы логичны и обоснованы – 1 балл, оформление работы соответствует требованиям – 1 балл, правильный ответ на один вопрос (при защите задаётся 2 вопроса) – 1 балл.	В качестве форм текущего контроля знаний студентов используются отчеты по лабораторным работам. К выполнению экспериментальной части лабораторной работы допускаются студенты, подготовившие протоколы выполнения лабораторной работы. Протоколы оформляются в соответствии с требованиями методических указаний кафедры. Отчет по лабораторной работе содержит протокол проведения лабораторной работы, расчеты, графическую часть, выводы. Защита отчета по лабораторной работе осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность расчетов и выводов. Студенты не выполнившие лабораторную работу к защите не допускаются

7.3 Оценочные средства

7.3.1 Текущий контроль

Типовой комплект контрольных работ

Контрольная работа № 1

1. В RSA криптосистеме открытым ключом абонента В служит (31,91). Выступая в роли криптоаналитика, определить его секретный ключ.

2. В гауссовском канале энергопотенциал составляет 60 дБ×Гц. Какова должна быть минимальная полоса сигнала, теоретически гарантирующая возможность передавать данные по каналу со скоростью 1 Мбит/сек?

3. Простейший дискретный источник (n=5) описывается схемой:

x5	x4	x2	x3	x1
0,341	0,289	0,187	0,171	0,012

Закодировать сообщения источника кодом Хаффмана. Найти среднюю и минимальную длину кодового слова.

Контрольная работа № 2

1. Что можно сказать о существовании двоичного кода длиной 10 со скоростью 0.5, исправляющий любую однократную и помимо того обнаруживающий любую двукратную ошибку?

2. Дана порождающая матрица двоичного кода.

а) Каковы скорость и расстояние этого кода?

б) сколько ошибок он исправляет?

в) декодируйте наблюдение y = (111111);

г) декодируйте наблюдение y = (001001).

3. Постройте слово систематического двоичного циклического кода длины 7 с проверочным полиномом, соответствующее информационным битам 101. Постройте каноническую порождающую матрицу кода.

Контрольная работа № 3

1. Сколько ошибок гарантированно исправляет укороченный двоичный БЧХкод длиной со скоростью 13/25?

2. Сверточный код задан порождающими полиномами .

(а) Какова скорость и длина кодового ограничения кода?

(б) Изобразите схему кодера;

(в) Постройте решетчатую диаграмму и используйте ее для определения свободного расстояния;

(г) Закодируйте поток источника, состоящий из 1000 единиц, и оцените вес кодового слова;

(д) Сколько бит источника окажутся неправильно декодированными, если кодовое слово из всех нулей было перепутано с кодовым словом из пункта (г)? Почему подобный код называется катастрофическим?

Примерный перечень заданий для подготовки к тестированию.

1. Какой из фазовых видов модуляции обеспечивает наибольшую помехоустойчивость?

- BPSK
- QPSK
- 8-PSK
- 16-QAM

2. Какой из фазовых видов модуляции обеспечивает наибольшую скорость передачи информации?

- BPSK
- QPSK
- 8-PSK –
- 16-QAM

3. Какой из видов частотной модуляции имеет минимальную ширину спектра?

- FSK
- MSK
- GMSK
- M-FSK

4. Какой из методов кодирования источника производит кодирование с потерями?

- Коды Шеннона-Фано
- Алгоритм Лемпеля – Зива
- Вейвлет преобразование
- Коды Хаффмана

5. Какой код является блоковым?

- Код Хемминга
- БЧХ (Боуза-Чоудхури-Хоквенгема)
- Рида-Соломона - Файра

6. Какой из кодов обеспечивает наибольшее число обнаруженных ошибок?

- Код Хемминга
- БЧХ (Боуза-Чоудхури-Хоквенгема)
- Рида-Соломона - Файра

7. Какой из циклических избыточных кодов CRC (Cyclic redundancy check) обеспечивает наибольшее число обнаруженных ошибок от числа контрольных сумм для различных полиномов CRC-кода?

- CRC-1
- CRC-16-IBM
- CRC-30
- CRC-4-ITU

8. Какой из кодов обеспечивает наименьшую вероятность битовой ошибки (BER) при SNR > 5 Дб?

- Сверточный
- Каскадный
- Рида-Соломона
- Турбокод

9. Какие из кодов и сигнально-кодовых конструкций наиболее приближены к верхней границе Шеннона?

