МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА 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) / специализация: **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 2018 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

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 20.12.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 24652

Рассмотрена и одобрена на заседании кафедры
протокол № 9 от « 26 » 4 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.05.01 Радиоэлектронные системы и комплексы, утвержденного 11.08.2016 года, рассмотрена и одобрена на заседании кафедры РТС « 26 » апреля 2018 года, протокол № 9.

Разработчик:

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

Заведующий обеспечивающей каф. РТС _____ С. В. Мелихов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РТС _____ С. В. Мелихов

Эксперты:

Доцент кафедры радиотехнических систем (РТС) _____ В. А. Громов

Старший преподаватель кафедры радиотехнических систем (РТС) _____ Д. О. Ноздреватых

Согласована на портале № 24652

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Дисциплина "Кодирование и шифрование информации в радиоэлектронных системах передачи информации" (КиШИвРЭСПИ) относится к числу дисциплин специализации 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, позволяющих самостоятельно проводить математический анализ физических процессов в аналоговых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчивости телекоммуникационных систем и сетей.

– В курсе КиШИвРЭСПИ принят единый методологический подход к анализу и синтезу современных 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.31.3) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Кодирование и шифрование информации в радиоэлектронных системах передачи информации.

Последующими дисциплинами являются: Кодирование и шифрование информации 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 обучающийся 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 прикладной 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

Согласована на портале № 24652

		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
Оформление отчетов по лабораторным работам	32	16	16
Проработка лекционного материала	12	6	6
Подготовка к практическим занятиям, семинарам	44	22	22
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	Де к., ч	ра к. за	б. ра б.,	м. ра б.,	в (б ез	уе м ые ко м
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	8	4	9	23	ПСК-2.4
3 Помехоустойчивое кодирование в телекоммуникационных системах	8	8	6	18	40	ПСК-2.4
4 Сигнально-кодовые конструкции в телекоммуникационных системах	2	8	2	7	19	ПСК-2.4
5 Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем (задание на самостоятельную работу)	0	0	0	1	1	ПСК-2.4
Итого за семестр	16	32	16	44	108	
9 семестр						
6 Классические шифры	2	4	2	7	15	ПСК-2.4
7 Шифрование с секретным ключом	4	8	6	16	34	ПСК-2.4
8 Шифрование с открытым ключом	4	8	4	9	25	ПСК-2.4
9 Криптографические протоколы в сетях передачи данных	4	6	4	9	23	ПСК-2.4
10 Шифрование в современных	2	6	0	3	11	ПСК-2.4

Согласована на портале № 24652

системах связи						
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	ое мкос	ые ко
8 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSKGMSK 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	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 телекоммуникационных системах	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.	8	ПСК-2.4
	Итого	8	
4 Сигнально-кодовые конструкции в телекоммуникационных системах	Сигнально-кодовые конструкции на основе Треллис кодовой модуляции(TCM) и их анализ. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO.	2	ПСК-2.4
	Итого	2	
Итого за семестр		16	
9 семестр			

Согласована на портале № 24652

6 Классические шифры	Помехоустойчивое кодирование является эффективным способом оптимизации ТКС. На практике инженеру проектировщику 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.	1	ПСК-2.4
	Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифров замены. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шифр Хилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.	1	
	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 режиме. Методы оценки качества алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммышифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров. 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 шифрMICKEY-128. Поточный шифр Trivium. Российский блочный шифр ГОСТ 28147-89 в поточном режиме. Блочный шифр AES в поточном	4	ПСК-2.4
	Итого	4	

Согласована на портале № 24652

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 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 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 работы SSL. Многослойная среда	4	ПСК-2.4

Согласована на портале № 24652

	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 theInternet 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. 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		
	Итого	4	
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	2	ПСК-2.4

	MATLAB с использованием встроенного пакета LTE System Toolbox		
	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 Кодирование и шифрование информации в радиоэлектронных системах передачи информации	+	+	+	+	+	+	+	+	+	+
Последующие дисциплины										
1 Кодирование и шифрование информации 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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Практ. зан.	Лаб. раб.	Сам. раб.	
ПСК-2.4	+	+	+	+	Контрольная работа, Отчет по индивидуальному заданию, Экзамен, Конспект самоподготовки, Коллоквиум, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Расчетная работа, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

