Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем »

РАБОЧАЯ ПРОГРАММА

по дисциплине

«М 1.2.4 Основы теории кодирования и шифрования в современных РТС»

направления подготовки

«11.04.02 Инфокоммуникационные технологии и системы связи»
Профиль 1 «*Инфокоммуникационные технологии и системы связи*»

форма обучения – очная
курс – 2
семестр – 1
зачетных единиц – 3
часов в неделю – 2
всего часов – 108,
в том числе:
лекции – 7
коллоквиумы – 2
практические занятия – 27
самостоятельная работа – 72
зачет – 3 семестр

1. Цели и задачи дисциплины

Целью курса является дать студентам основные понятия и представления из теории структуры сигналов с рассмотрением математических моделей сигналов, рассмотреть методы кодирования и передачи информации по каналам связи с оптимальной скоростью и с учетом создаваемых помех.

В результате изучения студенты должны знать основные понятия из теории информации и криптографии, а также уметь определять количество информации в сообщении и осуществлять оптимизацию кодирования сообщения с повышением надежности передачи сообщения.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Основы теории кодирования и шифрования в современных РТС» является дисциплиной вариативной части профессионального цикла дисциплин ФГОС ВО по направления подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи».

Дисциплина «Основы теории кодирования и шифрования в современных РТС» в учебном плане связана с дисциплиной «Цифровая обработка сигналов и защита информации».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способностью к разработке методов формирования и обработки сигналов, систем коммутации синхронизации и определению области эффективного их использования в инфокоммуникационных сетях, системах и устройствах (ПК-4);
- способностью разрабатывать прогрессивные методы технической эксплуатации инфокоммуникационных систем, сетей и устройств (ПК-6)

Студент должен знать:

- основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды;
- понятие энтропии как меры неопределенности состояния объекта, помехоустойчивости и связи ее с избыточностью сигналов;
- основные результаты о кодировании при наличии и отсутствии шума;
- основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи;
- основные криптографические методы управления информационной безопасностью.

Студент должен уметь:

- оценивать сложность алгоритмов и вычислений;
- вычислять теоретико-информационные характеристики источников сообщений и каналов связи;
- пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач;
- решать типовые задачи кодирования и декодирования;
- осуществлять оптимизацию кодирования сообщения в каналах связи без помех и повышать надежность передачи сообщения в каналах с помехами;
- использовать криптографические методы и средства защиты информации в автоматизированных системах.

Студент должен владеть:

- навыками применения математического аппарата для решения прикладных теоретико-информационных задач;
- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- **навыками использования ЭВМ в анализе простейших**
- навыками пользования библиотеками прикладных программ для решения прикладных математических задач.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	2	3	4	5	6	7		8	9
3 семестр									
1	1-4	1	Основы теории информации.	8/2	2			6/2	
1	5-8	2	Передача информации, каналы связи.	28/6	2/2			6/4	20

2	9 - 12	3	Основы теории помехоустойчивого кодирования.	38/4	2/2			6/2	30
2	13 - 18	4	Методы защиты информации. Элементы криптографии.	34/4	1	2		9/4	22
Всего				108/ 16	7/4	2		27/12	72

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	Основы теории информации. Источники сообщений, количество информации, энтропия. Кодирование источника. Взаимная информация.	1-10
2	2	2	Передача информации, каналы связи. Пропускная способность канала. Теоремы кодирования для канала. Расчет пропускной способности некоторых каналов.	1-10
3	2	3	Основы теории помехоустойчивого кодирования. Введение в блоковые коды. Линейные блоковые коды. Циклические коды. Коды Боуза–Чоудхури–Хоквингема и Рида-Соломона. Введение в сверточные коды. Исправление пакетов ошибок.	1-10
4	1	4	Аутентификация сообщений и устройств.	1-10

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	2	3	4	5
4	2	1	Методы защиты информации. Элементы криптографии. Системы шифрования с секретным и открытым ключами.	1-10

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое

				обеспечение
1	**2**	**3**	**4**	**5**

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	**2**	**4**	**3**
1	**6**	Блочное кодирование.	**1-10**
2	**6**	Построение кодов Шеннона-Фано и Хаффмана.	**1-10**
3	**6**	Избыточные коды.	**1-10**
4	**9**	Реализация системы шифрования с открытым ключом	**1-10**