- АФМ-16-СК
- БЧХ
- ФМ-2
- АМ-2

10. Какое расстояние между сигнальными точками ФМн-8 обеспечивает наибольшую помехоустойчивость?

- 0,765
- 1,414
- 1,848
- 2,000

11. Чему равна величиной предельной энергетической эффективности (предел Шеннона)?

- 1,59 Дб
- 1,69 Дб
- 2,56 Дб
- 3,22 Дб

12. Какова длина дайджеста Хеш-функции ГОСТ?

- 56
- 128
- 192
- 256

13. Какова длина ключа шифра DES?

- 48
- 56
- 128
- 256

14. Какова длина ключа шифра ГОСТ 28147?

- 48
- 56
- 128
- 256

15. Какое количество раундов шифра DES?

- 16
- 32
- 48
- 56

16. Какое количество раундов шифра ГОСТ 28147?

- 16
- 32
- 48
- 56

17. Какова длина ключа шифра AES?

- 128, 192, 256

- 32, 48, 56
- 48, 56, 128
- 56, 128, 256

18. Стандарты блочного шифрования DES (Data Encryption Standard) и AES (Advanced Encryption Standard) имеют следующие основные режимы. Какой из них работает как самосинхронизирующийся поточный шифр?

- Режим электронной кодовой книги, ECB (Electronic Code Book).
- Режим сцепления блоков шифртекста, CBC (Ciphertext Block Chaining).
- Режим обратной связи по шифртексту, CFB (Ciphertext Feedback).
- Режим обратной связи по выходу, OFB (Output Feedback).

19. Отечественный стандарт блочного шифрования ГОСТ 28147-89 может работать в следующих режимах. Какой из них работает как синхронный поточный шифр?

- Режим простой замены
- Режим гаммирования
- Режим гаммирования с обратной связью
- Режим выработки имитовставки

20. Какой из поточных шифров является победителем Международного конкурса eSTREAM?

- Rabbit
- Sosemanuk
- HC-128
- LEXv2

Вопросы для подготовки к практическим работам

1. Модемы сотовой связи FSK, MSKGMSK и численный анализ вероятности символьной ошибки. Модемы спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки.
2. Исследование кодирования источника дискретных сообщений методами Шеннона-Фано.
3. Исследование алгоритмов Лемпеля - Зива. Фрактальные методы кодирования изображений.
4. Вейвлет преобразования сигналов и изображений.
5. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона на базе MATLAB. Циклические избыточные коды CRC (Cyclic redundancy check). Сверточные коды.
6. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби с использованием ПО MATLAB.
7. Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов.
8. Характеристики помехоустойчивости сверточных турбокодов . Исследование турбокодов с использованием ПО MATLAB. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодированияна базе MATLAB и LabVIEW. Исследование каскадных кодов

9. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции(ТСМ) и их анализ с использованием MATLAB. Исследование сигнально-кодовой конструкции на базе системы

10. Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифров замены. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом.

11. Биграммный шифр Плейфейра. ШифрХилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор.

12. Регистр сдвига с линейной обратной связью.

13. Теория шифров с секретным ключом. Блочные и поточные системы шифрования.

14. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ 28147-89. Американский стандарт шифрования данных DES. Блочный криптоалгоритм RIJNDAEL и стандарт AES. Поточные системы шифрования. Поточные режимы блочных шифров.

15. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной связью по переносу. Поточный шифр HC128. Поточный шифр Rabbit. Поточный шифр Salsa20.Поточный шифр SOSEMANUK.SERPENT и его производные. Поточный шифр F-FCSR-H. Поточный шифр Grain-128. Поточный шифр MICKEY-128. Поточный шифр Trivium. Российский блочный шифр ГОСТ 28147-89 в поточном режиме. Блочный шифр AES в поточном режиме. Методы оценки качества алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров.

16. Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипосистемы.

17. Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля.

18. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).

19. Сети шифрованной связи. Организация сетей конфиденциальной связи .Основные термины и понятия. Угрозы сетям. Протоколы распределения ключей и их характеристики. Компрометация абонентов сети; способы построения протоколов распределения ключей, обеспечивающих защиту от компрометации.

20. Криптографические протоколы, протоколы распределения ключей, парольные системы разграничения доступа. Способы восстановления шифрованной связи после компрометации. Подходы к локализации негативных последствий компрометации. Сети связи

с открытым распределением ключей. Проблемы синхронизации в сетях шифрованной связи и методы их решения. Повторное использование ключей в сетях шифрованной связи. Подходы к снижению вероятности повторного использования. Современные тенденции развития средств и методов криптографической защиты информации. Программно-аппаратная реализация современных криптографических средств. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем.

21. PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP.

22. Сжатие данных. Сеть доверия. Сертификаты. Open PGP. Поглощение Network Associates. Современное состояние. Правовые аспекты использования в России. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр).

23. Электронная подпись (ЭП),Электронная цифровая подпись (ЭЦП).Аннулирования открытого ключа PGP. Дезактивация – временное отключение неиспользуемого ключа или ключевой пары. Отпечаток ключа.

24. Имплицитное доверие – полное доверие зарезервировано для ключевых пар, расположенных на локальном ключе. Безопасность сети передачи данных на транспортном уровне SSL и TLS.

25. Безопасность GSM сетей. Алгоритм шифрования A5/1. Системные сообщения GSM. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы истандарты защиты беспроводных сетей LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности.

Вопросы для подготовки к защите лабораторных работ

26. Модемы спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки.

27. Исследование кодирования источника дискретных сообщений методами Шеннона-Фано.

28. Исследование алгоритмов Лемпеля - Зива. Фрактальные методы кодирования изображений.

29. Вейвлет преобразования сигналов и изображений.

30. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона

31. Циклические избыточные коды CRC (Cyclic redundancycheck). Сверточные коды.

32. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби. Турбокодирование.

33. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов.

34. Характеристики помехоустойчивости сверточных турбокодов.

35. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования на базе MATLAB.

36. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции(TCM) и их анализ с использованием MATLAB. Исследование сигнально-кодовой конструкции на базе

системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO.

37. Теория классических шифров. Основные характеристики открытого текста.

38. Классификация шифров. Классификация шифров замены. Шифры перестановки.

39. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шифр Хилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистрсдвига с линейной обратной связью.

40. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров.

41. Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки

42. появления асимметричных криптосистем. Обобщенная схема асимметричной крипосистемы.

43. Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).

44. Сети шифрованной связи. Организация сетей конфиденциальной связи. Основные термины и понятия. Угрозы сетям. Протоколы распределения ключей и их характеристики. Компрометация абонентов сети; способы построения протоколов распределения ключей, обеспечивающих защиту от компрометации. Криптографические протоколы, протоколы распределения ключей, парольные системы разграничения доступа. Способы восстановления шифрованной связи после компрометации. Подходы к локализации негативных последствий компрометации. Сети связи с открытым распределением ключей.

45. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем. PGP кодирование и шифрование с открытым ключом. Общие сведения.

46. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP.

47. Сжатие данных. Сеть доверия. Сертификаты. Open PGP. Поглощение Network Associates.

48. Современное состояние. Правовые аспекты использования в России. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP.

49. Дезактивация – временное отключение неиспользуемого ключа или ключевой пары. Отпечаток ключа. Имплицитное доверие – полное доверие зарезервировано для ключевых пар, расположенных на локальном ключе. Безопасность сети передачи данных на транспортном уровне SSL и TLS. Протокол SSL. Принцип работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол. Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный ДиффиХеллман (Diffie-Hellman), кратковременный Диффи-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмышифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный

секретный код. Сеансы и соединение. Протокол TLS. Генерация криптографической секретности. Функция расширения данных. Псевдослучайная функция TLS.