Согласована на портале № 24652

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	ое мк ос	м ые ко
8 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Модемы сотовой связи FSK, MSKGMSK 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 базеMATLAB. Циклические избыточные коды CRC (Cyclic redundancycheck). 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.	6	ПСК-2.4
	Итого	6	
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.	2	ПСК-2.4
	Итого	2	
Итого за семестр		16	
9 семестр			
6 Классические шифры	Теория классических шифров. Основные характеристики открытого текста. Классификация	2	ПСК-2.4

Согласована на портале № 24652

	шифров. Классификация шифровзамены. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. ШифрХилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистрсдвига 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 шифрMICKEY-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 гаммышифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров	6	ПСК-2.4
	Итого	6	
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	4	ПСК-2.4

Согласована на портале № 24652

	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. Организациясетей 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 центрыдоверия, 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 не используемого 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	4	ПСК-2.4

Согласована на портале № 24652

	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 theInternet 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	
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)	ое мкос ые ко	
8 семестр			
1 Цифровые виды модуляции и сигнального кодирования, их спектральная и энергетическая эффективность	Модемы сотовой связи FSK, MSKGMSK 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.	8	ПСК-2.4
	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.	8	ПСК-2.4

Согласована на портале № 24652

	Итого	8	
3 Помехоустойчивое кодирование в телекоммуникационных системах	Исследование кодов Хемминга, БЧХ(Боуза-Чоудхури-Хоквенгема), Рида-Соломона на базе MATLAB. Циклические избыточные коды CRC (Cyclic redundancycheck).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 декодированияна базе MATLAB и LabVIEW. Исследование каскадных кодов	8	ПСК-2.4
	Итого	8	
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	8	ПСК-2.4
	Итого	8	
Итого за семестр		32	
9 семестр			
6 Классические шифры	Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифровзамены. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. ШифрХилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. 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 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.	8	ПСК-2.4

Согласована на портале № 24652

	Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига собратной 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 шифрMICKEY-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 гаммышифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров.		
	Итого	8	
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).	8	ПСК-2.4
	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 откомпрометации. 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	6	ПСК-2.4

	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 работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол. Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный Диффи-Хеллман (Diffie-Hellman), кратковременный Диффи-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 theInternet 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	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.	6	ПСК-2.4
	Итого	6	
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,	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	Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
2 Пропускная способность канала связи. Кодирование источника	Подготовка к практическим занятиям, семинарам	4	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по
	Проработка лекционного материала	1		

Согласована на портале № 24652

	Оформление отчетов по лабораторным работам	4		индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Итого	9		
3 Помехоустойчивое кодирование в телекоммуникационных системах	Подготовка к практическим занятиям, семинарам	10	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	6		
	Итого	18		
4 Сигнально-кодовые конструкции в телекоммуникационных системах	Подготовка к практическим занятиям, семинарам	4	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	7		
5 Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем (задание на самостоятельную работу)	Проработка лекционного материала	1	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Итого	1		
Итого за семестр		44		
	Подготовка и сдача экзамена	36		Экзамен
9 семестр				
6 Классические шифры	Подготовка к практическим занятиям, семинарам	4	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях,
	Проработка лекционного	1		

Согласована на портале № 24652

	материала			Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Итого	7		
7 Шифрование с секретным ключом	Подготовка к практическим занятиям, семинарам	8	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	6		
	Итого	16		
8 Шифрование с открытым ключом	Подготовка к практическим занятиям, семинарам	4	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
9 Криптографические протоколы в сетях передачи данных	Подготовка к практическим занятиям, семинарам	4	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
10 Шифрование в современных системах связи	Подготовка к практическим занятиям, семинарам	2	ПСК-2.4	Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе,
	Проработка лекционного материала	1		
	Итого	3		

Согласована на портале № 24652

				Отчет по практическому занятию, Расчетная работа, Собеседование, Тест, Экзамен
Итого за семестр		44		
	Подготовка и сдача экзамена	36		Экзамен
Итого		160		

10. Курсовая работа (проект)

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

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				
Конспект самоподготовки	2	2	2	6
Контрольная работа		4	4	8
Опрос на занятиях	2	2	2	6
Отчет по индивидуальному заданию			12	12
Отчет по лабораторной работе		4	4	8
Отчет по практическому занятию	4	4		8
Расчетная работа		12		12
Собеседование		4		4
Тест	2	2	2	6
Итого максимум за период	10	34	26	70
Экзамен				30
Нарастающим итогом	10	44	70	100
9 семестр				
Конспект самоподготовки	2	2	2	6
Контрольная работа		4	4	8
Опрос на занятиях	2	2	2	6
Отчет по индивидуальному заданию			12	12

Согласована на портале № 24652

Отчет по лабораторной работе		4	4	8
Отчет по практическому занятию	4	4		8
Расчетная работа		12		12
Собеседование		4		4
Тест	2	2	2	6
Итого максимум за период	10	34	26	70
Экзамен				30
Нарастающим итогом	10	44	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 зачтено)	Ниже 60 баллов	F (неудовлетворительно)

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: 02.05.2018.

