МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Кодирование и шифрование информации в радиоэлектронных системах передачи информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль): **Радиоэлектронные системы передачи информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РТС, Кафедра радиотехнических систем**
Курс: **4, 5**
Семестр: **8, 9**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	16	16	32	часов
2	Практические занятия	32	32	64	часов
3	Лабораторные работы	16	16	32	часов
4	Всего аудиторных занятий	64	64	128	часов
5	Самостоятельная работа	44	44	88	часов
6	Всего (без экзамена)	108	108	216	часов
7	Подготовка и сдача экзамена	36	36	72	часов
8	Общая трудоемкость	144	144	288	часов
		4.0	4.0	8.0	З.Е

Экзамен: 8, 9 семестр

Томск 2017

Согласована на портале № 22777

Рассмотрена и одобрена на заседании кафедры
протокол № 3 от «29» 11 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.05.01 Радиоэлектронные системы и комплексы, утвержденного 11 августа 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент кафедры, к.т.н., ст.н.с. каф.
РТС _____ А. М. Голиков

Заведующий обеспечивающей каф.
РТС _____ С. В. Мелихов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РТС _____ С. В. Мелихов

Эксперт:

старший преподаватель кафедры
РТС кафедра РТС _____ Д. О. Ноздреватых

Согласована на портале № 22777

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Дисциплина "Кодирование и шифрование информации в системах связи" (КиШИвСС) относится к числу дисциплин специализации С3+В1.2 рабочего учебного плана для подготовки инженеров по специальности 11.05.02-Радиоэлектронные системы и комплексы (специализация Радиоэлектронные системы передачи информации). Целью преподавания дисциплины является изучение основных закономерностей передачи информации в цифровых телекоммуникационных системах.

1.2. Задачи дисциплины

– Основной задачей дисциплины является формирование у студентов компетенций, по¬зволяющих 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.

– В курсе КиШИвСС принят единый методологический подход к анализу и синтезу совре¬менных телекоммуникационных систем и устройств на основе вероятностных моделей сообщений, сигналов, помех и каналов в системах связи. Предусмотренные программой курса КиШИвСС знания являются не только базой для последующего изучения специальных дисциплин, но имеют также самостоятельное значение для формирования инженеров по специальности 11.05.02 Радиоэлектронные системы и комплексы.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Кодирование и шифрование информации в радиоэлектронных системах передачи информации» (Б1.Б.30.3) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Введение в специальность, Защита информации в радиоэлектронных системах передачи информации, Информационные технологии 2. Сетевые информационные технологии. Базы данных., Космические системы, Научно-исследовательская работа, Основы компьютерного проектирования и моделирования радиоэлектронных средств, Практика по получению профессиональных умений и опыта профессиональной деятельности, Проектирование радиосистемы (ГПО 1-6), Радиоприемные устройства систем передачи информации, Статистическая теория радиотехнических систем, Теория радиосистем передачи информации, Цифровые устройства и микропроцессоры.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Моделирование в радиоэлектронных системах передачи информации, Проектирование радиотехнических систем, Радиоэлектронные системы передачи информации, Системотехника, Тестирование и диагностика в радиоэлектронных системах передачи информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-2.4 способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;

В результате изучения дисциплины студент должен:

– **знать** знать - физические и математические модели процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем; - основные закономерности исторического процесса в науке и технике, этапы исторического развития радиотехники, место и значение радиосистем передачи информации в современном мире; - методологические основы и принципы современной науки.

– **уметь** уметь - формулировать и решать задачи, грамотно использовать математический аппарат и численные методы для анализа и синтеза радиотехнических устройств и систем; - готовить методологическое обоснование научных исследований и технических разработок в области радиосистем передачи информации.

– **владеть** владеть - математическим аппаратом для решения задач теоретической и при-

Согласована на портале № 22777

кладной радиотехники, методами исследования и моделирования систем передачи информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 8.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		8 семестр	9 семестр
Аудиторные занятия (всего)	128	64	64
Лекции	32	16	16
Практические занятия	64	32	32
Лабораторные работы	32	16	16
Самостоятельная работа (всего)	88	44	44
Выполнение расчетных работ	24	8	16
Выполнение индивидуальных заданий	4		4
Оформление отчетов по лабораторным работам	24	16	8
Проработка лекционного материала	11	5	6
Подготовка к практическим занятиям, семинарам	25	15	10
Всего (без экзамена)	216	108	108
Подготовка и сдача экзамена	72	36	36
Общая трудоемкость ч	288	144	144
Зачетные Единицы	8.0	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
8 семестр						
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	4	8	4	9	25	ПСК-2.4
2 Пропускная способность канала связи. Кодирование источника	2	6	4	7	19	ПСК-2.4
3 Помехоустойчивое кодирование в телекоммуникационных системах.	4	12	4	11	31	ПСК-2.4

Согласована на портале № 22777

4 Сигнально-кодовые конструкции в телекоммуникационных системах	4	6	4	8	22	ПСК-2.4
5 Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем (задание на самостоятельную работу)	2	0	0	9	11	ПСК-2.4
Итого за семестр	16	32	16	44	108	
9 семестр						
6 Классические шифры	2	6	4	5	17	ПСК-2.4
7 Шифрование с секретным ключом	4	8	4	14	30	ПСК-2.4
8 Шифрование с открытым ключом	4	8	4	13	29	ПСК-2.4
9 Криптографические протоколы в сетях передачи данных	4	6	2	9	21	ПСК-2.4
10 Шифрование в современных системах связи	2	4	2	3	11	ПСК-2.4
Итого за семестр	16	32	16	44	108	
Итого	32	64	32	88	216	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
8 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 вероятностисимвольной ошибки с использованием ПО LabVIEW. Модемы спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW	4	ПСК-2.4
	Итого	4	
2 Пропускная способность канала связи. Кодирование источника	Пропускная способность канала связи. Объем сигнала и емкость канала связи, условия их согласования. Исследование кодирования источника. Методы эффективного кодирования.Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.	2	ПСК-2.4
	Итого	2	
3 Помехоустойчивое кодирование в	Исследование кодов Хемминга, БЧХ	4	ПСК-2.4

Согласована на портале № 22777

телекоммуникационных системах.	(Боуза-Чоудхури-Хоквенгема), Рида-Соломона.Циклические избыточные коды CRC (Cyclic redundancy check).Сверточные коды. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби. Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием.Сверточные турбокоды. Декодирование турбокодов. Характеристикипомехоустойчивости сверточных турбокодов . Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов.Исследование каскадных кодов.		
	Итого	4	
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 мультиплексированием и пространственно-временным кодированием OFDM - MIMO.	4	ПСК-2.4
	Итого	4	
5 Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем (задание на самостоятельную работу)	Помехоустойчивое кодирование яв¬ляется эффективным способом оптимизации ТКС. На практике инженеру проектровщику ТКС приходится решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов. Решение именно такой задачи положено в основу СР.	2	ПСК-2.4
	Итого	2	
Итого за семестр		16	
9 семестр			
6 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	2	ПСК-2.4

Согласована на портале № 22777

	система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.		
	Итого	2	
7 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифрования. 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. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной 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 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.	4	ПСК-2.4
	Итого	4	
8 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	4	ПСК-2.4

Согласована на портале № 22777

	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).		
	Итого	4	
9 Криптографические протоколы в сетях передачи данных	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. 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.PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. 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, асиммет-	4	ПСК-2.4

Согласована на портале № 22777

	ричный шифр). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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 работыSSL. 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-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный секретный код.Сеансы и соединение. Протокол TLS. Генерация криптографической 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 является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for the Internet Protocol. Размещение 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. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.		
	Итого	4	

