Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Галунин Сергей Александрович
Должность: проректор по учебной работе
Дата подписания: 07.07.2023 12:00:45
Уникальный программный ключ:
08ef34338325bdb0ac5a47baa5472ce36cc3fc3b

Приложение к ОПОП
«Системы мобильной связи»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)**

РАБОЧАЯ ПРОГРАММА

дисциплины

«ОСНОВЫ ПОСТРОЕНИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

для подготовки бакалавров

по направлению

11.03.02 «Инфокоммуникационные технологии и системы связи»

по профилю

«Системы мобильной связи»

Санкт-Петербург

2022

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент, к.т.н. Хачатурян А.Б.

Рабочая программа рассмотрена и одобрена на заседании кафедры РС 17.03.2022, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФРТ, 29.03.2022, протокол № 3

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФРТ
Обеспечивающая кафедра	РС
Общая трудоемкость (ЗЕТ)	3
Курс	4
Семестр	7
Виды занятий	
Практические занятия (академ. часов)	34
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	35
Самостоятельная работа, включая часы на контроль (академ. часов)	73
Всего (академ. часов)	108
Вид промежуточной аттестации	
Дифф. зачет (курс)	4

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«ОСНОВЫ ПОСТРОЕНИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

Рассматриваются методы решения основных задач, возникающих при проектировании инфокоммуникационных систем: вопросы защиты информации от несанкционированного использования, установления подлинности сообщений и абонентов, сжатия данных, помехоустойчивого кодирования. Приводятся примеры помехоустойчивых кодов, применяемых в системах связи, обсуждаются алгоритмы кодирования и декодирования, механизмы безопасности информации: системы шифрования данных, управления ключами шифрования, протоколы аутентификации сообщений и абонентов, современные методы сжатия данных.

SUBJECT SUMMARY

«THE INFORMATION AND COMMUNICATION NETWORKS DESIGN»

The course highlights the solutions of the major problems in the communication systems design, such as: the information protection from unauthorized use, the authentication messages and subscribers, data compression and error-correcting coding. Examples of error-correcting codes used in communication systems are presented. The encoding and decoding algorithms, the information security mechanisms are being discussed: data encryption, encryption key management, message authentication protocols and subscribers, modern methods of data compression.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Цели дисциплины: формирование знаний принципов построения и проектирования инфокоммуникационных систем, умений и навыков построения ее отдельных элементов.

2. Задачи дисциплины: формирование знаний, умений и навыков построения инфокоммуникационных систем в соответствии с заданными характеристиками.

3. Формируются знания требований, предъявляемых к инфокоммуникационным системам, принципов построения и проектирования инфокоммуникационных систем.

4. Вырабатываются умения сравнительной оценки различных инфоком-муникационных систем с позиций основных тактических параметров.

5. Формируются навыки анализа таких параметров открытых систем как эффективность, помехозащищенность и безопасность.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Математический аппарат радиотехники»

2. «Радиотехнические цепи и сигналы»

и обеспечивает подготовку выпускной квалификационной работы.

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	Наименование компетенции/индикатора компетенции
ПК-1	Способен к развитию коммутационных подсистем и сетевых платформ, сетей передачи данных, транспортных сетей и сетей радиодоступа, спутниковых систем связи
ПК-1.1	*Знает принципы и методы планирования и организации проведения работ по обслуживанию радиоэлектронного оборудования и радиоэлектронных систем различного назначения*
ПК-3	Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований
ПК-3.1	*Знает основы сетевых технологий, нормативно-техническую документацию, требования технических регламентов, международные и национальные стандарты в области качественных показателей работы инфокоммуникационного оборудования*
ПК-3.3	*Владеет навыками анализа оперативной информации о запланированных и аварийных работах, связанных с прерыванием предоставления услуг, контроля качества предоставляемых услуг*
ПК-5	Способен осуществлять подготовку типовых технических проектов и первичный контроль соответствия разрабатываемых проектов и технической документации на различные инфокоммуникационные объекты национальным и международным стандартам и техническим регламентам
ПК-5.1	*Знает современные технические решения создания объектов и систем связи (телекоммуникационных систем) и ее компонентов, новейшее оборудование и программное обеспечение*
ПК-5.3	*Владеет навыками оформления проектной документации в соответствии со стандартами и техническими регламентами*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Пр, ач	ИКР, ач	СР, ач
1	Введение	1		1
2	Обобщенная схема системы передачи информации	1		2
3	Информационные характеристики системы	2		4
4	Симметричные системы шифрования	3		8
5	Системы шифрования с открытым ключом	3		8
6	Аутентификация сообщений и устройств	4		8
7	Линейные блоковые коды	7		10
8	Коды БЧХ	2		8
9	Коды Рида-Соломона	2		8
10	Сверточные коды	4		8
11	Кодирование сообщений источника	4		8
12	Заключение	1	1	
	Итого, ач	34	1	73
	Из них ач на контроль	0	0	0
	Общая трудоемкость освоения, ач/зе	108/3		