12.2. Дополнительная литература

1. Акулиничев, Ю. П. Радиотехнические системы передачи информации: Учебное пособие [Электронный ресурс] / Акулиничев Ю. П., Бернгардт А. С. — Томск: ТУСУР, 2015. — 196 с. — Режим доступа: https://edu.tusur.ru/publications/5851. дата обращения: 02.05.2018.

Согласована на портале № 24652

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: 02.05.2018.

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

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

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. www.elibrary.ru
2. uisrussia.msu.ru

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

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

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager

Согласована на портале № 24652

- Free Pascal
- Free Pascal Lazarus (версия 1.6)
- GIMP
- Google Chrome
- Microsoft Windows Server 2008
- Microsoft Windows XP
- Mozilla Firefox
- OpenOffice
- Opera
- Opera Developer
- PTC Mathcad13, 14
- Scilab

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

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

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Free Pascal
- Free Pascal Lazarus (версия 1.6)
- GIMP
- Google Chrome
- Microsoft Windows Server 2008
- Microsoft Windows XP
- Mozilla Firefox
- OpenOffice
- Opera
- Opera Developer
- PTC Mathcad13, 14
- Scilab

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

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

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

Состав оборудования:

Согласована на портале № 24652

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

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

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

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

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какой из фазовых видов модуляции обеспечивает наибольшую помехоустойчивость?
- BPSK
- QPSK
- 8-PSK
- 16-QAM

2. Какой из фазовых видов модуляции обеспечивает наибольшую скорость передачи информации?
- BPSK
- QPSK
- 8-PSK
- 16-QAM

3. Какой из видов частотной модуляции имеет минимальную ширину спектра?
- FSK
- MSK
- GMSK
- M-FSK

4. Какой из методов кодирования источника производит кодирование с потерями?
- Коды Шеннона-Фано

Согласована на портале № 24652

- Алгоритм Лемпеля - Зива
- Вейвлет преобразование
- Коды Хаффмана

5. Какой код является блоковым?
- Код Хемминга
- БЧХ (Боуза-Чоудхури-Хоквенгема)
- Рида-Соломона
- Файра

6. Какой из кодов обеспечивает наибольшее число обнаруженных ошибок ?
- Код Хемминга
- БЧХ (Боуза-Чоудхури-Хоквенгема)
- Рида-Соломона
- Файра

7. Какой из циклических избыточных кодов CRC (Cyclic redundancy check) обеспечивает наибольшее число обнаруженных ошибок от числа контрольных сумм для различных полиномов CRC-кода?
- CRC-1
- CRC-16-IBM
- CRC-30
- CRC-4-ITU

8. Какой из кодов обеспечивает наименьшую вероятность битовой ошибки (BER) при SNR > 5 Дб?
- Сверточный
- Каскадный
- Рида-Соломона
- Турбокод

9. Какие из кодов и сигнально-кодовых конструкций наиболее приближены к верхней границе Шеннона?
- АФМ-16-СК
- БЧХ
- ФМ-2
- АМ-2

10. Какое расстояние между сигнальными точками ФМн-8 обеспечивает наибольшую помехоустойчивость?
- 0,765
- 1,414
- 1,848
- 2,000

11. Чему равна величиной предельной энергетической эффективности (предел Шеннона)?
- 1,59 Дб
- 1,69 Дб
- 2,56 Дб
- 3,22 Дб

12. Какова длина дайджеста Хеш-функции ГОСТ?
- 56
- 128
- 192
- 256

13. Какова длина ключа шифра DES?
- 48
- 56
- 128
- 256

14. Какова длина ключа шифра ГОСТ 28147?

Согласована на портале № 24652

- 48
- 56
- 128
- 256

15. Какое количество раундов шифра DES?
- 16
- 32
- 48
- 56

16. Какое количество раундов шифра ГОСТ 28147?
- 16
- 32
- 48
- 56

17. Какова длина ключа шифра AES?
- 128, 192, 256
- 32, 48, 56
- 48, 56, 128
- 56, 128, 256

18. Стандарты блочного шифрования DES (Data Encryption Standard) и AES (Advanced Encryption Standard) имеют следующие основные режимы. Какой из них работает как самосинхронизирующийся поточный шифр?
- Режим электронной кодовой книги, ECB (Electronic Code Book).
- Режим сцепления блоков шифртекста, CBC (Ciphertext Block Chaining).
- Режим обратной связи по шифртексту, CFB (Ciphertext Feedback).
- Режим обратной связи по выходу, OFB (Output Feedback).