Согласована на портале № 22777

10 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 беспроводных сетей 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 технологии LTE в среде MATLAB с использованием встроенного пакета LTE System Toolbox.	2	ПСК-2.4
	Итого	2	
Итого за семестр		16	
Итого		32	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин									
	1	2	3	4	5	6	7	8	9	10
Предшествующие дисциплины										
1 Введение в специальность	+		+				+	+		+
2 Защита информации в радиоэлектронных системах передачи информации			+			+	+		+	+
3 Информационные технологии 2. Сетевые информационные технологии. Базы данных.									+	
4 Космические системы	+		+	+			+	+	+	+
5 Научно-исследовательская работа	+	+	+	+		+	+		+	+
6 Основы компьютерного проектирования и моделирования радиоэлектронных средств	+		+					+		+
7 Практика по получению профессиональных умений и опыта профессиональной деятельности	+	+		+	+	+	+	+	+	+

Согласована на портале № 22777

8 Проектирование радиосистемы (ГПО 1-6)	+	+	+	+	+	+	+	+	+	+
9 Радиоприемные устройства систем передачи информации	+		+							
10 Статистическая теория радиотехнических систем			+		+			+		
11 Теория радиосистем передачи информации	+	+	+	+	+	+	+	+	+	+
12 Цифровые устройства и микропроцессоры	+		+				+		+	+
Последующие дисциплины										
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+	+	+	+	+
2 Моделирование в радиоэлектронных системах передачи информации	+	+	+	+	+	+	+	+	+	+
3 Проектирование радиотехнических систем	+	+	+	+	+	+	+	+	+	+
4 Радиоэлектронные системы передачи информации	+	+	+	+	+	+	+	+	+	+
5 Системотехника	+	+	+	+	+		+	+	+	+
6 Тестирование и диагностика в радиоэлектронных системах передачи информации	+	+							+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий				Формы контроля
	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	

Согласована на портале № 22777

ПСК-2.4	+	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Экзамен, Конспект самоподготовки, Коллоквиум, Защита отчета, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Зачет, Выступление (доклад) на занятии, Расчетная работа, Тест, Отчет по курсовой работе, Реферат, Отчет по практическому занятию, Дифференцированный зачет

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Модемы сотовой связи FSK, MSK GMSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW. Модемы спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW.	4	ПСК-2.4
	Итого	4	
2 Пропускная способность канала связи. Кодирование источника	Исследование кодирования источника дискретных сообщений методами Шеннона-Фано. Исследование алгоритмов Лемпеля - Зива. Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.	4	ПСК-2.4
	Итого	4	
3 Помехоустойчивое кодирование в телекоммуникационных системах.	Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона на базе MATLAB.Циклические избыточные коды CRC (Cyclic redundancy check).Сверточные коды.	4	ПСК-2.4

Согласована на портале № 22777

	Декодирование сверточных кодов.Декодирование сверточных кодов по методу Витерби с использованием ПО MATLAB.Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов . Исследование турбокодов с использованием ПО MATLAB 3.6. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования на базе MATLAB и LabVIEW.Исследование каскадных кодов.		
	Итого	4	
4 Сигнально-кодовые конструкции в телекоммуникационных системах	Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (ТСМ) и их анализ с использованием MATLAB. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO с использованием NI LabVIEW.	4	ПСК-2.4
	Итого	4	
Итого за семестр		16	
9 семестр			
6 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.	4	ПСК-2.4
	Итого	4	
7 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифро-	4	ПСК-2.4

Согласована на портале № 22777

	вания. 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. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной 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 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.		
	Итого	4	
8 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 криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).	4	ПСК-2.4
	Итого	4	
9 Криптографические протоколы в	Сети шифрованной связи. Организация	2	ПСК-2.4

Согласована на портале № 22777

сетях передачи данных	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. 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.PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. 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). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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		

Согласована на портале № 22777

	данных на транспортном уровне SSL и TLS. Протокол SSL. Принцип работыSSL. 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-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный секретный код.Сеансы и соединение. Протокол TLS. Генерация криптографической 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 является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for the Internet Protocol. Размещение 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. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.		
	Итого	2	
10 Шифрование в современных системах связи	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, па-	2	ПСК-2.4

Согласована на портале № 22777

	рольные 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.PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. 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). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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 работыSSL. 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. Пред-		

	варительные объекты секретности: NULL, RSA, анонимный Диффи-Хелл-ман (Diffie-Hellman), кратковременный Диффи-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгорит-мы шифрования/дешифрования. Алго-ритмы хэширования. Генерирование криптографических параметров. Глав-ный секретный код.Сеансы и соедине-ние. Протокол TLS. Генерация крипто-графической секретности. Функция расширения данных. Псевдослучайная функция TLS. Главный секретный код TLS. Материал для ключей TLS. Ава-рийный протокол в TLS. Протокол установления соединения TLS. Без-опасность сети ПД на сетевом уровне IPsec. IPsec является неотъемлемой ча-стью IPv6 Интернет-протокола следую-щего поколения. Архитектура средств безопасности для IP-уровня специфи-цирована в документе Security Architecture for the Internet Protocol. Размещение и функционирование IPsec. Транспортный режим работы. Туннельный режим работы. Контексты безопасности и управление ключами. Протокольные контексты и политика безопасности. Аутентификационный заголовок. Безопасное сокрытие суще-ственных данных. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.		
	Итого	2	
Итого за семестр		16	
Итого		32	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Модемы сотовой связи FSK, MSK GMSK и численный анализ вероятно-сти символьной ошибки с использова-нием ПО LabVIEW. Модемы спутни-ковых систем связи M-QAM, M-PSK и численный анализ вероятности сим-	8	ПСК-2.4

Согласована на портале № 22777

	вольной ошибки с использованием ПО LabVIEW.		
	Итого	8	
2 Пропускная способность канала связи. Кодирование источника	Исследование кодирования источника дискретных сообщений методами Шеннона-Фано. Исследование алгоритмов Лемпеля - Зива. Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.	6	ПСК-2.4
	Итого	6	
3 Помехоустойчивое кодирование в телекоммуникационных системах.	Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона на базе MATLAB.Циклические избыточные коды CRC (Cyclic redundancy check).Сверточные коды. Декодирование сверточных кодов.Декодирование сверточных кодов по методу Витерби с использованием ПО MATLAB.Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов . Исследование турбокодов с использованием ПО MATLAB 3.6. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования на базе MATLAB и LabVIEW.Исследование каскадных кодов.	12	ПСК-2.4
	Итого	12	
4 Сигнально-кодовые конструкции в телекоммуникационных системах	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 с использованием NI LabVIEW.	6	ПСК-2.4
	Итого	6	
Итого за семестр		32	
9 семестр			
6 Классические шифры	Теория классических шифров. Основные характеристики открытого текста. Классификация шифров.Классифика-	6	ПСК-2.4

Согласована на портале № 22777

	ция 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.		
	Итого	6	
7 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифрования. 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. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной 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 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.	8	ПСК-2.4
	Итого	8	
8 Шифрование с открытым ключом	Теория шифров с открытым ключом. Асимметричные криптосистемы. Пред-	8	ПСК-2.4

Согласована на портале № 22777

	посылки 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 криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).		
	Итого	8	
9 Криптографические протоколы в сетях передачи данных	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. 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.PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP.	6	ПСК-2.4

Согласована на портале № 22777

	Ключи PGP. Цифровая подпись на PGP. 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). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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 работыSSL. 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-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный секретный код.Сеансы и соединение. Протокол TLS. Генерация криптографической 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 является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for the Internet Protocol. Размещение и функционирование IPsec. Транспортный режим работы. Туннельный режим работы. Контексты безопасности и управление ключами.		