7.3.2 Промежуточная аттестация

Вопросы к экзамену

1. Поясните термин «Свёрточный код». Важнейшие отличия сверточных кодов от блоковых? Что представляет собой свёрточный кодер?	ПК-7
2. Дайте определения (приведите формулы) показателей информационной, энергетической и частотной эффективности ТКС	ПК-7
3. Средства обеспечения безопасности GSM сетей. Опишите принцип работы семейства алгоритмов A5, используемых для шифрования трафика в сетях GSM.	ПК-7
4. Пропускная способность канала связи. Кодирование источника	ПК-7
5. Как судят о совершенстве методов передачи цифровой информации по степени приближения реальных значений эффективности к предельным значениям?	ПК-7
6. Для чего используются Ассиметричные криптосистемы?	ПК-7
7. Как определяется энергетический выигрыш от применения помехоустойчивого кодирования?	ПК-7
8. Перечислите виды многоуровневой фазовой модуляции	ПК-7
9. По каким схемам производится аппаратная реализация Поточных шифров	ПК-7
10. Коды Боуза-Чоудхури-Хоквенгема (БЧХ).	ПК-7
11. Дайте определение предельной эффективности телекоммуникационных систем и границы К. Шеннона.	ПК-7
12. Сравните основные характеристики шифров DES и AES. Перечислите основные характеристики DES и AES.	ПК-7
13. Энергетическая и спектральная эффективность цифровой радиосвязи.	ПК-7
14. Как называются, как производятся и чем отличаются Многоуровневые модуляции MPSK, M-QAM?	ПК-7
15. Опишите услуги 5G: сверхширокополосная мобильная связь (enhanced Mobile Broadband, eMBB). Опишите услуги 5G: сверхнадежная межмашинная связь с низкими задержками (Ultra-Reliable Low Latency Communication, URLLC). Опишите услуги 5G: массовая межмашинная связь (Massive Machine-Type Communications, mMTC).	ПК-7
16. Как называются, как производятся и чем отличаются Многоуровневые модуляции MFSK, MSK и GMSK?	ПК-7
17. Какая модуляция обеспечивает большую помехоустойчивось систем передачи информации M-PSK или M-QPSK?	ПК-7
18. Какие скорости передачи информации достигались при тестировании 5G в мире? Какие задержки достигались при тестировании 5G?	ПК-7
19. Коды Рида-Соломона в каналах с независимыми ошибками.	ПК-7
20. Дайте определение и сравните характеристики модуляций 16-APSK и 32-APSK.	ПК-7

21. Перечислите характеристики сетей мобильной связи 1G, 2G, 3G, 4G: (зоны обслуживания, количество каналов, Скорости передачи, Дальность действия, Диапазоны частот, Ширину полосы).	ПК-7
22. Перечислите методы кодирования источника без потерь.	ПК-7
23. Что такое CRC кодирование? Перечислите все полиномы CRC кодирования и запишите полиномы для CRC-1 и CKC-30.	ПК-7
24. Приведите основные технические характеристики системы мобильной связи WiMAX. Как работает скремблер WiMAX?	ПК-7
25. Кодирование/декодирование в беспроводных системах цифрового вещания и связи. Коды LDPC	ПК-7
26. Как производится кодирование и декодирование Хэмминга?	ПК-7
27. Приведите основные технические характеристики системы мобильной связи IEEE 802.11ax (WiFi6). Какая максимальная скорость передачи WiFi6?	ПК-7
28. Модемы сотовой системы связи (FSK, MSK, GFSK, GMSK).	ПК-7
29. Перечислите методы помехоустойчивого кодирования. Дайте их характеристику.	ПК-7
30. Приведите основные технические характеристики системы мобильной связи IEEE 802.11n. Что такое DSSS и FHSS?	ПК-7
31. Что такое Низкоплотностные коды LDPC? Опишите методы LDPC кодирования.	ПК-7
32. Перечислите виды многоуровневой фазовой модуляции.	ПК-7
33. Сравните основные характеристики шифров DES и AES. Перечислите основные характеристики DES и AES. Опишите работу Алгоритма шифрования DES. Опишите работу Алгоритма шифрования AES.	ПК-7
34. Чем отличаются методы мягкого и жесткого сверточного декодирования Витерби?	ПК-7
35. Опишите криптографические протоколы SSL и TLS. Опишите криптографические протоколы IP SEC. Что включает в себя протокол IP SEC? Перечислите уровни моделей ISO/OSI и уровни TCP/IP.	ПК-7
36. Что такое Джиттер? Опишите методы его измерения. Как Джиттер используется для оценки помехоустойчивости систем связи.	ПК-7
37. Дайте определение и сравните характеристики модуляций 16-APSK и 32-APSK.	ПК-7
38. Приведите основные технические характеристики системы мобильной связи IEEE 802.11ax (WiFi 6). Какая максимальная скорость передачи WiFi6?	ПК-7
39. Перечислите методы помехоустойчивого кодирования.	ПК-7
40. Опишите методы кодирования с потерями - фрактальные и вейвлет.	ПК-7

Типовой вариант билета

по дисциплине **«Кодирование и шифрование информации в радиоэлектронных системах»**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Дисциплина «Кодирование и шифрование информации в радиоэлектронных системах»

Курс 5, семестр 9

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ

1. Сравните основные характеристики шифров DES и AES. Перечислите основные характеристики DES и AES. Опишите работу Алгоритма шифрования DES. Опишите работу Алгоритма шифрования AES.
2. Перечислите виды многоуровневой фазовой модуляции.
3. В гауссовском канале энергопотенциал составляет 60 дБ×Гц. Какова должна быть минимальная полоса сигнала, теоретически гарантирующая возможность передавать данные по каналу со скоростью 1,5 Мбит/сек?