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	**2**	**3**	**4**
2	20	Марковские и эргодические источники информации (2, 3, 4)	**1-10**
3	16	Циклические коды. Порождающие многочлены. Линейные пространства.	**1-10**
3	14	Линии связи с помехами: двоичные симметричные линии, m-ичные симметричные линии. Симметричные линии со стиранием	**1-10**
4	22	Симметричные и асимметричные алгоритмы шифрования. Проблема генерации ключей.	**1-10**

Виды, график контроля СРС, (по решению кафедры УМКС/УМКН).

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
5 семестр			
1-2	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация)
3-4	Работа с печатными источниками,	Рубежный контроль, промежуточный	Зачет

	разбор типовых заданий	контроль, самоконтроль	

10. Расчетно-графическая работа

Учебным планом не предусмотрена

11. Курсовая работа

Учебным планом не предусмотрена

12. Курсовой проект

Учебным планом не предусмотрена

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Текущий контроль усвоения знаний по дисциплине «Основы теории кодирования и шифрования в современных РТС» осуществляется в течение семестра в ходе учебного процесса и консультирования студентов, по результатам выполнения аудиторных самостоятельных проверочных работ, контрольной работы и активного участия в проведении занятия в интерактивной форме.

Основными формами текущего контроля знаний являются:

- решение проблемных задач в области теории информации и кодирования;
- участие в обсуждении актуальных вопросов, связанных с развитием отечественной и зарубежной индустрии в области противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты, в проведении занятия в интерактивной форме;
- собеседование по теоретическим вопросам;
- выполнение аудиторных самостоятельных работ, лабораторных работы, обсуждение и анализ их результатов.

Промежуточная аттестация (зачет) проводится в письменной форме в виде ответов на вопросы билета.

Оценка знаний студентов осуществляется в баллах с учетом:

- оценки за работу в семестре;
- оценки итоговых знаний в ходе зачета.

Оценка знаний студентов реализуются следующим образом

Требования к результатам освоения дисциплины	Оценка или зачет
Глубокое усвоение или твердое усвоение программного материала, связанное со знанием закономерностей процесса кодирования и передачи информации по каналам связи	Зачет

Незнание значительной части программного материала, неумение сформулировать правильные ответы на вопросы, невыполнение практических заданий в течение семестра.	Незачет

Вопросы для зачета

1. Энтропия. Энтропия как мера неопределенности состояния объекта.
2. Зависимость величины энтропии от распределения вероятностей состояния системы.
3. Энтропия дискретных систем. Основные свойства энтропии. Единицы измерения.
4. Физический смысл двоичной единицы энтропии. Энтропия объединения зависимых и независимых систем.
5. Условная энтропия. Принцип экстремума энтропии. Экстремальные свойства некоторых законов распределения
6. Распространение понятия энтропии на непрерывные системы
7. Количество информации. Количество информации по Хартли.
8. Статистический подход Шеннона к понятию количества информации
9. Основные свойства количества информации. Единицы измерения.
10. Основные характеристики источников информации и информационных систем.
11. Дискретный источник без памяти.
12. Пропускная способность канала связи. Помехоустойчивость, эффективность и надежность информационной системы.
13. Понятие избыточности информации. Количественное определение избыточности.
14. Введение в блоковые коды. Линейные блоковые коды.
15. Циклические коды. Коды Боуза–Чоудхури–Хоквингема и Рида-Соломона.
16. Введение в сверточные коды. Исправление пакетов ошибок.
17. Связь помехоустойчивости с избыточностью информации.
18. Теория структуры сигнала. Сигнал как материальный носитель и средство отображения информации.
19. Элементы криптографии.
20. Системы шифрования с секретным и открытым ключами.
21. Аутентификация сообщений и устройств.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВПО в рамках учебного курса предусмотрены активные