Согласована на портале № 22777

	Протокольные контексты и политика безопасности. Аутентификационный заголовок. Безопасное сокрытие существенных данных. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.		
	Итого	6	
10 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 беспроводных сетей 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 технологии LTE в среде MATLAB с использованием встроенного пакета LTE System Toolbox.	4	ПСК-2.4
	Итого	4	
Итого за семестр		32	
Итого		64	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Подготовка к практическим занятиям, семинарам	4	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
2 Пропускная	Подготовка к практиче-	2	ПСК-2.4	Выступление (доклад) на

Согласована на портале № 22777

способность канала связи. Кодирование источника	ским занятиям, семинарам			занятии, Домашнее задание, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	7		
3 Помехоустойчивое кодирование в телекоммуникационных системах.	Подготовка к практическим занятиям, семинарам	6	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Зачет, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по курсовой работе, Отчет по лабораторной работе, Отчет по практическому занятию, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	11		
4 Сигнально-кодовые конструкции в телекоммуникационных системах	Подготовка к практическим занятиям, семинарам	3	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Зачет, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по курсовой работе, Отчет по лабораторной работе, Отчет по практическому занятию, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	8		
5 Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем (задание на самостоятельную работу)	Проработка лекционного материала	1	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Коллоквиум, Контрольная работа, Опрос на занятиях, Отчет по курсовой работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест
	Выполнение расчетных работ	8		
	Итого	9		
Итого за семестр		44		
	Подготовка и сдача экзамена	36		Экзамен

Согласована на портале № 22777

9 семестр				
6 Классические шифры	Подготовка к практическим занятиям, семинарам	2	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	5		
7 Шифрование с секретным ключом	Подготовка к практическим занятиям, семинарам	2	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Собеседование, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Выполнение расчетных работ	8		
	Итого	14		
8 Шифрование с открытым ключом	Подготовка к практическим занятиям, семинарам	2	ПСК-2.4	Выступление (доклад) на занятии, Дифференцированный зачет, Домашнее задание, Зачет, Защита курсовых проектов (работ), Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по курсовой работе, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Выполнение расчетных работ	8		
	Итого	13		
9 Криптографические протоколы в сетях передачи данных	Подготовка к практическим занятиям, семинарам	2	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивиду-
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		

Согласована на портале № 22777

	Выполнение индивидуальных заданий	4		альному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Реферат, Собеседование, Тест, Экзамен
	Итого	9		
10 Шифрование в современных системах связи	Подготовка к практическим занятиям, семинарам	2	ПСК-2.4	Выступление (доклад) на занятии, Домашнее задание, Защита курсовых проектов (работ), Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по курсовой работе, Отчет по практическому занятию, Реферат, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
Итого за семестр		44		
	Подготовка и сдача экзамена	36		Экзамен
Итого		160		

9.1. Темы расчетных работ

1. Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.
2. Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.
3. Атака на алгоритм шифрования RSA Посредством метода Ферма.
4. Атака на алгоритм шифрования RSA методом повторного шифрования.
5. Атака на алгоритм шифрования RSA Методом бесключевого чтения.
6. Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.
7. Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем. Содержание пояснительной записки работы:
8. 1. Задание и исходные данные.
9. 2. Описание структурной схемы проектируемой телекоммуникационной системы с указанием мест включения кодера помехоустойчивого кода, модуля¬тора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.
10. 3. Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов.
11. 4. Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.
12. 5. Расчет ширины спектра цифрового сигнала с заданным видом модуля¬ции.
13. 6. Расчет ширины спектра кодированного цифрового сигнала с заданным
14. видом модуляции в зависимости от скорости кода.

Согласована на портале № 22777

15. 7. Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала (ограниче¬ние 1.1).

16. 8. Определение перечня кодов со скоростями, превышающими допусти¬мую скорость , которые могут быть использованы для решения поставлен¬ной задачи.

17. 9. Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита (условие 1) и удовлетворяющего требованию ограничения по сложности декодера (ограничение 1.2).

18. 10. Проверочный расчет зависимости вероятности ошибки на выходе де¬кодера выбранного СК.

19. 11. Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.

20. 12. Заключение с подведением итогов выполненной работы.

21. 13. Список использованных источников.

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	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
8 семестр				
Выступление (доклад) на занятии		2	2	4
Домашнее задание		2	2	4
Защита отчета			8	8
Конспект самоподготовки		2	2	4
Контрольная работа		4	4	8
Опрос на занятиях	2	2	2	6
Отчет по индивидуальному заданию			8	8
Отчет по лабораторной работе		4	4	8
Отчет по практическому занятию	2	2	2	6
Расчетная работа			8	8
Тест	2	2	2	6
Итого максимум за период	6	20	44	70
Экзамен				30
Нарастающим итогом	6	26	70	100
9 семестр				
Выступление (доклад) на занятии			4	4

Согласована на портале № 22777

Домашнее задание			8	8
Защита отчета			2	2
Конспект самоподготовки	2	2	2	6
Контрольная работа		2	2	4
Опрос на занятиях		2	2	4
Отчет по индивидуальному заданию			8	8
Отчет по лабораторной работе		2	2	4
Отчет по практическому занятию	2	2	2	6
Расчетная работа			8	8
Реферат			6	6
Собеседование		2	2	4
Тест	2	2	2	6
Итого максимум за период	6	14	50	70
Экзамен				30
Нарастающим итогом	6	20	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	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	Ниже 60 баллов	F (неудовлетворительно)

Согласована на портале № 22777

зачтено)		

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Кодирование и шифрование информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 746 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7063, дата обращения: 29.11.2017.

12.2. Дополнительная литература

1. Кодирование в телекоммуникационных системах: Курс лекций, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 349 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7082, дата обращения: 29.11.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Кодирование и шифрование информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 746 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7063, дата обращения: 29.11.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Яндекс

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Компьютерный класс и видеодемонстрационная система

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74, 4 этаж, ауд. XXX. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

Согласована на портале № 22777

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 401. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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	Решение дистанционных тестов,	Преимущественно дистанционными

Согласована на портале № 22777

опорно-двигательного аппарата	контрольные работы, письменные самостоятельные работы, вопросы к зачету	методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 22777

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Кодирование и шифрование информации в радиоэлектронных системах передачи информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль): **Радиоэлектронные системы передачи информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РТС, Кафедра радиотехнических систем**
Курс: **4, 5**
Семестр: **8, 9**

Учебный план набора 2016 года

Разработчик:
- доцент кафедры, к.т.н., ст.н.с. каф. РТС А. М. Голиков

Экзамен: 8, 9 семестр

Томск 2017

Согласована на портале № 22777

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПСК-2.4	способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем	Должен знать знать - физические и математические модели процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем; - основные закономерности исторического процесса в науке и технике, этапы исторического развития радиотехники, место и значение радиосистем передачи информации в современном мире; - методологические основы и принципы современной науки. ; Должен уметь уметь - формулировать и решать задачи, грамотно использовать математический аппарат и численные методы для анализа и синтеза радиотехнических устройств и систем; - готовить методологическое обоснование научных исследований и технических разработок в области радиосистем передачи информации. ; Должен владеть владеть - математическим аппаратом для решения задач теоретической и прикладной радиотехники, методами исследования и моделирования систем передачи информации. ;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем

Согласована на портале № 22777

Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПСК-2.4

ПСК-2.4: способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	знать: - физические и математические модели процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем; - основные закономерности исторического процесса в науке и технике, этапы исторического развития радиотехники, место и значение радиосистем передачи информации в современном мире; - методологические основы и принципы современной науки; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем	уметь: - формулировать и решать задачи, грамотно использовать математический аппарат и численные методы для анализа и синтеза радиотехнических устройств и систем; - готовить методологическое обоснование научных исследований и технических разработок в области радиосистем передачи информации; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем	владеть: - математическим аппаратом для решения задач теоретической и прикладной радиотехники, методами исследования и моделирования систем передачи информации; - навыками методологического анализа научных исследований и их результатов; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем
Виды занятий	• Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Отчет по индивиду-	• Контрольная работа; • Домашнее задание; • Отчет по индивиду-	• Домашнее задание; • Отчет по лабораторной работе;