19. Отечественный стандарт блочного шифрования ГОСТ 28147-89 может работать в следующих режимах. Какой из них работает как синхронный поточный шифр?
- Режим простой замены
- Режим гаммирования
- Режим гаммирования с обратной связью
- Режим выработки имитовставки

20. Какой из поточных шифров является победителем Международного конкурса eSTREAM?
- Rabbit
- Sosemanuk
- HC-128
- LEXv2

14.1.2. 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

Согласована на портале № 24652

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. 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 (ТСМ). 26. Временные и частотные аналоговые скремблеры 27. Какова зависимость вероятность ошибки оптимального приема сигналов от числа позиций М? 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. 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

Согласована на портале № 24652

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. 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. 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

Согласована на портале № 24652

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. 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-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

Согласована на портале № 24652

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 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.

14.1.3. Темы опросов на занятиях

Анализ цифровых методов модуляции. Модемы сотовой связи FSK, MSKGMSK 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 избыточныекоды CRC (Cyclic redundancycheck). 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(TCM) и их анализ. Исследование сигнально-кодовой конструкции на базе системы с ортогональным частотным мультиплексированием и пространственно-временным кодированием OFDM - MIMO.

Согласована на портале № 24652

Помехоустойчивое кодирование является эффективным способом оптимизации ТКС. На практике инженеру проектировщику 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.

Теория классических шифров. Основные характеристики открытого текста. Классификацияшифров. Классификация шифровзамены. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. ШифрХилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. 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 крипто алгоритм RIJNDAEL и стандарт AES. Поточные режиме. Методы оценки качества алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммышифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализгаммы шифров. Анализ результатов тестирования. Исследование производительности шифров системы шифрования. Поточные режимы блочных шифров .Строительные блоки поточных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейнойобратной 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 шифрMICKEY-128. Поточный шифр Trivium. Российский блочный шифр ГОСТ 28147-89 в поточном режиме. Блочный шифр AES в поточном

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. Угрозысетям. Протоколы распределения ключей и их характеристики. Компрометация абонентов сети; способы построения протоколов шифрованной связи и методы их решения. Повторное использование ключей в сетях шифрованной связи. Подходы к снижению вероятности повторного использования. Современные тенденции развития средств и методов криптографической защиты информации. Программно-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 работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол. Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей

Согласована на портале № 24652

сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный Диффи-Хеллман (Diffie-Hellman), кратковременный Диффи-Хеллман, фиксированный Диффи-Хеллман иFortezza. 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 theInternet 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 распределения ключей, обеспечивающих защиту откомпрометации. Криптографические протоколы, протоколы распределения ключей, парольные системы разграничения доступа. Способы восстановления шифрованной связи после компрометации. Подходы клокализации негативных последствий компрометации. Сети связи с открытым распределением ключей. Проблемы синхронизации в сетях

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

14.1.4. Темы индивидуальных заданий

Аппаратно-программный комплекс визуализации и исследования метода свёрточного декодирования на основе последовательного алгоритма Аппаратно-программный комплекс для исследования и визуализации «КОДЕР КОДА ХЕММИНГА» Аппаратно-программный комплекс для визуализации и исследования алгоритма Витерби для декодирования сверточного кода Учебный аппаратно-программный комплекс для визуализации и исследование кодов Рида-Соломона в каналах с независимыми ошибками на базе MATLAB Учебный аппаратно-программный комплекс для визуализации и исследования алгоритма Лемпеля - Зива Учебный аппаратно-программный комплекс для визуализации и исследования кодов Боуза-Чоудхури-Хоквенгема (БЧХ) с использованием MATLAB Учебный аппаратно-программный комплекс для визуализации и исследования Турбокодов Учебный аппаратно-программный комплекс для визуализации и исследование процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView Учебный аппаратно-программный комплекс для визуализации и исследования процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView Учебный аппаратно-программный комплекс для исследования, визуализации Методы сжатия с потерей информации. Кодирование преобразований. Стандарт сжатия JPEG. Фрактальный метод Учебный аппаратно-программный комплекс для визуализации и исследования кодирования источника дискретных сообщений методом Шеннона-Фано Учебный аппаратно-программный комплекс для визуализации и исследования методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC Учебный аппаратно-программный комплекс для визуализации и исследования кодов Рида-Маллера 1. Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabVIEW Учебного аппаратно-программного комплекса для исследования и визуализации методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC Разработка программного комплекса для исследования алгоритма ассиметричного шифрования Эль-Гамаля Российский алгоритм функции хэширования ГОСТ Р 34.11-94 и его программная реализация Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ Алгоритм шифрования данных DES и его программная реализация Алгоритм ассиметричного шифрования

