МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **11.04.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль) / специализация: **Радиоэлектронные системы передачи информации**
Форма обучения: **очная**
Факультет: **Радиотехнический факультет (РТФ)**
Кафедра: **Кафедра радиотехнических систем (РТС)**
Курс: **1**
Семестр: **2**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	2 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Практические занятия	18	18	часов
Лабораторные занятия	16	16	часов
Самостоятельная работа	128	128	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	216	216	часов
	6	6	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	2

Томск

1. Общие положения

1.1. Цели дисциплины

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

1.2. Задачи дисциплины

1. Задачей 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.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль направленности (профиля) (major).
Индекс дисциплины: Б1.В.01.ДВ.02.02.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		

ПКР-1. Способен использовать современные достижения науки и передовые инфокоммуникационные технологии, методы проведения теоретических и экспериментальных исследований в научно-исследовательских работах в области ИКТиСС, ставить задачи исследования, выбирать методы экспериментальной работы с целью совершенствования и созданию новых перспективных инфокоммуникационных систем	ПКР-1.1. Знает технические характеристики и экономические показатели отечественных и зарубежных разработок в области радиоэлектронной техники, действующие нормативные требования и государственные стандарты.	Знает технические характеристики и экономические показатели отечественных и зарубежных разработок в области кодирования и шифрование информации в системах связи, действующие нормативные требования и государственные стандарты
	ПКР-1.2. Умеет осуществлять патентный поиск, проводить сбор, анализ и систематизацию научно-исследовательской информации, формулировать цели и задачи научно-исследовательских работ в области создания и проектирования радиоэлектронных устройств и систем.	Умеет осуществлять патентный поиск, проводить сбор, анализ и систематизацию научно-исследовательской информации, формулировать цели и задачи научно-исследовательских работ в области кодирования и шифрование информации в системах связи
	ПКР-1.3. Умеет разрабатывать техническое задание, требования и условия на разработку и проектирование радиоэлектронных устройств и систем.	Умеет разрабатывать техническое задание, требования и условия на разработку и проектирование радиоэлектронных устройств и систем кодирования и шифрование информации в системах связи
	ПКР-1.4. Владеет навыками разработки и анализа вариантов создания радиоэлектронного устройства или радиоэлектронной системы на основе синтеза накопленного опыта, изучения литературы и собственной интуиции; прогноза последствий, поиска компромиссных решений в условиях многокритериальности.	Владеет навыками разработки и анализа вариантов создания радиоэлектронного устройства или радиоэлектронной систем кодирования и шифрование информации в системах связи

ПКР-2. Способен самостоятельно выполнять экспериментальные исследования для решения научно-исследовательских и производственных задач с использованием современной аппаратуры и методов исследования	ПКР-2.1. Знает методики сбора, анализа и обработки статистической информации инфокоммуникационных систем.	Знает методики сбора, анализа и обработки статистической информации систем кодирования и шифрование информации в системах связи.
	ПКР-2.2. Умеет проводить исследования характеристик телекоммуникационного оборудования и оценки качества предоставляемых услуг.	Умеет проводить исследования характеристик оборудования и оценки качества предоставляемых услуг кодирования и шифрование информации в системах связи
	ПКР-2.3. Владеет навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников.	Владеет навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников в области кодирования и шифрование информации в системах связи
	ПКР-2.4. Владеет навыками проведения экспериментальных работ по проверке достижимости технических характеристик радиоэлектронной аппаратуры.	Владеет навыками проведения экспериментальных работ в области кодирования и шифрование информации в системах связи