Согласована на портале № 22777

	альному заданию; • Конспект самоподготовки; • Коллоквиум; • Собеседование; • Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Выступление (доклад) на занятии; • Расчетная работа; • Тест; • Отчет по курсовой работе; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет; • Экзамен;	альному заданию; • Конспект самоподготовки; • Коллоквиум; • Собеседование; • Отчет по лабораторной работе; • Опрос на занятиях; • Защита курсовых проектов (работ); • Зачет; • Выступление (доклад) на занятии; • Расчетная работа; • Тест; • Отчет по курсовой работе; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет; • Экзамен;	• Отчет по индивидуальному заданию; • Защита курсовых проектов (работ); • Зачет; • Выступление (доклад) на занятии; • Расчетная работа; • Коллоквиум; • Отчет по курсовой работе; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• знать: - физические и математические модели процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем; - основные закономерности исторического процесса в науке и технике, этапы исторического развития радиотехники, место и значение радиосистем передачи информации в современном мире; - методологические основы и принципы современной науки; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проекти-	• уметь: - формулировать и решать задачи, грамотно использовать математический аппарат и численные методы для анализа и синтеза радиотехнических устройств и систем; - готовить методологическое обоснование научных исследований и технических разработок в области радиосистем передачи информации; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;	• владеть: - математическим аппаратом для решения задач теоретической и прикладной радиотехники, методами исследования и моделирования систем передачи информации; - навыками методологического анализа научных исследований и их результатов; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;

Согласована на портале № 22777

	рование и моделирование радиоэлектронных систем передачи информации и их подсистем;		
Хорошо (базовый уровень)	• знать: - физические и математические модели процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем; , место и значение радиосистем передачи информации в современном мире; - методологические основы и принципы современной науки; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;	• уметь: - формулировать и решать задачи, грамотно использовать математический аппарат и численные методы для анализа и синтеза радиотехнических устройств и систем; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;	• владеть: - математическим аппаратом для решения задач теоретической и прикладной радиотехники, методами исследования и моделирования систем передачи информации; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;
Удовлетворительно (пороговый уровень)	• знать: - основные закономерности исторического процесса в науке и технике, этапы исторического развития радиотехники, место и значение радиосистем передачи информации в современном мире; - методологические основы и принципы современной науки; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;	• уметь:- готовить методологическое обоснование научных исследований и технических разработок в области радиосистем передачи информации; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;	• владеть: - навыками методологического анализа научных исследований и их результатов; способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем; способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные

Согласована на портале № 22777

задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Вопросы на самоподготовку

– 1. Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– 2. Атака на алгоритм шифрования RSA Посредством метода Ферма.

– 3. Атака на алгоритм шифрования RSA методом повторного шифрования.

– 4. Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– 5. Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

– 6. Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

– 7. Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем.

3.2 Тестовые задания

– Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

– Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– Атака на алгоритм шифрования RSA Посредством метода Ферма.

– Атака на алгоритм шифрования RSA методом повторного шифрования.

– Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

–

3.3 Темы рефератов

– Аппаратно-программный комплекс визуализации и исследования Арифметических кодовАппаратно-программный комплекс для исследования и визуализации кода ХеммингаАппаратно-программный комплекс визуализации и исследования модемов сотовой связи FSK, MSK GMSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEWАппаратно-программный комплекс визуализации и исследования кода ХаффменаАппаратно-программный комплекс для визуализации и исследования алгоритма Витерби для декодирования сверточного кодаАппаратно-программный комплекс визуализации и исследования источника дискретных сообщений методом Шеннона-ФаноАппаратно-программный комплекс визуализации и исследования кодов Боуза-Чоудхури-Хоквенгема (БЧХ) с использованием MATLABРазработка программного комплекса для исследования методов аналогового скремблирования на базе LabVIEWАппаратно-программный комплекс визуализации и исследования алгоритмов Лемпеля - ЗиваАппаратно-про-

Согласована на портале № 22777

граммный комплекс визуализации и исследования Треллис кодовой модуляции (ТСМ). Сигнально-кодовые конструкцииАппаратно-программный комплекс визуализации и исследования схем OFDM-модуляторов и демодуляторовАппаратно-программный комплекс визуализации и исследования кодов Рида-Соломона в каналах с независимыми ошибками на базе MATLABАппаратно-программный комплекс визуализации и исследования низкоплотных кодов LDPCАппаратно-программный комплекс визуализации и исследования циклических избыточных кодов CRCАппаратно-программный комплекс визуализации и исследования каскадных кодовАппаратно-программный комплекс визуализации и исследования фрактальные методы кодирования изображенийАппаратно-программный комплекс визуализации и исследования решетчатого кодированияАппаратно-программный комплекс визуализации и исследования модемов спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEWАппаратно-программный комплекс визуализации и исследования метода свёрточного декодирования на основе последовательного алгоритмаАппаратно-программный комплекс визуализации и исследования Турбо кодовАппаратно-программный комплекс визуализации и исследования Перемежителей

3.4 Зачёт

– Нет зачета

3.5 Темы коллоквиумов

– Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– Атака на алгоритм шифрования RSA Посредством метода Ферма.

– Атака на алгоритм шифрования RSA методом повторного шифрования.

– Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

–

3.6 Темы домашних заданий

– Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

– Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– Атака на алгоритм шифрования RSA Посредством метода Ферма.

– Атака на алгоритм шифрования RSA методом повторного шифрования.

– Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

–

– Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем. Содержание пояснительной записки работы:

– 1. Задание и исходные данные.

– 2. Описание структурной схемы проектируемой телекоммуникационной системы с указанием мест включения кодера помехоустойчивого кода, модуля¬тора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.

– 3. Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в

Согласована на портале № 22777

проекте сверточных кодов.

– 4. Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.

– 5. Расчет ширины спектра цифрового сигнала с заданным видом модуля¬ции.

– 6. Расчет ширины спектра кодированного цифрового сигнала с заданным

– видом модуляции в зависимости от скорости кода.

– 7. Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала (ограниче¬ние 1.1).

– 8. Определение перечня кодов со скоростями, превышающими допусти¬мую скорость , которые могут быть использованы для решения поставлен¬ной задачи.

– 9. Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита (условие 1) и удовлетворяющего требованию ограничения по сложности декодера (ограничение 1.2).

– 10. Проверочный расчет зависимости вероятности ошибки на выходе де¬кодера выбранного СК.

– 11. Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.

– 12. Заключение с подведением итогов выполненной работы.

– 13. Список использованных источников.

–

3.7 Темы индивидуальных заданий

– Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

3.8 Вопросы на собеседование

– Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

– Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– Атака на алгоритм шифрования RSA Посредством метода Ферма.

– Атака на алгоритм шифрования RSA методом повторного шифрования.

– Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

–

– Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем. Содержание пояснительной записки работы:

– 1. Задание и исходные данные.

– 2. Описание структурной схемы проектируемой телекоммуникационной системы с ука-

Согласована на портале № 22777

занием мест включения кодера помехоустойчивого кода, модуля¬тора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.

– 3. Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов.

– 4. Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.

– 5. Расчет ширины спектра цифрового сигнала с заданным видом модуля¬ции.

– 6. Расчет ширины спектра кодированного цифрового сигнала с заданным

– видом модуляции в зависимости от скорости кода.

– 7. Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала (ограниче¬ние 1.1).

– 8. Определение перечня кодов со скоростями, превышающими допусти¬мую скорость , которые могут быть использованы для решения поставлен¬ной задачи.

– 9. Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита (условие 1) и удовлетворяющего требованию ограничения по сложности декодера (ограничение 1.2).

– 10. Проверочный расчет зависимости вероятности ошибки на выходе де¬кодера выбранного СК.

– 11. Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.

– 12. Заключение с подведением итогов выполненной работы.