Согласована на портале № 24652

Диффи-Хеллмана и его программная реализация Алгоритм шифрования данных AES и его программная реализация Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabView Разработка системы обеспечения защищенного маршрутизируемого взаимодействия ViPNet OFFICE Новый российский стандарт ЭЦП ГОСТ Р 34.10-2001 и его программная реализация Алгоритм цифровой подписи RSA и его программная реализация Разработка системы обеспечения защищенного маршрутизируемого взаимодействия ViPNet CUSTOM

14.1.5. Вопросы на собеседование

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.

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.

14.1.6. Темы коллоквиумов

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. 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

Согласована на портале № 24652

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: 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

14.1.7. Темы контрольных работ

Аппаратно-программный комплекс визуализации и исследования метода свёрточного декодирования на основе последовательного алгоритма Аппаратно-программный комплекс для исследования и визуализации «КОДЕР КОДА ХЕММИНГА» Аппаратно-программный комплекс для визуализации и исследования алгоритма Витерби для декодирования сверточного кода Учебный аппаратно-программный комплекс для визуализации и исследование кодов Рида-Соломона в каналах с независимыми ошибками на базе MATLAB Учебный аппаратно-программный комплекс для визуализации и исследования алгоритма Лемпеля - Зива Учебный аппаратно-программный комплекс для визуализации и исследования кодов Боуза-Чоудхури-Хоквенгема (БЧХ) с использованием MATLAB Учебный аппаратно-программный комплекс для визуализации и исследования Турбокодов Учебный аппаратно-программный комплекс для визуализации и исследование процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView Учебный аппаратно-программный комплекс для визуализации и исследования процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView Учебный аппаратно-программный комплекс для исследования, визуализации Методы сжатия с потерей информации. Кодирование преобразований. Стандарт сжатия JPEG. Фрактальный метод Учебный аппаратно-программный комплекс для визуализации и исследования кодирования источника дискретных сообщений методом Шеннона-Фано Учебный аппаратно-программный комплекс для визуализации и исследования методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC Учебный аппаратно-программный комплекс для визуализации и исследования кодов Рида-Маллера 1. Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabVIEW Учебного аппаратно-программного комплекса для исследования и визуализации методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC Разработка программного комплекса для исследования алгоритма ассиметричного шифрования Эль-Гамаля Российский алгоритм функции хэширования ГОСТ Р 34.11-94 и его программная реализация Методы оценки качества алгоритмов

Согласована на портале № 24652

поточного шифрования и программная реализация статистических тестов НИСТ Алгоритм шифрования данных DES и его программная реализация Алгоритм ассиметричного шифрования Диффи-Хеллмана и его программная реализация Алгоритм шифрования данных AES и его программная реализация Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabView Разработка системы обеспечения защищенного маршрутизируемого взаимодействия ViPNet OFFICE Новый российский стандарт ЭЦП ГОСТ Р 34.10-2001 и его программная реализация Алгоритм цифровой подписи RSA и его программная реализация Разработка системы обеспечения защищенного маршрутизируемого взаимодействия ViPNet CUSTOM