и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

Общее количество занятий, проводимых в интерактивных формах, не менее 16 часов.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Алешин Л. И. Информационные технологии : учеб. пособие / Л. И. Алешин. - М. : Маркет ДС, 2011. - 384 с. : ил. ; 21 см. - (Университетская серия). - Библиогр.: с. 379-383. - ISBN 978-5-94416-136-9 (22 экз.)
2. Скляров О.К. Волоконно-оптические сети и системы связи : учеб. пособие / О. К. Скляров. - 2-е изд., стер. - СПб. ; М. ; Краснодар : Лань, 2010. - 272 с. : ил. ; 24 см. - (Учебники для вузов. Специальная литература). - Библиогр.: с. 254-261 (189 назв.). - Имеется электрон. аналог печ. изд. - ISBN 978-5-8114-1028-6 (31 экз.)
3. Гашков С. Б. Криптографические методы защиты информации : учеб. пособие / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - М. : ИЦ "Академия", 2010. - 304 с. : ил. ; 22 см. - (Высшее профессиональное образование). - Библиогр.: с. 287-294 (157 назв.). - Гриф: допущено УМО по классич. университет. образованию в качестве учеб. пособия для студ. вузов, обуч. по напр. "Прикладная математика и информатика" и "Информационные технологии". - Имеется электронный аналог печатного издания. - ISBN 978-5-7695-4962-5 (17 экз.)

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Бройдо В. Л. Вычислительные системы, сети и телекоммуникации : учеб. пособие / В. Л. Бройдо, О. П. Ильина. - 3-е изд. - СПб. [и др.] : Питер, 2008. - 766 с. : ил. ; 24 см. - (Учебное пособие). - Библиогр.: с. 756-759 (72 назв.) . - Гриф: допущено М-вом образования и науки РФ в качестве учеб. пособия для студ. вузов, обучающихся по спец. "Прикладная информатика" и "Информ. системы в экономике". - ISBN 978-5-91180-754-2
5. Златопольский Д. М. Программирование: типовые задачи, алгоритмы, методы / Д. М. Златопольский. - М. : БИНОМ. Лаборатория знаний,

2007. - 223 с. : ил. ; 25 см. - Библиогр.: с. 219 (12 назв.). - ISBN 978-5-94774-461-3

ПЕРИОДИЧЕСКИЕ ИЗДАНИЯ

6. Информационная безопасность регионов [Текст] : науч.-техн. журнал. - Саратов : Изд-во СГСЭУ, 2007 - . - Выходит раз в два месяца. - ISSN 1995-5731
7. Информационные ресурсы России [Текст] : науч.-практ. журнал. - Выходит раз в два месяца. - ISSN 0204-3653

ИНТЕРНЕТ-РЕСУРСЫ

8. Основы теории информации [Электронный ресурс] / В.В. Панин. - Москва : БИНОМ, 2012. - . - ISBN 978-5-9963-0759-3 http://www.studentlibrary.ru/book/ISBN9785996307593.html
9. Мировые информационные ресурсы [Электронный ресурс] / А.В. Коротков. -Москва:МГИМО,2012.-.- ISBN 978-5-9228-0806-4 http://www.studentlibrary.ru/book/ISBN9785996307593.html
10. Защита компьютерной информации [Электронный ресурс] : эффективные методы и средства : учеб. пособие / В. Ф. Шаньгин. - Электрон. текстовые дан. - М. : Изд-во ДМК Пресс, 2010. http://lib.sstu.ru/index.php/elmrazdel/melellib/3321-elreselibonline.

16. Материально-техническое обеспечение

Для реализации образовательной программы подготовки магистра по направлению подготовки *«Инфокоммуникационные технологии и системы связи»*, имеется материально-техническая база, обеспечивающая проведение всех видов занятий по дисциплине «*Основы теории кодирования и шифрования в современных РТС*», включая лекционные и практические занятия, которая соответствует действующим санитарным и противопожарным правилам и нормам.

Для преподавания дисциплины предоставляется оснащенная современным проекционным оборудованием лекционная аудитория и компьютерные классы.

В компьютерном классе установлено по 15 персональных компьютеров, объединенных в локальную сеть с автоматическим выходом в корпоративную сеть СГТУ и глобальную сеть Интернет. Все персональные компьютеры оснащены лицензионным ПО Microsoft Windows, Microsoft Office.

Для пользования электронными изданиями и информационно-обучающей средой (ИОС) СГТУ во время самостоятельной подготовки студентам предоставляются рабочие места в библиотеке СГТУ.