– 13. Список использованных источников.

–

3.9 Темы опросов на занятиях

– Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSK GMSK и численный анализ вероятности

– символьной ошибки с использованием ПО LabVIEW.

– Модемы спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW

– Пропускная способность канала связи. Объем сигнала и емкость канала связи, условия их согласования.

– Исследование кодирования источника. Методы эффективного кодирования.

– Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.

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

– Циклические избыточные коды CRC (Cyclic redundancy check).

– Сверточные коды. Декодирование сверточных кодов.

– Декодирование сверточных кодов по методу Витерби.

– Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием.

– Сверточные турбокоды. Декодирование турбокодов. Характеристики

– помехоустойчивости сверточных турбокодов .

– Низкоплотностные коды. Классификация LDPC-кодов. Методы построения

– проверочных матриц. Алгоритмы декодирования низкоплотных кодов.

– Исследование каскадных кодов.

– 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.

– Помехоустойчивое кодирование яв¬ляется эффективным способом оптимизации ТКС. На практике инженеру проектровщику ТКС приходится решать задачи оптимизации на основе

Согласована на портале № 22777

численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов. Решение именно такой задачи положено в основу СР.

– Теория шифров с секретным ключом. Блочные и поточные системы шифрования. 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. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной 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 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.

3.10 Темы докладов

– Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

– Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– Атака на алгоритм шифрования RSA Посредством метода Ферма.

– Атака на алгоритм шифрования RSA методом повторного шифрования.

– Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

–

3.11 Темы контрольных работ

– 1. Дайте определение электронной цифровой подписи (ЭЦП) приведете термины, связанные с ЭЦП. Опишите порядок реорганизации, ликвидации, прекращения выполнения функций Центров сертификации открытых ключей ЭЦП.

–

–

–

– 2. В закон об электронной торговле используются следующие термины и определения: электронная торговля; электронный документ; отправитель электронного документа; получатель электронного документа; участник электронной торговли; лицо, осуществляющее электронную торговлю; клиент;

– информационный посредник; информационная система.

–

–

–

– 3. Договоры с лицами, осуществляющими предпринимательскую деятельность с использованием электронных средств. Использование электронных подписей в электронной коммерции.Правовой режим сделок , заключаемых при осуществлении электронной торговли.

Согласована на портале № 22777

–

–

– 4. Определите функцию криптографического хэширования. Перечислите представителей семейства хэш-функций, которые используют шифр как функцию сжатия. Перечислите некоторые схемы, который были разработаны, чтобы использовать блочный шифр как функцию сжатия.

–

– 5. Перечислите главные особенности функции криптографического хэширования SHA-512. Какой типа функции сжатия используется в SHA-512? Перечислите некоторые особенности функции криптографического хэширования. Какая функция сжатия используется в Whirlpool? Сравните контрастные особенности SHA-512 и функций криптографического хэширования Whirlpool.

–

– 6. Каков российский стандарт на алгоритм формирования криптографической хеш-функции? Каким образом можно использовать блочный алгоритм шифрования для формирования хеш-функции?

–

– 7. Чем асимметричные алгоритмы шифрования отличаются от симметричных? Для решения каких задач могут на практике применяться алгоритмы шифрования с открытым ключом? Каков алгоритм формирования цифровой подписи при использовании алгоритмов шифрования с открытым ключом?

–

– 8. Каким образом алгоритмы шифрования с открытым ключом могут использоваться для формирования общего секретного ключа у группы пользователей? Какие требования предъявляются к асимметричным алгоритмам? Для каких целей может применяться алгоритм RSA?

–

– 9. Опишите процесс шифрования с использованием алгоритма RSA. Для каких целей может применяться алгоритм Диффи-Хеллмана? Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана. Какие атаки возможны при использовании алгоритмов шифрования с открытым ключом?

–

– 10. Дайте определение схеме цифровой подписи RSA и сравните ее с криптографической системой RSA. Дайте определение схеме стандарта цифровой подписи (DSS) и сравните ее со схемами Эль-Гамаля и Шнорра. Дайте определение схеме цифровой подписи эллиптической кривой и сравните ее с криптосистемой на основе метода эллиптических кривых.

–

– 11. Напишите два алгоритма для DSS-схемы: один для процесса подписания и один для процесса проверки. Напишите два алгоритма для схемы эллиптической кривой: один для процесса подписания и один для процесса проверки.

–

– 12. В чем заключается проблема сертификации открытых ключей? Что включается в понятие инфраструктуры открытых ключей? Каковы функции центра сертификации открытых ключей? Что такое сертификат открытого ключа? Какая схема распределения открытых ключей абонентов может использоваться в системе связи, имеющей в своем составе центр сертификации открытых ключей?

–

– 13. Дайте определение центра сертификации (CA) и расскажите о его отношении к криптографии общедоступного ключа. Дайте определение рекомендации X.509 и разъясните ее цель. Перечислите режимы работы PKI.

–

– 14. Назовите семь типов пакетов, используемых в PGP, и объясните их цели.Назовите три типа сообщений в PGP и объясните их цели. Какие типы пакетов нужно передать в PGP, чтобы обеспечить следующие услуги безопасности:

Согласована на портале № 22777

– a. Конфиденциальность
– b. Целостность сообщения
– c. Определение подлинности
–
– 15. Перечислите услуги, обеспеченные SSL или TLS. Перечислите цель четырех протоколов, определенных в SSL или TLS. Определите цель каждой фазы в протоколе установления соединения.
–
– 16. Сравните и противопоставьте протоколы установления соединения в SSL и TLS. Сравните и противопоставьте протоколы передачи записей в SSL и TLS.
–
– 17. Покажите различия между двумя режимами IPSec. Определите протокол AH и услуги безопасности, которые он обеспечивает. Определите протокол ESP и услуги безопасности, которые он обеспечивает. Определите услуги обеспечения безопасности (SA) и объясните их цель.
–
– 18. Определите стратегию безопасности и объясните ее цель в отношении к IPSec. Определите IKE и объясните, почему этот протокол необходим в IPSec. Определите фазы IKE и цели каждой фазы. Определите ISAKMP и его отношение к IKE.
–
– 19. Покажите, как IPSec реагирует на атаку грубой силы. Если злоумышленник может сделать исчерпывающий компьютерный поиск, сможет ли он найти ключ шифрования

3.12 Экзаменационные вопросы

– 1. Турбокоды. Составные коды
–
– 2. Как возрастет сложность декодера Витерби при увеличении длины кодового ограничения СК вдвое? За счет чего повышается сложность декодера Витерби при переходе к мягкому решению на выходе демодулятора?
– 3. Что такое информация, сообщение, сигнал? Что такое линия связи, канал связи? Какие радиотехнические устройства обязательно входят в систему электросвязи?
–
– 4. Пропускная способность канала связи. Кодирование источника
–
– 5. Дайте характеристику зависимости протяженности магистрали системы передачи с ВОЛС от величины энергетического выигрыша, обеспечиваемого помехоустойчивым кодированием.
– 6. Что понимается под аддитивными и мультипликативными помехами? Перечислите известные Вам источники помех. В чем состоит сущест¬венное отличие помех от искажений?
– 7. Сигнально-кодовые конструкции
–
– 8. Как определяется энергетический выигрыш от применения помехо¬устойчивого кодирования? Каковы причины расширения спектра сигнала при использовании ко¬дирования?
– 9. Что называется кодированием источника? Что такое собственная информация символа? Перечислите свойства собственной информации. Что называется энтропией сигнала и как она вычисляется. Как вычисляется коэффициент избыточности?
– 10.Каскадное кодирование.
–
– 11. Дайте определение сигнально-кодовым конструкциям (СКК). Приведите структурную схему кодера-модулятора СКК.
–
– 12. Дайте формулировку теоремы Шеннона о кодировании в дискретном канале без помех.