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение	Информация. Виды информации. Системы передачи информации
2	Обобщенная схема системы передачи информации	Основные блоки системы передачи информации. Модели непрерывных и дискретных каналов
3	Информационные характеристики системы	Энтропия -мера количества информации. Характеристики источника. Скорость передачи и пропускная способность канала
4	Симметричные системы шифрования	Шифрование методами подстановки, перестановки, гаммирования. Примеры
5	Системы шифрования с открытым ключом	Понятие об односторонних функциях. Система RSA
6	Аутентификация сообщений и устройств	Примеры хэш-функций. Электронная подпись. Протоколы аутентификации сообщений и абонентов в системах мобильной связи

№ п/п	Наименование темы дисциплины	Содержание
7	Линейные блоковые коды	Классификация кодов, исправляющих ошибки. Параметры и способы задания линейного кода. Циклические коды. Кодирование и декодирование циклических кодов. Простейшие линейные коды. Код с простой проверкой на четность, код с повторением. Коды Хэм-минга
8	Коды БЧХ	Введение в конечные поля Галуа. Спектры циклических кодов. Этапы декодирования кодов БЧХ. Пример
9	Коды Рида-Соломона	Особенности декодирования кодов. Исправление пакетов ошибок
10	Сверточные коды	Параметры и способы задания. Принцип декодирования Витерби. Понятие о турбо-кодах
11	Кодирование сообщений источника	Метод статистического кодирования Хаффмана. Словарные методы сжатия. Кодирование с предсказанием
12	Заключение	Перспективные системы передачи информации

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Информационная характеристика системы	4
2. Обеспечение секретности передачи данных	2
3. Симметричные системы шифрования	2
4. Системы шифрования с открытым ключом	2
5. Аутентификация сообщений	4
6. Линейные блоковые коды	4
7. Циклические коды	4
8. Коды БЧХ и РС	4
9. Сверточные коды	4
10. Кодирование сообщений источника. Сжатие данных	4
Итого	34

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым

образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Самостоятельное изучение студентами теоретических основ дисциплины обеспечено необходимыми учебно-методическими материалами (учебники, учебные пособия, конспект лекций и т.п.), выполненными в печатном или электронном виде.

По каждой теме содержания рабочей программы могут быть предусмотрены индивидуальные домашние задания (расчетно-графические работы, рефераты, конспекты изученного материала, доклады и т.п.).

Изучение студентами дисциплины сопровождается проведением регулярных консультаций преподавателей, обеспечивающих практические занятия по дисциплине, за счет бюджета времени, отводимого на консультации (внеаудиторные занятия, относящиеся к разделу «Самостоятельные часы для изучения дисциплины»).