ПКР-3. Способен самостоятельно собирать и анализировать исходные данные с целью формированию плана развития, выработке и внедрению научно обоснованных решений по оптимизации сети связи	ПКР-3.1. Знает методы и подходы к формированию планов развития сети.	Знает методы и подходы к формированию планов развития методов кодирования и шифрование информации в системах связи
	ПКР-3.2. Знает рынок услуг связи, средства сбора и анализа исходных данных для развития и оптимизации сети связи.	Знает рынок услуг связи, средства сбора и анализа исходных данных для развития и оптимизации сети связи, использующих кодирование и шифрование информации
	ПКР-3.3. Умеет составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи.	Умеет составлять технико-экономические обоснования планов развития сети, применять современные методы исследований с целью создания перспективных сетей связи, использующих кодирования и шифрование информации
	ПКР-3.4. Умеет осуществлять поиск, анализировать и оценивать информацию, необходимую для эффективного выполнения задачи планирования, анализировать перспективы технического развития и новые технологии.	Умеет осуществлять поиск, анализировать и оценивать информацию, необходимую для эффективного выполнения задачи планирования, анализировать перспективы технического развития и новые технологии в области кодирования и шифрование информации в системах связи
	ПКР-3.5. Владеет навыками определения стратегии жизненного цикла услуг связи, выбора технологий для предоставления различных услуг связи, расчета экономической эффективности принимаемых технических решений.	Владеет навыками определения стратегии жизненного цикла услуг кодирования и шифрование информации, расчета экономической эффективности принимаемых технических решений.
	ПКР-3.6. Владеет навыками анализа качества работы каналов и технических средств связи.	Владеет навыками анализа качества работы каналов и технических средств кодирования и шифрование информации в системах связи

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	52	52

Лекционные занятия	18	18
Практические занятия	18	18
Лабораторные занятия	16	16
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	128	128
Подготовка к лабораторной работе, написание отчета	26	26
Написание отчета по лабораторной работе	26	26
Написание отчета по практическому занятию (семинару)	36	36
Выполнение практического задания	20	20
Подготовка к тестированию	20	20
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	216	216
Общая трудоемкость (в з.е.)	6	6

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр						
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	2	2	4	24	32	ПКР-1, ПКР-3, ПКР-2
2 Пропускная способность канала связи. Кодирование источника	2	2	-	8	12	ПКР-1, ПКР-3, ПКР-2
3 Помехоустойчивое кодирование в телекоммуникационных системах	2	2	4	24	32	ПКР-1, ПКР-3, ПКР-2
4 Сигнально-кодовые конструкции в телекоммуникационных системах	2	2	4	20	28	ПКР-1, ПКР-3, ПКР-2
5 Классические шифры	2	2	-	8	12	ПКР-1, ПКР-3, ПКР-2
6 Шифрование с секретным ключом	2	2	4	20	28	ПКР-1, ПКР-3, ПКР-2
7 Шифрование с открытым ключом	2	2	-	8	12	ПКР-1, ПКР-3, ПКР-2
8 Криптографические протоколы в сетях передачи данных	2	2	-	8	12	ПКР-1, ПКР-3, ПКР-2
9 Шифрование в современных системах связи	2	2	-	8	12	ПКР-1, ПКР-3, ПКР-2
Итого за семестр	18	18	16	128	180	
Итого	18	18	16	128	180	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
2 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSK, GMSK и численный анализ вероятно сти символьной ошибки. Модемы спутниковых систем связи M-QAM, M-PSK, 16-APSK, 32-APSK, и численный анализ вероятности символьной ошибки.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
2 Пропускная способность канала связи. Кодирование источника	Пропускная способность канала связи. Объем сигнала и емкость канала связи, условия их согласования. Кодирования источника. Методы эффективного кодирования. Фрактальное кодирование изображений. Вейвлет-преобразования сигналов и изображений.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
3 Помехоустойчивое кодирование в телекоммуникационных системах	Коды Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона. Циклические избыточные коды CRC (Cyclic redundancycheck). Сверточные коды. Декодирование сверточных кодов по методу Витерби. Турбокодирование. Сверточные турбокоды. Декодирование турбокодов. Характеристики по мехоустойчивости сверточных турбокодов. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Каскадных кодов.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
4 Сигнально-кодовые конструкции в телекоммуникационных системах	Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (ТСМ) и их анализ. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексировани ем и пространственно-временным кодиро ванием OFDM - MIMO.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
5 Классические шифры	Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифров замены. Шифры перестановки. Шифры простой замены. Система шифрования Це заря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шиф р Хилла. 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	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
6 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шиф ров. Стандарт шифрования данных ГОСТ. Американский стандарт шифро вания данных DES. Блочный криптоалгоритм стандарт AES. Методы оценки качества алго ритмов 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. Поточные режимы блочных шифров. Строительные блоки по точных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обрат ной связью по переносу. Поточный шифр HC-128. 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 в поточном режиме. Блочный шифр AES в поточном	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
7 Шифрование с открытым ключом	Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипосистемы. 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 крипто систем с открытым ключом. Алгоритм Ра бина-Миллера (Rabin-Miller).	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	

8 Криптографические протоколы в сетях передачи данных	Сети шифрованной связи. Организация се тей 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. Подходы к снижению вероятности повторного использования. Современные тенденции развития- средств и методов криптографической защиты информации. Программно-аппарат ная реализация современных криптографических средств. Криптографические про токолы: 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. Сов местимость. Защищённость. Механизм ра боты PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных. Сеть доверия. Сертификаты. Open PGP. Поглощение NetworkAssociates. 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. Дезакти вация – временное отключениене используемого ключа или ключевой пары. Отпечаток ключа. Имплицитное доверие – пол ное 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 Диффи-Хеллман (Diffie- Hellman), кратковременный Диффи-Хелл ман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования.Алгоритмы хэширования. Ге нерирование криптографических парамет ров. Главный секретный код. Сеансы и соединение. Протокол TLS. Генерация крип тографической секретности. Функция расширения данных. Псевдослучайная функция TLS. Главный секретный код TLS. Материал для ключей TLS. Аварийный протокол в TLS. Протокол установления соединения TLS. Безопасность сети ПД на сетевом уровне IPsec. IPsec являет сянеотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уров ня специфицирована в документе Security Architecture for theInternet Protocol. Разме щение и функционирование IPsec. Транспортный режим работы. Туннельный режим работы. Контексты безопасности и управление ключами. Протокольные контексты и политика безопасности. Аутентификационный заголовок. Безопасное сокрытие существенных данных. Про токол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций. распре деления 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. Проблемы синхронизации в сетях.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
9 Шифрование в современных системах связи	Безопасность GSM сетей. Алгоритм шифрования A5/1. Системные сообщения GSM. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы и стандарты защиты беспро водных сетей LTE. Алгоритм аутентифика ции и генерации ключа. Слои безопасности. Иерархия ключей в E-UTRAN. Генери рование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в E-UTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование технологии шифрования в сетях LTE.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
Итого за семестр		18	
Итого		18	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.
Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
2 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Модемы сотовой связи FSK, MSKGMSK и численный анализ вероятности символьной ошибки. Модемы спутниковых систем связи M-QAM, M-PSK и численный ана- лиз вероятности символьной ошибки	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
2 Пропускная способность канала связи. Кодирование источника	Исследование кодирования источника дис кретных сообщений методами Шеннона- Фано. Исследование алгоритмов Лемпеля- Зива. Фрактальные методы кодирования и зображений. Вейвлет преобразования сигналов и изображений.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
3 Помехоустойчивое кодирование в телекоммуникационных системах	Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо. Циклические избыточ ные коды CRC (Cyclic redundancycheck). Сверточные коды. Деко- дирование сверточных кодов. Декодирование сверточныхкодов по методу Витерби.Турбокоди рование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточ ные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов. Исследование турбокодов. Низкоплотностные коды. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования. Исследование каскадных кодов.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
4 Сигнально-кодовые конструкции в телекоммуникационных системах	Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (TCM). Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	

5 Классические шифры	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. 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. Регистр сдвига с линейной обратной связью.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
6 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифро вания данных DES. Блочный криптоалгоритм RIJNDAEL и стандарт AES. Поточные системы шифрования. Поточные режимы блочных шифров. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линей ной обратной связью. Регистры сдвига с обратной связью по переносу. Российский блочный шифр ГОСТ 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 шифов.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	

7 Шифрование с открытым ключом	Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипо системы. 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).	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
8 Криптографические протоколы в сетях передачи данных	Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных. Сеть доверия. Сертификаты. Open PGP. Электронная цифровая подпись (ЭЦП). 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. Безопасность сети ПД на сетевом уровне IPsec. IPsec является неотъемлемой частью IPv6 Интернет протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for theInternet Protocol. Размещение и функционирование IPsec.Транспортный режим работы.Туннельный режим работы.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	

9 Шифрование в современных системах связи	Безопасность GSM сетей. Алгоритм шифрования A5/1. Криптографическая защита беспроводных сетей стандартов LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности. Иерархия ключей в E-UTRAN. Генерирование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в E-UTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование алгоритмовзащиты LTE.	2	ПКР-1, ПКР-3, ПКР-2
	Итого	2	
	Итого за семестр	18	
	Итого	18	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
2 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSK, GMSK и численный анализ вероятности символьной ошибки . Модемы спутниковых систем связи M-QAM, M-PSK, 16-APSK, 16-APSK и численный анализ вероятности символьной ошибки.	4	ПКР-1, ПКР-3, ПКР-2
	Итого	4	
3 Помехоустойчивое кодирование в телекоммуникационных системах	Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо. Циклические избыточныекоды CRC (Cyclic redundancycheck). Сверточные коды. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби. Турбокодирование. Сверточные турбокоды. Декодирование турбокодов .Характеристики помехоустойчивости сверточных турбокодов. Низкоплотностные коды. Алгоритмы декодирования низкоплотных кодов. Исследование каскадных кодов.	4	ПКР-1, ПКР-3, ПКР-2
	Итого	4	

4 Сигнально-кодовые конструкции в телекоммуникационных системах	Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (TCM) и их анализ. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексировани ем и пространственно-временным кодиро ванием OFDM - MIMO.	4	ПКР-1, ПКР-3, ПКР-2
	Итого	4	
6 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шиф ров. 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.	4	ПКР-1, ПКР-3, ПКР-2
	Итого	4	
	Итого за семестр	16	
	Итого	16	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
2 семестр				

1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Подготовка к лабораторной работе, написание отчета	8	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа
	Написание отчета по лабораторной работе	8	ПКР-1, ПКР-3, ПКР-2	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	24		
2 Пропускная способность канала связи. Кодирование источника	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	8		
3 Помехоустойчивое кодирование в телекоммуникационных системах	Подготовка к лабораторной работе, написание отчета	6	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа
	Написание отчета по лабораторной работе	6	ПКР-1, ПКР-3, ПКР-2	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	4	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	4	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	24		

4 Сигнально-кодовые конструкции в телекоммуникационных системах	Подготовка к лабораторной работе, написание отчета	6	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа
	Написание отчета по лабораторной работе	6	ПКР-1, ПКР-3, ПКР-2	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	20		
5 Классические шифры	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	8		
6 Шифрование с секретным ключом	Подготовка к лабораторной работе, написание отчета	6	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа
	Написание отчета по лабораторной работе	6	ПКР-1, ПКР-3, ПКР-2	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	20		

7 Шифрование с открытым ключом	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	8		
8 Криптографические протоколы в сетях передачи данных	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	8		
9 Шифрование в современных системах связи	Написание отчета по практическому занятию (семинару)	4	ПКР-1, ПКР-3, ПКР-2	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПКР-1, ПКР-3, ПКР-2	Практическое задание
	Подготовка к тестированию	2	ПКР-1, ПКР-3, ПКР-2	Тестирование
	Итого	8		
Итого за семестр		128		
	Подготовка и сдача экзамена	36		Экзамен
Итого		164		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лек. зан.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПКР-1	+	+	+	+	Лабораторная работа, Практическое задание, Тестирование, Экзамен, Отчет по лабораторной работе, Отчет по практическому занятию (семинару)

ПКР-2	+	+	+	+	Лабораторная работа, Практическое задание, Тестирование, Экзамен, Отчет по лабораторной работе, Отчет по практическому занятию (семинару)
ПКР-3	+	+	+	+	Лабораторная работа, Практическое задание, Тестирование, Экзамен, Отчет по лабораторной работе, Отчет по практическому занятию (семинару)

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
2 семестр				
Лабораторная работа	8	10	10	28
Практическое задание	4	4	4	12
Тестирование	2	2	2	6
Отчет по лабораторной работе	4	4	4	12
Отчет по практическому занятию (семинару)	4	4	4	12
Экзамен				30
Итого максимум за период	22	24	24	100
Нарастающим итогом	22	46	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)

3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Голиков, А. М. Кодирование и шифрование информации в радиоэлектронных системах передачи информации. Часть 1. Кодирование: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу [Электронный ресурс] / А. М. Голиков. — 2-е изд. перераб. и доп. — Томск: ТУСУР, 2018. — 333 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8844.

7.2. Дополнительная литература

1. Голиков, А. М. Кодирование и шифрование информации в радиоэлектронных системах передачи информации. Часть 2. Шифрование: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу. — [Электронный ресурс] / А. М. Голиков. — Изд. перераб. и доп. — Томск: ТУСУР, 2018. — 377 с. — [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8846.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Голиков, А. М. Кодирование и шифрование информации в радиоэлектронных системах передачи информации. Часть 1. Кодирование: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу [Электронный ресурс] / А. М. Голиков. — 2-е изд. перераб. и доп. — Томск: ТУСУР, 2018. — 333 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8844.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие

тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория радиоэлектронных систем передачи информации: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ); 634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Free Pascal;
- Free Pascal Lazarus (версия 1.6);
- GIMP;
- Google Chrome;
- Microsoft Windows Server 2008;
- Microsoft Windows XP;
- Mozilla Firefox;
- OpenOffice;
- Opera;
- Opera Developer;
- PTC Mathcad 13, 14;
- Scilab;

8.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория радиоэлектронных систем передачи информации: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ); 634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Free Pascal;
- Free Pascal Lazarus (версия 1.6);
- GIMP;
- Google Chrome;
- Microsoft Windows Server 2008;
- Microsoft Windows XP;
- Mozilla Firefox;
- OpenOffice;
- Opera;

- Opera Developer;
- PTC Mathcad 13, 14;
- Scilab;

8.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.5. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)

1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Пропускная способность канала связи. Кодирование источника	ПКР-1, ПКР-3, ПКР-2	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Помехоустойчивое кодирование в телекоммуникационных системах	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

4 Сигнально-кодовые конструкции в телекоммуникационных системах	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Классические шифры	ПКР-1, ПКР-3, ПКР-2	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
6 Шифрование с секретным ключом	ПКР-1, ПКР-3, ПКР-2	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

7 Шифрование с открытым ключом	ПКР-1, ПКР-3, ПКР-2	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
8 Криптографические протоколы в сетях передачи данных	ПКР-1, ПКР-3, ПКР-2	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
9 Шифрование в современных системах связи	ПКР-1, ПКР-3, ПКР-2	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков

4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какой из фазовых видов модуляции обеспечивает наибольшую помехоустойчивость: а) BPSK; б) QPSK; в) 8-PSK; г) 16-QAM.
2. Какой из видов частотной модуляции имеет минимальную ширину спектра: а) FSK; б) MSK; в) GMSK; г) M-FSK.
3. Какой из методов кодирования источника производит кодирование с потерями: а) Коды Шеннона-Фано; б) Алгоритм Лемпеля – Зива; в) Вейвлет преобразование; г) Коды Хаффмана.
4. Какой код является блоковым: -а) Код Хемминга; б) БЧХ (Боуза-Чоудхури-Хоквенгема); в) Рида- Соломона; - Файра; г)Лемпеля – Зива.
5. Какие из кодов и сигнально-кодовых конструкций наиболее приближены к верхней границе Шеннона: а) АФМ-16-СК; б) БЧХ; в) ФМ-2; г) АМ-2.
6. Какова длина ключа шифра DES: а) 48; б) 56; в) 128; г) 256.
7. Какова длина ключа шифра AES: а) 128, 192, 256; -б)32, 48, 56; в) 48, 56, 128; г) 56, 128, 256.
8. Отечественный стандарт блочного шифрования ГОСТ может работать в следующих

режимах. Какой из них работает как синхронный поточный шифр: а) Режим простой замены; б) Режим гаммирования; в) Режим гаммирования с обратной связью; г) Режим выработки имитовставки.

9. Чему равна величиной предельной энергетической эффективности (предел Шеннона): а) 1,59 Дб; б) 1,69 Дб; в) 2,56 Дб; г) 3,22 Дб.
10. Системы мобильной связи стандарта IEEE 802.15.1(Bluetooth). Какой метод расширения спектра используется в стандарте IEEE 802.11 (WIFI): а) CDMA: б) DSSS; в) FHSS; г) Коды Баркера.

9.1.2. Перечень экзаменационных вопросов

1. Поясните термин «Свёрточный код». Важнейшие отличия сверточных кодов от блоковых? Что представляет собой свёрточный кодер?
2. Дайте определения (приведите формулы) показателей информационной, энергетической и частотной эффективности ТКС
3. Средства обеспечения безопасности GSM сетей. Опишите принцип работы семейства алгоритмов А5, используемых для шифрования трафика в сетях GSM.
4. Пропускная способность канала связи. Кодирование источника
5. Как судят о совершенстве методов передачи цифровой информации по степени приближения реальных значений эффективности к предельным значениям?
6. Для чего используются Ассиметричные криптосистемы?
7. Как определяется энергетический выигрыш от применения помехоустойчивого кодирования?
8. Перечислите виды многоуровневой фазовой модуляции
9. По каким схемам производится аппаратная реализация Поточных шифров
10. Коды Боуза-Чоудхури-Хоквенгема (БЧХ).
11. Дайте определение предельной эффективности телекоммуникационных систем и границы К. Шеннона.
12. Сравните основные характеристики шифров DES и AES. Перечислите основные характеристики DES и AES.
13. Энергетическая и спектральная эффективность цифровой радиосвязи.
14. Как называются, как производятся и чем отличаются Многоуровневые модуляции M-PSK, M-QAM?
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).
16. Как называются, как производятся и чем отличаются Многоуровневые модуляции M-FSK, MSK и GMSK?
17. Какая модуляция обеспечивает большую помехоустойчивось систем передачи информации M-PSK или M-QPSK?
18. Какие скорости передачи информации достигались при тестировании 5G в мире? Какие задержки достигались при тестировании 5G?
19. Коды Рида-Соломона в каналах с независимыми ошибками.
20. Дайте определение и сравните характеристики модуляций 16-APSK и 32-APSK.
21. Перечислите характеристики сетей мобильной связи 1G, 2G, 3G, 4G: (зоны обслуживания, количество каналов, Скорости передачи, Дальность действия, Диапазоны частот, Ширину полосы).
22. Перечислите методы кодирования источника без потерь.
23. Что такое CRC кодирование? Перечислите все полиномы CRC кодирования и запишите полиномы для CRC-1 и СКС-30.
24. Приведите основные технические характеристики системы мобильной связи WiMAX. Как работает скремблер WiMAX?
25. Кодирование/декодирование в беспроводных системах цифрового вещания и связи. Коды LDPC
26. Как производится кодирование и декодирование Хэмминга?
27. Приведите основные технические характеристики системы мобильной связи IEEE 802.11ax (WiFi6). Какая максимальная скорость передачи WiFi6?

28. Модемы сотовой системы связи (FSK, MSK, GFSK, GMSK).
29. Перечислите методы помехоустойчивого кодирования. Дайте их характеристику.
30. Приведите основные технические характеристики системы мобильной связи IEEE 802.11n. Что такое DSSS и FHSS?
31. Что такое Низкоплотностные коды LDPC? Опишите методы LDPC кодирования.
32. Перечислите виды многоуровневой фазовой модуляции.
33. Сравните основные характеристики шифров DES и AES. Перечислите основные характеристики DES и AES. Опишите работу Алгоритма шифрования DES. Опишите работу Алгоритма шифрования AES.
34. Чем отличаются методы мягкого и жесткого сверточного декодирования Витерби?
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.
36. Что такое Джиттер? Опишите методы его измерения. Как Джиттер используется для оценки помехоустойчивости систем связи.
37. Дайте определение и сравните характеристики модуляций 16-APSK и 32-APSK.
38. Приведите основные технические характеристики системы мобильной связи IEEE 802.11ax (WiFi 6). Какая максимальная скорость передачи WiFi6?
39. Перечислите методы помехоустойчивого кодирования.
40. Опишите методы кодирования с потерями - фрактальные и вейвлет.

9.1.3. Темы лабораторных работ

1. Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSK, GMSK и численный анализ вероятности символьной ошибки . Модемы спутниковых систем связи M-QAM, M-PSK, 16-APSK, 16-APSK и численный анализ вероятности символьной ошибки.
2. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо. Циклические избыточныекоды CRC (Cyclic redundancycheck). Сверточные коды. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби. Турбокодирование. Сверточные турбокоды. Декодирование турбокодов .Характеристики помехоустойчивости сверточных турбокодов. Низкоплотностные коды. Алгоритмы декодирования низкоплотных кодов. Исследование каскадных кодов.
3. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (TCM) и их анализ. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексировани ем и пространственно-временным кодиро ванием OFDM - MIMO.
4. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шиф ров. 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.

9.1.4. Темы практических заданий

Модемы сотовой связи FSK, MSKGMSK и численный анализ вероятности символьной ошибки. Модемы спутниковых систем связи M-QAM, M-PSK и численный ана- лиз вероятности символьной ошибки

1. Исследование кодирования источника дис кретных сообщений методами Шеннона- Фано. Исследование алгоритмов Лемпеля- Зива. Фрактальные методы кодирования и зображений. Вейвлет преобразования сигналов и изображений.
2. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо. Циклические избыточ ные коды CRC (Cyclic redundancycheck). Сверточные коды. Декодирование сверточных кодов. Декодирование сверточныхкодов по методу Витерби.Турбокоди рование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточ ные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов. Исследование турбокодов. Низкоплотностные коды. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования. Исследование каскадных кодов.

3. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (ТСМ). Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO.
4. 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. 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. Регистр сдвига с линейной обратной связью.
5. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифро вания данных DES. Блочный криптоалгоритм RIJNDAEL и стандарт AES. Поточные системы шифрования. Поточные режимы блочных шифров. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линей ной обратной связью. Регистры сдвига с обратной связью по переносу. Российский блочный шифр ГОСТ 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 шифов.
6. Теория шифров с открытым ключом. Асимметричные криптосистемы. Пред- посылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипо системы. 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).
7. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных. Сеть доверия. Сертификаты. Open PGP. Электронная цифровая подпись (ЭЦП). 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. Безопасность сети ПД на сетевом уровне IPsec. IPsec является неотъемлемой частью IPv6 Интернет протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for theInternet Protocol. Размещение и функционирование IPsec.Транспортный режим работы.Туннельный режим работы.
8. Безопасность GSM сетей. Алгоритм шифрования A5/1. Криптографическая защита беспроводных сетей стандартов LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности. Иерархия ключей в E-UTRAN. Генерирование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в E-UTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование алгоритмовзащиты LTE.

9.1.5. Темы практических занятий

1. Модемы сотовой связи FSK, MSKGMSK и численный анализ вероятности символьной ошибки. Модемы спутниковых систем связи M-QAM, M-PSK и численный ана- лиз вероятности символьной ошибки
2. Исследование кодирования источника дис кретных сообщений методами Шеннона- Фано. Исследование алгоритмов Лемпеля- Зива. Фрактальные методы кодирования и зображений. Вейвлет преобразования сигналов и изображений.
3. Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломо.

Циклические избыточ ные коды CRC (Cyclic redundancycheck). Сверточные коды. Декодирование сверточных кодов. Декодирование сверточныхкодов по методу Витерби.Турбокоди рование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточ ные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов. Исследование турбокодов. Низкоплотностные коды. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования. Исследование каскадных кодов.

4. Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (ТСМ). Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO.
5. 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. 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. Регистр сдвига с линейной обратной связью.
6. Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифро вания данных DES. Блочный криптоалгоритм RIJNDAEL и стандарт AES. Поточные системы шифрования. Поточные режимы блочных шифров. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линей ной обратной связью. Регистры сдвига с обратной связью по переносу. Российский блочный шифр ГОСТ 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 шифов.
7. Теория шифров с открытым ключом. Асимметричные криптосистемы. Пред- посылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипо системы. 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).
8. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных. Сеть доверия. Сертификаты. Open PGP. Электронная цифровая подпись (ЭЦП). 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. Безопасность сети ПД на сетевом уровне IPsec. IPsec является неотъемлемой частью IPv6 Интернет протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for theInternet Protocol. Размещение и функционирование IPsec.Транспортный режим работы.Туннельный режим работы.
9. Безопасность GSM сетей. Алгоритм шифрования A5/1. Криптографическая защита беспроводных сетей стандартов LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности. Иерархия ключей в E-UTRAN. Генерирование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в E-UTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование алгоритмовзащиты LTE.

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;
– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры РТС
протокол № 4 от «19» 11 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. РТС	А.А. Мещеряков	Согласовано, 5bbb058c-a625-4513-8e7f-25eb16694704
Заведующий обеспечивающей каф. РТС	А.А. Мещеряков	Согласовано, 5bbb058c-a625-4513-8e7f-25eb16694704
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. РТС	В.А. Громов	Согласовано, bbaa5b2b-4c38-484f-a5bb-85f9ddafe277
Старший преподаватель, каф. РТС	Д.О. Ноздреватых	Согласовано, bd0039b0-9c48-4859-9803-60c9ddba7116

РАЗРАБОТАНО:

Доцент, каф. РТС	А.М. Голиков	Разработано, d76b3893-b3a9-44a5-84f8-e53e691ec9d0