Аппаратно-программный комплекс визуализации и исследования метода свёрточного декодирования на основе последовательного алгоритма Аппаратно-программный комплекс для исследования и визуализации «КОДЕР КОДА ХЕММИНГА» Аппаратно-программный комплекс для визуализации и исследования алгоритма Витерби для декодирования сверточного кода Учебный аппаратно-программный комплекс для визуализации и исследование кодов Рида-Соломона в каналах с независимыми ошибками на базе MATLAB Учебный аппаратно-программный комплекс для визуализации и исследования алгоритма Лемпеля - Зива Учебный аппаратно-программный комплекс для визуализации и исследования кодов Боуза-Чоудхури-Хоквенгема (БЧХ) с использованием MATLAB Учебный аппаратно-программный комплекс для визуализации и исследования Турбокодов Учебный аппаратно-программный комплекс для визуализации и исследование процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView Учебный аппаратно-программный комплекс для визуализации и исследования процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView Учебный аппаратно-программный комплекс для исследования, визуализации Методы сжатия с потерей информации. Кодирование преобразований. Стандарт сжатия JPEG. Фрактальный метод Учебный аппаратно-программный комплекс для визуализации и исследования кодирования источника дискретных сообщений методом Шеннона-Фано Учебный аппаратно-программный комплекс для визуализации и исследования методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC Учебный аппаратно-программный комплекс для визуализации и исследования кодов Рида-Маллера 1. Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabVIEW Учебного аппаратно-программного комплекса для исследования и визуализации методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC Разработка программного комплекса для исследования алгоритма ассиметричного шифрования Эль-Гамаля Российский алгоритм функции хэширования ГОСТ Р 34.11-94 и его программная реализация Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ Алгоритм шифрования данных DES и его программная реализация Алгоритм ассиметричного шифрования Диффи-Хеллмана и его программная реализация Алгоритм шифрования данных AES и его программная реализация Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabView Разработка системы обеспечения защищенного маршрутизируемого взаимодействия ViPNet OFFICE Новый российский стандарт ЭЦП ГОСТ Р 34.10-2001 и его программная реализация Алгоритм цифровой подписи RSA и его программная реализация Разработка системы обеспечения защищенного маршрутизируемого взаимодействия ViPNet CUSTOM

14.1.8. Вопросы на самоподготовку

Вопросы на самоподготовку

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.

Криптоанализ шифротекстов полученных методом гаммирования. Заданием для данной

Согласована на портале № 24652

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.

14.1.9. Вопросы для подготовки к практическим занятиям, семинарам

Модемы сотовой связи FSK, MSKGMSK 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 redundancycheck). Сверточные коды. Декодирование сверточных кодов. Декодирование сверточных кодов по методу Витерби сиспользованием ПО MATLAB. Турбокодирование. Обобщенная схема турбокодера с параллельным каскадированием. Сверточные турбокоды. Декодирование турбокодов. Характеристики помехоустойчивости сверточных турбокодов . Исследование турбокодов с использованием ПО MATLAB. Низкоплотностные коды. Классификация LDPC-кодов. Методы построения проверочных матриц. Алгоритмы декодирования низкоплотных кодов. Оценка сложности алгоритмов декодированияна базе MATLAB и LabVIEW. Исследование каскадных кодов

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

Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифровзамены. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. ШифрХилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистрсдвига 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 гаммышифров. 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.

Согласована на портале № 24652

Методэкспоненциального 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 соткрытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатиеданных. 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 работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол. Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный Диффи-Хеллман (Diffie-Hellman), кратковременный Диффи-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 сетевомуровне IPsec. IPsec является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Архитектура средств безопасности для IP-уровня специфицирована в документе Security Architecture for theInternet Protocol. Размещение и функционирование IPsec. Транспортный режим работы. Туннельный режим работы. 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 истандарты 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.

14.1.10. Темы расчетных работ

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.

Согласована на портале № 24652

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.

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.

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 модуляции.

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.

14.1.11. Темы лабораторных работ

Модемы сотовой связи FSK, MSKGMSK и численный анализ вероятности символьной

Согласована на портале № 24652

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 redundancycheck). 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. 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 ипространственно-временнымкодированием OFDM - MIMO с использованием NI LabVIEW.

Теория классических шифров. Основные характеристики открытого текста. Классификацияшифров. Классификация шифровзамены. Шифры перестановки.Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. ШифрХилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистрсдвига 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 поточныхшифров. 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 гаммышифров. 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

Согласована на портале № 24652

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 работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол. Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный Диффи-Хеллман (Diffie-Hellman), кратковременный Диффи-Хеллман, фиксированный Диффи-Хеллман и Fortezza. Алгоритмышифрования/дешифрования. Алгоритмы хэширования. Генерирование криптографических параметров. Главный секретный код. Сеансы и соединение. Протокол TLS. Генерация криптографической секретности. Функция расширения данных. Псевдослучайная функция TLS. Главный секретный код TLS. Материал для ключей TLS. Аварийный протокол в TLS. Протоколустановления 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 theInternet Protocol. Размещение и функционирование IPsec. Транспортный режим работы.Т уннельный 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

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

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14. Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Согласована на портале № 24652

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

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

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

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

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

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

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

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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

Согласована на портале № 24652