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	20
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	0
Самостоятельное изучение разделов дисциплины	0
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	23
Подготовка к контрольным работам, коллоквиумам	20
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0

Текущая СРС	Примерная трудоемкость, ач
Подготовка к зачету, дифференцированному зачету, экзамену	10
ИТОГО СРС	73

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Радиосистемы передачи информации [Текст] : учеб. пособие для вузов по специальности 201600 -”Радиоэлектрон. системы” направления 654200 -”Радиотехника” / В.А. Васин [и др.], 2005. -472 с.	27
2	Петраков, Алексей Васильевич. Защита абонентского телетрафика [Текст] : монография / А.В.Петраков, В.С.Лагутин, 2001. -499 с.	20
3	Системы мобильной связи [Текст] : Учеб. пособие для вузов по специальности 200700 ”Радиотехника” / [В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; Под ред. В.П. Ипатова], 2003. -272 с.	48
Дополнительная литература		
1	Ипатов, Валерий Павлович. Основы теории связи [Текст] : Учеб. пособие / В.П.Ипатов, И.М.Самойлов, А.Н.Смирнов, 1999. -79 с.	164
2	Сергиенко, Александр Борисович. Цифровая связь [Текст] : учеб. пособие / А. Б. Сергиенко, 2012. -163, [1] с.	23

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Центр компьютерной безопасностиhttp://csrc.nist.gov/

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/enrol/index.php?id=9636

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Основы построения инфокоммуникационных систем» формой промежуточной аттестации является дифф. зачет. Оценивание качества освоения дисциплины производится с использованием рейтинговой системы.

Дифференцированный зачет

Оценка	Количество баллов	Описание
Неудовлетворительно	0 – 10	теоретическое содержание курса не освоено, необходимые практически навыки и умения не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над курсом не приведет к существенному повышению качества выполнения учебных заданий
Удовлетворительно	11 – 15	теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки и умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки
Хорошо	16 – 20	теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки и умения сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками
Отлично	21 – 25	теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки и умения сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено количеством баллов, близким к максимальному

Особенности допуска

В течение семестра студент должен выполнить 6 практических работ и написать 2 контрольных работы

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к дифф.зачету

№ п/п	Описание
1	См. Вопросы к коллоквиумам

Образцы задач (заданий) для контрольных (проверочных) работ

Вопросы к коллоквиумам

1.1. Как осуществляется кодирование методом подстановки Виженера?

1.2. Поясните процедуру декодирования при наличии априорной информации.

1.3. Поясните процедуру декодирования с использованием частотного анализа.

1.4. Как определить фазу кода? Существуют ли случаи, когда это сделать невозможно? Почему?

2.1. Поясните процедуру получения коэффициентов рекуррентного уравнения $\Gamma(j)$.

2.2. Каким образом определить фазу $\Gamma(0)$, если известны остальные коэффициенты рекуррентной формулы?

2.3. Можно ли отнести метод гаммирования к надежным методам шифрования данных?

2.4. Как следует изменить метод гаммирования, чтобы зашифрованная с его помощью передача была надежной?

3.1. Что такое однонаправленная функция? Приведите примеры однонаправленных функций?

3.2. Поясните роль функции Эйлера в конечном n-мерном поле.

3.3. Поясните смысл ограничений, накладываемых на p и q при кодировании методом RSA. Отличаются ли они от ограничений, заложенных в лабораторной работе?

3.4. Каким образом перехватчик получает шифровки отдельных символов? Как этого избежать?

3.5. Какой вид криптоатаки используется во второй части лабораторной работы?

4.1. Какие функции выполняет электронная подпись? Каким требованиям она должна удовлетворять?

4.2. Почему CRC-код не используется в качестве хэш-функции?

4.3. Какая хэш-функция используется в лабораторной работе? Поясните принцип получения вашего хэш-значения?

4.4. Как изменить исходное сообщение так, чтобы хэш-значение не изменилось?

4.5. Как осуществляется кодирование RSA кодом открытого текста и хэш-значения?

4.6. Почему необходимо шифрование как открытого текста, так и хэш-значения?

4.7. Поясните процедуру аутентификации сообщения адресатом.

5.1. Сколько способов задания линейного кода вы знаете? Приведите эти способы для своего информационного сообщения.

5.2. Каковы исправляющая/обнаруживающая способность кода Хэмминга? Какими способами ее можно улучшить?

5.3. Поясните с помощью временных диаграмм принцип кодирования заданного информационного сообщения кодером на основе РСЛОС.