Согласована на портале № 22777

– 13. Энергетическая и спектральная эффективность цифровой радиосвязи

– 14. Какими параметрами блоковых корректирующих кодов определяется вероятность ошибки декодирования в двоичном симметричном канале?

– 15. Дайте определение пропускной способности канала без помех приведите формулу. Приведите формулу для пропускной способности непрерывного канала с шумом.

– 16. Пропускная способность канала связи. Кодирование источника

– 17. Каково назначение корректирующего кодирования при передаче дис¬кретной информации?

– 18 Дайте определение сигнально-кодовым конструкциям, что они в себя включают? Что такое информационная эффективность ТКС? Приведите формулу для расчета

– 19. Метод свёрточного декодирования на основе последовательного алгоритма

–

– 20. Приведите основные параметры кода Хемминга. В чем состоят преимущества циклических кодов? Можно ли использовать коды Хемминга и циклические коды для ис¬правления однократных ошибок? Какими будут параметры этих кодов?

–

– 21. Перечислите показатели эффективности использования ресурсов ТКС. Приведите формулы для расчета. Что понимается под пределом Шеннона?

–

– 22. Дайте определение пространственно-временному кодированию (MIMO).

–

– 23. К какой границе (верхней либо нижней) следует стремиться при раз¬работке новых блоковых кодов?

–

– 24. Что такое удельная скорость передачи информации и как она зависит от отношения сигнал/шум?

– 25. Методы решетчатого кодирования/декодирования на базе Треллис кодовой модуляции (TCM).

–

– 26. Временные и частотные аналоговые скремблеры

–

– 27. Какова зависимость вероятность ошибки оптимального приема сигналов от числа позиций M?

–

– 28. Модемы сотовой системы связи (FSK, MSK, GFSK, GMSK).

–

– 29. Циклические коды. 1. Определение циклического кода. 2. Полиномиальное описание циклических кодов

–

– 30. Приведите формулу определяющую зависимость энергетической эффективности от частотной эффективности для идеальной системы, обеспечивающей равенство скорости передачи информации пропускной способности канала, определяющую зависимость "Предел Шеннона".

– 31. Технологии множественного доступа на базе OFDM-модуляции и технологии MIMO

–

– 32. Примеры линейных кодов. 1. Границы минимального расстояния для линейных кодов. 33. Коды Хэмминга. 3. Q-ичный код Хэмминга. 4. Коды Рида-Маллера

–

– 34. Какую величину не может превышать энергетическая эффективность любой системы передачи информации по Гауссовскому каналу (приведите численное значение)? Каким требованиям должны удовлетворять сигнально-кодовые конструкции?

– 35. Методы модуляции QPSK и QAM.

Согласована на портале № 22777

–

– 36. Какими параметрами описываются синусоидальный сигнал и меандр, а также их спектры?

– 37. Опишите метод последовательного каскадного кодирования/декодирования предложенного Д. Форни.

– 38. Многоуровневые методы модуляции сигналов, используемые в спутниковых системах связи

–

– 39.Дайте характеристику смеси АВ+шум на входе и выходе фильтров нижних частот (lowpass): Баттерворта, Чебышева, Чебышева инверсного, эллиптического, Бесселя.

– 40. Опишите структуру Турбокодов.

– 41. Помехоустойчивые коды Хэминга.

–

– 42. Каково практическое значение использования нижней границы Варшамова-Гилберта и верхней границы Хемминга для оценки характеристик бло¬ковых корректирующих кодов?

–

– 43. Как строится автокорреляционная функция и какими свойствами она обладает. Для чего производится квантование сигнала и каким принципам оно должно удовлетворять?

– 44. Технологии множественного доступа на базе OFDM-модуляции.

–

– 45. Исправление и обнаружение ошибок с помощью линейных кодов. 2.1. Стандартное расположение. 2.2. Исправление ошибок

–

– 46. Дайте определение модуляции FSK, MSK и GMSK, опишите их свойства, Дайте характеристику зависимости величины ошибки (в BER) от отношения сигнал/шум при использовании фильтров. Дайте характеристику "глазковой диаграммы" и джиттера.

–

– 47. Обработка звуковых сигналов с использованием вейвлет преобразований.

–

– 48. Какова основная идея алгоритма Лемпеля-Зива? За счет чего происходит увеличение избыточности вместо уменьшения при малых длинах произвольной входной последовательности?

–

– 49. Приведите характеристики методов помехоустойчивого кодирования в системах ВОЛС.

–

– 50. Методы сжатия с потерей информации. Кодирование преобразований. Стандарт сжатия JPEG и JPEG 2000. Фрактальный метод.

–

– 51. Проблема кодирования. 1. Симметричный канал. Блоковые коды. 2. Ошибки типа замещения символов и принцип максимального правдоподобия . 3. Кодовое расстояние и исправление ошибок

–

– 53. Принцип последовательного декодирования? Отличие последовательного алгоритма от алгоритма Витерби?

–

– 54. Методы свёрточного кодирования и декодирования на основе последовательного алгоритма. Пороговое декодирование.

–

– 55. Линейные блоковые коды. 1. Структура линейных блоковых кодов. 2. Матричное описание линейных блоковых кодов. 2.1. Порождающая матрица линейного кода. 2.2. Проверочная матрица линейного кода.

–

Согласована на портале № 22777

– 56. Поясните термин «Свёрточный код». Важнейшие отличия сверточных кодов от блоковых? Что представляет собой свёрточный кодер?

– 57. Коды Боуза-Чоудхури-Хоквенгема (БЧХ).

–

– 58. Кодирование источника дискретных сообщений методом Вейвлет преобразований.

– 59. Как следует выбрать свободное расстояние СК, обеспечивающего исправление двухкратных ошибок? К чему приводит увеличение свободного расстояния СК? Зависит ли сложность реализации алгоритма Витерби от длины свободного расстояния СК?

–

– 60. Кодирование и декодирование с использованием Турбокодов.

–

– 61.Кодирование источника дискретных сообщений методом. Фрактальных преобразований.

– 62. Принцип последовательного декодирования? Отличие последовательного алгоритма от алгоритма Витерби?

– 63. Алгоритм Витерби для декодирования сверточного кода

–

– 64. Кодирование источника дискретных сообщений методом Хаффмена.

– 65. Дайте определения (приведите формулы) показателей информационной, энергетической и частотной эффективности ТКС.

– 66. Коды Рида-Соломона в каналах с независимыми ошибками.

–

– 67.Кодирование источника дискретных сообщений методом Лемпеля-Зива.

– 68. Дайте определение предельная эффективность телекоммуникационных систем и границы К. Шеннона.

–

– 69. Кодирование/декодирование в беспроводных системах цифрового вещания и

– связи. Коды LDPC

–

– 70. Кодирование источника дискретных сообщений методом Шеннона-Фано

– 71. Как судят о совершенстве методов передачи цифровой информации по степени приближения реальных значений эффективности к предельным значениям?

– 72. Методы аналогового скремблирования.

–

– 73. Кодирование источника дискретных сообщений методом Арифметического

– кодирования.

– 74. Эффективность систем передачи дискретных сообщений можно существен¬но повысить путем применения многопозиционных сигналов и корректирую¬щих кодов, а также их комбинаций. Выбор сигналов и кодов в этих случаях яв¬ляется определяющим для построения высокоэффективных систем передачи (согласованных между собой кодеков и модемов). В чем заключается их согласование?

–

– 75. На секретности какого элемента основана защита информации надежными алгоритмами шифрования? Каковы три вида атак на схему шифрования?

–

– 76. Опишите поточные режимы AES, режим обратной связи по шифртексту (CFB), режим обратной связи по выходу (OFB) и режим счетчика (Counter mode).

–

– 77. Дайте определение электронной цифровой подписи (ЭЦП) приведете термины, связанные с ЭЦП. Опишите порядок реорганизации, ликвидации, прекращения выполнения функций Центров сертификации открытых ключей ЭЦП.

Согласована на портале № 22777

–

– 78. Покажите, как IPSec реагирует на атаку грубой силы. Если злоумышленник может сделать исчерпывающий компьютерный поиск, сможет ли он найти ключ шифрования для IPSec?

–

– 79. Какую длину имеют ключи DES? В чем заключается основной недостаток DES? За счет чего тройной DES повышает уровень безопасности алгоритма DES?

– 80. Опишите поточные режимы ГОСТ 28147-89, алгоритм криптографического преобразования ГОСТ 28147-89, реализацию алгоритма зашифрования в режиме гаммирования, реализацию алгоритма зашифрования в режиме гаммирования с обратной связью. Каким образом производится расшифрование в режиме гаммирования с обратной связью?

–

– 81. В закон об электронной торговле используются следующие термины и определения: электронная торговля; электронный документ; отправитель электронного документа; получатель электронного документа; участник электронной торговли; лицо, осуществляющее электронную торговлю; клиент;

– информационный посредник; информационная система.

–

– 82. Определите стратегию безопасности и объясните ее цель в отношении к IPSec. Определите IKE и объясните, почему этот протокол необходим в IPSec. Определите фазы IKE и цели каждой фазы. Определите ISAKMP и его отношение к IKE.

–

– 83. На сложности какой задачи базируется безопасность, обеспечиваемая алгоритмом Диффи-Хеллмана? Можно ли использовать алгоритм Диффи-Хеллмана для шифрования трафика? Назовите основную атаку, которой подвержен алгоритм Диффи-Хеллмана (с правильно выбранными a и b).

–

– 84. Генераторы на основе LFSR. На какие системы подразделяют поточные шифры на основе LFSR. Дайте им определения. Опишите работу регистров сдвига с нелинейной обратной связью и регистров сдвига с обратной связью по переносу.

–

– 85. Договоры с лицами, осуществляющими предпринимательскую деятельность с использованием электронных средств. Использование электронных подписей в электронной коммерции.Правовой режим сделок , заключаемых при осуществлении электронной торговли.

–

– 86. Покажите различия между двумя режимами IPSec. Определите протокол AH и услуги безопасности, которые он обеспечивает. Определите протокол ESP и услуги безопасности, которые он обеспечивает. Определите услуги обеспечения безопасности (SA) и объясните их цель.

–

– 87. Что такое цифровая подпись? Почему открытые ключи должны быть сертифицированными? В чем заключается проблема, связанная с управлением ключами, которая вызывает сбои в большей части систем PKI?

–

– 88. Строительные блоки поточных шифров. Опишите регистры сдвига с обратной связью. Опишите регистры сдвига с линейной обратной связью.

–

– 89. Определите функцию криптографического хэширования. Перечислите представителей семейства хэш-функций, которые используют шифр как функцию сжатия. Перечислите некоторые схемы, который были разработаны, чтобы использовать блочный шифр как функцию сжатия.

–

– 90. Сравните и противопоставьте протоколы установления соединения в SSL и TLS. Сравните и противопоставьте протоколы передачи записей в SSL и TLS.

Согласована на портале № 22777

–

– 91. Дайте определения ключевой симметричной криптосистемы и ключевая асимметричной криптосистемы, а также криптографической стойкости. Что такое криптографический протокол и протокол распределения ключей? Что представляет собой цифровая подпись (сообщения или электронного документа)?

–

– 92. Поточные шифры. Дайте опредесения синхронным и самосинхронизирующимся поточным шифрам. Поточные режимы блочных шифров. Дайте определения основным поточным режимам стандартов блочного шифрования DES (Data Encryption Standard) и AES (Advanced Encryption Standard) и отечественного стандарта блочного шифрования ГОСТ 28147-89.

–

– 93. Перечислите главные особенности функции криптографического хэширования SHA-512. Какой типа функции сжатия используется в SHA-512? Перечислите некоторые особенности функции криптографического хэширования. Какая функция сжатия используется в Whirlpool? Сравните контрастные особенности SHA-512 и функций криптографического хэширования Whirlpool.

–

– 94. Перечислите услуги, обеспеченные SSL или TLS. Перечислите цель четырех протоколов, определенных в SSL или TLS. Определите цель каждой фазы в протоколе установления соединения.

–

– 95. Опишите структуру сети Фейстеля. Что является основной характеристикой алгоритма, построенного на основе сети Фейстеля?

–

– 96. Опишите спецификации алгоритма Rijndael. Состояние, ключ шифрования и число раундов. Преобразование раунда. Преобразование ByteSub. Преобразование ShiftRow. Преобразование MixColumn. Сложение с ключом раунда. Создание ключей раунда Расширение ключа. Выбор ключа раунда. Опишите алгоритм шифрования, преимущества алгоритма, формирование различной длины блока и ключа шифрования, как Rijndael может применяться в качестве алгоритма MAC, хэш-функция Rijndael, генератор псевдослучайных чисел на основе Rijndael

–

– 97. Перечислите главные особенности функции криптографического хэширования SHA. Какой типа функции сжатия используется в SHA-512? Перечислите некоторые особенности функции криптографического хэширования. Какая функция сжатия используется в Whirlpool? Сравните контрастные особенности SHA-512 и функций криптографического хэширования Whirlpool.

–

– 99. Назовите семь типов пакетов, используемых в PGP, и объясните их цели.Назовите три типа сообщений в PGP и объясните их цели. Какие типы пакетов нужно передать в PGP, чтобы обеспечить следующие услуги безопасности:

– a. Конфиденциальность

– b. Целостность сообщения

– c. Определение подлинности

– 2. Перечислите используемые критерии при разработке алгоритмов симметричного шифрования. Дайте определения алгоритмам симметричного шифрования DES (Data Encryption Standard) тройной DES с двумя ключами.

–

– 100. Дайте характеристику алгоритмам RC6 и Rijndael в соответствии с параметрами: общая безопасность; программные реализации; окружения с ограничениями пространства; шифрование и дешифрование; свойства ключа; другие возможности настройки. Приведите математические понятия, лежащие в основе алгоритма Rijndael. Какие три критерия использовались при обосновании разработки алгоритма Rijndael?

– 101. Каков российский стандарт на алгоритм формирования криптографической хеш-

Согласована на портале № 22777

функции? Каким образом можно использовать блочный алгоритм шифрования для формирования хеш-функции?

–

– 102. Дайте определение центра сертификации (CA) и расскажите о его отношении к криптографии общедоступного ключа. Дайте определение рекомендации X.509 и разъясните ее цель. Перечислите режимы работы PKI.

–

– 103. Каким образом вычисляются подключи с использованием алгоритма Blowfish?. Дайте определение алгоритму IDEA (International Data Encryption Algorithm). Какие характеристики IDEA характеризуют его криптографическую стойкость? Опишите алгоритмы шифрования и дешифрования IDEA

–

– 104. Дайте характеристику программной реализации AES. Дайте характеристику в зависимости скорости выполнения AES в зависимости от длины ключа и краткий вывод о скорости выполнения на основных программных платформах.

–

– 105. Чем асимметричные алгоритмы шифрования отличаются от симметричных? Для решения каких задач могут на практике применяться алгоритмы шифрования с открытым ключом? Каков алгоритм формирования цифровой подписи при использовании алгоритмов шифрования с открытым ключом?

–

– 106. В чем заключается проблема сертификации открытых ключей? Что включается в понятие инфраструктуры открытых ключей? Каковы функции центра сертификации открытых ключей? Что такое сертификат открытого ключа? Какая схема распределения открытых ключей абонентов может использоваться в системе связи, имеющей в своем составе центр сертификации открытых ключей?

–

– 107. Опишите алгоритмы шифрования и дешифрования ГОСТ 28147, являющийся отечественным стандартом для алгоритмов симметричного шифрования. Опишите основные различия между DES и ГОСТ 28147.

–

– 108. В случае линейной или дифференциальной атаки на DES требуется 243 известного незашифрованного текста и 247 шифрований выбранного незашифрованного текста. Какова криптостойкость AES? Что определяет "фактор безопасности" алгоритма шифрования? Как производится статистическое тестирование алгоритма шифрования? Дайте описание.

–

– 109. Каким образом алгоритмы шифрования с открытым ключом могут использоваться для формирования общего секретного ключа у группы пользователей? Какие требования предъявляются к асимметричным алгоритмам? Для каких целей может применяться алгоритм RSA?

–

– 110. Напишите два алгоритма для DSS-схемы: один для процесса подписания и один для процесса проверки. Напишите два алгоритма для схемы эллиптической кривой: один для процесса подписания и один для процесса проверки.

–

– 111. Дайте определения четырем режимам выполнения алгоритмов симметричного шифрования (ECB - Electronic Codebook, CBC - Cipher Block Chaining, CFB - Cipher Feedback, OFB - Output Feedback). Опишите алгоритмы шифрования и дешифрования в режиме CFB.

– 112. Какие четыре фундаментальных принципа выбора алгоритма использовала команда NIST при выборе алгоритма AES? Дайте сравнение алгоритмам тройной DES и AES. Можно ли изменять количество раундов AES-алгоритма?

–

– 113. Опишите процесс шифрования с использованием алгоритма RSA. Для каких целей

Согласована на портале № 22777

может применяться алгоритм Диффи-Хеллмана? Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана. Какие атаки возможны при использовании алгоритмов шифрования с открытым ключом?

–

– 114. Дайте определение схеме цифровой подписи RSA и сравните ее с криптографической системой RSA. Дайте определение схеме стандарта цифровой подписи (DSS) и сравните ее со схемами Эль-Гамаля и Шнорра. Дайте определение схеме цифровой подписи эллиптической кривой и сравните ее с криптосистемой на основе метода эллиптических кривых.

3.13 Вопросы для подготовки к практическим занятиям, семинарам

– Модемы сотовой связи FSK, MSK GMSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW. Модемы спутниковых систем связи M-QAM, M-PSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW.

– Исследование кодирования источника дискретных сообщений методами Шеннона-Фано. Исследование алгоритмов Лемпеля - Зива. Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.

– Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона на базе MATLAB.

– Циклические избыточные коды CRC (Cyclic redundancy check).

– Сверточные коды. Декодирование сверточных кодов.

– Декодирование сверточных кодов по методу Витерби с использованием ПО MATLAB.

– Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов . Исследование турбокодов с использованием ПО MATLAB 3.6. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования на базе MATLAB и LabVIEW.

– Исследование каскадных кодов.

– 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 с использованием NI LabVIEW.

– 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.

– Теория шифров с секретным ключом. Блочные и поточные системы шифрования. 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. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной 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 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.

– Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки по-

Согласована на портале № 22777

явления 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 криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).

– 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. 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.

– PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. 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). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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 работыSSL. 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-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный секретный код.Сеансы и соединение. Протокол TLS. Генерация криптографической 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 является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for the Internet Protocol. Размещение 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. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.

– 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. Иерархия ключей в E-UTRAN. Генерирование ключей шифрации и целостности для NAS сигнализации. Алгоритм шифрации в E-UTRAN. Алгоритм проверки целостности E-UTRAN. Моделирование технологии LTE в среде MATLAB с использованием встроенного пакета LTE System Toolbox.

Согласована на портале № 22777

3.14 Вопросы дифференцированного зачета

– Зачета нет

3.15 Темы расчетных работ

– Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной самостоятельной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

– Криптоанализ алгоритма RSA. Атаки на алгоритм RSA. Взлом RSA при неудачном выборе параметров криптосистемы. Атака повторным шифрованием. Атака на основе Китайской теоремы об остатках.Бесключевое чтение.

– Атака на алгоритм шифрования RSA Посредством метода Ферма.

– Атака на алгоритм шифрования RSA методом повторного шифрования.

– Атака на алгоритм шифрования RSA Методом бесключевого чтения.

– Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках.

–

– Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем. Содержание пояснительной записки работы:

– 1. Задание и исходные данные.

– 2. Описание структурной схемы проектируемой телекоммуникационной системы с указанием мест включения кодера помехоустойчивого кода, модуля¬тора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.

– 3. Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов.

– 4. Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.

– 5. Расчет ширины спектра цифрового сигнала с заданным видом модуля¬ции.

– 6. Расчет ширины спектра кодированного цифрового сигнала с заданным

– видом модуляции в зависимости от скорости кода.

– 7. Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала (ограниче¬ние 1.1).

– 8. Определение перечня кодов со скоростями, превышающими допусти¬мую скорость , которые могут быть использованы для решения поставлен¬ной задачи.

– 9. Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита (условие 1) и удовлетворяющего требованию ограничения по сложности декодера (ограничение 1.2).

– 10. Проверочный расчет зависимости вероятности ошибки на выходе де¬кодера выбранного СК.

– 11. Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.

– 12. Заключение с подведением итогов выполненной работы.

– 13. Список использованных источников.

–

3.16 Темы лабораторных работ

– Модемы сотовой связи FSK, MSK GMSK и численный анализ вероятности символьной ошибки с использованием ПО LabVIEW. Модемы спутниковых систем связи M-QAM, M-PSK и

Согласована на портале № 22777

численный анализ вероятности символьной ошибки с использованием ПО LabVIEW.

– Исследование кодирования источника дискретных сообщений методами Шеннона-Фано. Исследование алгоритмов Лемпеля - Зива. Фрактальные методы кодирования изображений. Вейвлет преобразования сигналов и изображений.

– Исследование кодов Хемминга, БЧХ (Боуза-Чоудхури-Хоквенгема), Рида-Соломона на базе MATLAB.Циклические избыточные коды CRC (Cyclic redundancy check).Сверточные коды. Декодирование сверточных кодов.Декодирование сверточных кодов по методу Витерби с использованием ПО MATLAB.Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов . Исследование турбокодов с использованием ПО MATLAB 3.6. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодирования на базе MATLAB и LabVIEW.Исследование каскадных кодов.

– Сигнально-кодовые конструкции на основе Треллис кодовой модуляции (ТСМ) и их анализ с использованием MATLAB. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO с использованием NI LabVIEW.

– 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.

– Теория шифров с секретным ключом. Блочные и поточные системы шифрования. 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. Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обратной 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 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.

– 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 криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).

– 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. 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 криптогра-

Согласована на портале № 22777

фических 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. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. 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). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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 работыSSL. 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-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный секретный код.Сеансы и соединение. Протокол TLS. Генерация криптографической 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 является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for the Internet Protocol. Размещение и функционирование IPsec. Транспортный режим работы. Тунельный режим работы. Контексты безопасности и управление ключами. Протокольные контексты и политика безопасности. Аутентификационный заголовок. Безопасное сокрытие существенных данных. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.

– 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. 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.PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. 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). Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. 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 работыSSL. 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-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Ге-

Согласована на портале № 22777

нерирование криптографических параметров. Главный секретный код.Сеансы и соединение. Протокол TLS. Генерация криптографической 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 является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for the Internet Protocol. Размещение 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. Протокол обмена ключами – IKE. Расширенный обзор безопасных ассоциаций.

3.17 Темы курсовых проектов (работ)

– Курсовой работы нет

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Кодирование и шифрование информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 746 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7063, свободный.

4.2. Дополнительная литература

1. Кодирование в телекоммуникационных системах: Курс лекций, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 349 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7082, свободный.

4.3. Обязательные учебно-методические пособия

1. Кодирование и шифрование информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 746 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7063, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. Яндекс

Согласована на портале № 22777