5.4. Поясните принцип синдромного декодировния. Чему равны синдромы и лидеры смежных классов для вашего задания?

5.5. С помощью временных диаграмм поясните принцип работы вычислителя синдрома на основе РСЛОС.

5.6. Были ли исправлены двухкратные и трехкратные ошибки во второй части работ? Почему?

6.1. Приведите полиномы сверточного кодера из работы. Поясните полученную в ходе работы решетчатую диаграмму кода.

6.2. Поясните принцип работы сверточного кодера.

6.3. Как определяется свободное расстояние кода по решетчатой диаграмме? Чему равно свободное расстояние, расмотренного в работе решетчатого кода?

6.4. Какова исправляющая/обнаруживающая способность рассмотренного кода?

6.5. Поясните принцип декодирования Витерби.

6.6. Каков минимальный вес ошибки, которую алгоритм Витерби не сможет исправить?

6.7. Постройте систематический эквивалент сверточного кодера из практического задания.

Контрольная работа № 1

1. В RSA криптосистеме одним из параметров открытого ключа абонента A является $nA = 55$. Предложить второй параметр eA и секретный ключ dA для абонентаA. Зашифровать открытый текст $x = 4$.

2. Что произойдет с энтропией ансамбля значений дискретной системы

ξ, если:

а) прибавить к ξ одно и то же постоянное число;

б) умножить ξ на одно и то же постоянное число;

в) подвергнуть ξ монотонному преобразованию;

г) возвести ξ в квадрат?

3. Возможно ли по каналу, имеющему информационную емкость 2 бит/симв, осуществляет передачу со скоростью R = 2,5 бит/симв и вероятностью ошибки декодирования pe = 0,05?

Контрольная работа № 2

1. В векторном пространстве *VF*, состоящем из всех 6-ти компонентных двоичных векторов, выбраны следующие четыре представителя: (100101), (010111), (110011), и (000001). Какова размерность пространства *VF*, содержащего указанные вектора?

2. Изобразить вычислитель синдрома на основе линейного регистра сдвига для циклического (7,3) кода с порождающим полиномом . Привести состояние регистра сдвига, определить полином синдрома и осуществить исправление ошибок для наблюдаемой комбинации Y = (1010010).

3. Построить код Шеннона-Фано для ансамбля из 6-ти состояний с вероятностями, равными 0,3; 0,3; 0,2; 0,1; 0,06 и 0,04 соответственно. Может ли существовать для данного ансамбля лучший код?

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
1	Введение Обобщенная схема системы передачи информации Информационные характеристики системы Симметричные системы шифрования Системы шифрования с открытым ключом Аутентификация сообщений и устройств	
2		
3		
4		
5		
6		Коллоквиум
7	Линейные блоковые коды	
8		
9		
10		Контрольная работа
11	Коды БЧХ Коды Рида-Соломона	
12		
13		Коллоквиум
14	Сверточные коды Кодирование сообщений источника	
15		
16		
17		Коллоквиум
18	Заключение	Контрольная работа

6.4 Методика текущего контроля

на практических (семинарских) занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий), выполнение 6 практических работ и написание 2 контрольных работ, по результатам которых студент получает допуск на диф. зачет. Практические работы защищаются на коллоквиумах (по 2 работы на 3-х коллоквиумах). Контрольные работы состоят из 3 теоретических вопросов.

Контрольные и защита практических работ оцениваются по 4-х-балльной системе:

5 - правильные ответы на все вопросы,

4 - ответы на все вопросы с незначительными погрешностями,

3 - правильные ответы не на все вопросы или ответы на все вопросы с

существенными ошибками,

2 - отсутствие ответов или ответы с грубыми ошибками.

Результирующая оценка промежуточной аттестации (диф. зачета) формируется как среднее арифметическое оценок за коллоквиумы и контрольные работы с округлением в пользу студента. При наличии неудовлетворительных оценок общая оценка - неудовлетворительно.

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Практические занятия	Аудитория	Количество рабочих мест -в соответствии с контингентом, рабочее место преподавателя, маркерная доска.	
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА