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

Кафедра «Радиоэлектроника и телекоммуникации»

РАБОЧАЯ ПРОГРАММА

по дисциплине
«М.1.3.4.2 Цифровая обработка сигналов и защита информации»

направления подготовки
«11.04.02 Инфокоммуникационные технологии и системы связи»
Профиль 2 «Радиофизические и оптические системы связи»

форма обучения – заочная
курс – 2
семестр – 3
зачетных единиц – 6
всего часов – 216,
в том числе:
лекции – 4
практические занятия – 28
лабораторные занятия – 10
самостоятельная работа – 174
зачет – нет
экзамен – 3 семестр
РГР – нет
курсовая работа – 3 семестр
курсовой проект – нет

1. Цели и задачи дисциплины

Цель преподавания дисциплины: теоретическое и практическое освоение методов и средств цифровой обработки сигналов (ЦОС), формирование у студентов представлений по основным методам криптографической обработки данных для их защиты от несанкционированных действий, а также выработка практических навыков работы в области обработки сигналов цифровыми устройствами и защиты информации в компьютерных системах.

Задачи изучения дисциплины: подготовка специалиста, способного самостоятельно применять методы математического моделирования и криптографической защиты систем цифровой обработки и передачи информации.

2. Место дисциплины в структуре ООП ВО

Дисциплина входит в вариативную часть образовательной программы магистра (направление "Инфокоммуникационные технологии и системы связи"). Дисциплина основывается на умениях и компетенциях, приобретенных студентами при изучении дисциплин: "Дискретная математика", "Физика", "Информатика", "Цифровая обработка сигналов". Для изучения данной дисциплины студент должен знать основные законы физики и электротехники, быть знаком с основами информатики и цифровой техники, иметь навыки самостоятельной работы с компьютером.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-3: способность осваивать современные и перспективные направления развития ИКТиСС;

ПК-8: готовность использовать современные достижения науки и передовые инфокоммуникационные технологии, методы проведения теоретических и экспериментальных исследований в научно-исследовательских работах в области ИКТиСС.

Студент должен знать: физические и математические основы преобразования сигналов при цифровой обработке; математические алгоритмы цифровой фильтрации и спектрально-корреляционного анализа сигналов; методы синтеза цифровых фильтров; защиты информации при создании и использовании распределенных корпоративных информационных систем, методам и алгоритмам криптографической зашиты (симметричным и асимметричным алгоритмам шифрования, функциям хэширования, электронной цифровой подписи, аутентификации и управления криптографическими ключами).

Студент должен уметь: составлять техническое задание на проектирование устройства или системы ЦОС; принимать решения по разработке криптографических средств защиты информации; применять современные методы и средства защиты информации. Уметь творчески применять и самостоятельно углублять полученные знания.

Студент должен владеть: методами ЦОС; методами защиты информации.

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

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	2	3	4	5	6	7	8	9	10
2 семестр									
1	1	1	Предмет курса. Математическое представление сигналов.	2					2
1	1	2	Особенности спектров периодического сигнала и сигнала конечной длины. Дискретизация непрерывных сигналов, заданных на бесконечном интервале.	10					10
1	2	3	Спектр дискретизованного сигнала при его периодическом продолжении. Периодические явления.	10					10
2	3	4	Восстановление сигнала при его дискретном задании. Применение теоремы отсчетов для полосовых сигналов.	12			2		10
2	3	5	Конечное дискретное преобразование Фурье и его свойства.	10					10
2	4	6	Особенности спектрального анализа на основе КДПФ. Временные и спектральные окна.	16			2	4	10
2	4	7	Принципы построения алгоритма БПФ с прореживанием по времени.	10					10
3	5	8	Дискретный комплексный сигнал со свойствами аналитического и его применения.	10					10
3	5	9	Цифровые фильтры.	10					10
3	6	10	Методы ЦОС: перенос и инверсия спектра, формирование	16			2	4	10

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	2	3	4	5	6	7	8	9	10
			сигналов с одной боковой несущей, интерполяция, децимация.						
3	7	11	Основные понятия и модель криптосистемы с секретными ключами Простейшие методы шифрования.	14				4	10
3	8	12	Вскрытие несовершенного шифра. Достоверность и обман. Требования к криптосистемам.	14				4	10
3	9	13	Стандарт шифрования данных с секретными ключами: алгоритм шифрования DES, общие применения.	14				4	10
4	10	14	Шифрование с открытыми ключами. Односторонние функции и открытое распространение ключей. Алгоритм RSA.	20	2		4	4	10
4	11	15	Общие требования безопасности к алгоритму RSA. Криптосистема Эль-Гамаля. Управление ключами.	16	2			4	10
4	12	16	Основные принципы аутентификации. Процедура простой аутентификации Строгая аутентификация: исходные положения.	16					16
4	12	17	Способ цифровой подписи информации, процедура извлечения общедоступного ключа пользователя.	916					16
Всего				**216**	**4**		**10**	**28**	**174**

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
10	0,5	1	Симметричное шифрование. Алгоритм шифрования AES.	1-6

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
10	0,5	1	Области применения симметричного шифрования.	1-6
10	0,5	2	Назначение программного обеспечения "TryeCrypt".	1-6
10	0,5	2	Несимметричное шифрование. Шифрование с открытыми ключами.	1-6

6. Содержание коллоквиумов

(не предусмотрено учебным планом)

7. Перечень практических занятий

№ темы	Всего часов	Наименование практической работы. Задания, вопросы, отрабатываемые на занятии	Учебно-методическое обеспечение
1	2	3	4
6	4	Дискретизация и восстановление непрерывных сигналов	1-6
10	4	Исследование низкочастотной дискретизации сигналов.	1-6
11	4	Симметричное шифрование в архиваторах.	1-6
12	4	Способы шифрования в "TrueCrypt".	1-6
13	4	Асимметричное шифрование.	1-6
14	4	Исследование метода кодирования сообщений с использованием алгоритма RSA.	1-6
15	4	Исследование криптографической защиты (PGP и GnuPG) сообщений в почтовых программах.	1-6

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	3	4
4	2	Введение. Лабораторная станция "NI ELVIS".	1-6
6	2	Ограничение полосы частот канала и восстановление цифровых сигналов.	1-6
10	2	Исследование метода PCM-TDM передачи данных.	1-6
14	4	Спектральный анализ сигналов с DSBSC модуляцией	1-6

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение

1	2	3	4
1	2	Предмет курса. Математическое представление сигналов.	1-6
2	10	Особенности спектров периодического сигнала и сигнала конечной длины. Дискретизация непрерывных сигналов, заданных на бесконечном интервале.	1-6
3	10	Спектр дискретизованного сигнала при его периодическом продолжении. Периодические явления.	1-6
4	10	Восстановление сигнала при его дискретном задании. Применение теоремы отсчетов для полосовых сигналов.	1-6
5	10	Конечное дискретное преобразование Фурье и его свойства.	1-6
6	10	Особенности спектрального анализа на основе КДПФ. Временные и спектральные окна.	1-6
7	10	Принципы построения алгоритма БПФ с прореживанием по времени.	1-6
8	10	Дискретный комплексный сигнал со свойствами аналитического и его применения.	1-6
9	10	Цифровые фильтры.	1-6
10	10	Методы ЦОС: перенос и инверсия спектра, формирование сигналов с одной боковой несущей, интерполяция, децимация.	1-6
11	10	Основные понятия и модель криптосистемы с секретными ключами Простейшие методы шифрования.	1-6
12	10	Вскрытие несовершенного шифра. Достоверность и обман. Требования к криптосистемам.	1-6
13	10	Стандарт шифрования данных с секретными ключами: алгоритм шифрования DES, общие применения.	1-6
14	10	Шифрование с открытыми ключами. Односторонние функции и открытое распространение ключей. Алгоритм RSA.	1-6
15	10	Общие требования безопасности к алгоритму RSA. Криптосистема Эль-Гамаля. Управление ключами.	1-6
16	16	Основные принципы аутентификации. Процедура простой аутентификации Строгая аутентификация: исходные положения.	1-6
17	16	Способ цифровой подписи информации, процедура извлечения общедоступного ключа пользователя.	1-6

10. Расчетно-графическая работа

(не предусмотрено учебным планом)

11. Курсовая работа

Тема работы: "Проектирование нерекурсивных цифровых фильтров". При выполнении курсовой работы студенты проводят анализ задания, изучают способы расчета коэффициентов нерекурсивных цифровых фильтров с использованием конечного дискретного преобразования Фурье и исследуют характеристики фильтра.

Индивидуальные варианты, содержащие задания для курсовой работы, выдаются каждому студенту.

Курсовая работа содержит 15–30 страниц пояснительной записки, содержащих расчеты, алгоритмы, программы, чертежи и графики на листах стандартных форматов. Работа сдается в электронном виде (приказ по СГТУ от 28.02.2011 г. № 207-П).

12. Курсовой проект

(не предусмотрено учебным планом)

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

В процессе освоения образовательной программы формируются следующий перечень компетенций: ОПК-3, ПК-8.

Типовые контрольные задания, необходимые для оценки знаний:

- Импульсная характеристика системы.
- Z-преобразование.
- Свертка дискретных сигналов.
- Проектирование КИХ фильтров.
- Преобразование Гильберта.
- Прямой цифровой синтез частот.
- Коды Хэмминга. Линейные коды.
- Циклические коды.
- Сверточное кодирование.
- Методы защиты данных при преднамеренных воздействиях.
- Модель криптосистемы с секретными ключами.
- Симметричное шифрование. Алгоритм шифрования DES.
- Алгоритм шифрования AES.
- Области применения симметричного шифрования.
- Несимметричное шифрование.
- Алгоритм Диффи-Хеллмана.
- Алгоритм шифрования RSA.
- Области применения криптосистемы RSA.

Вопросы для экзамена

1. Обобщенная схема цифровой обработка сигналов (ЦОС). Области применения ЦОС.
2. Способы и методы проектирования устройств ЦОС.
3. Математическое описание сигнала. Примеры дискретных сигналов.
4. Основная полоса частот. Эффект подмены частот в ЦОС.
5. Прямое и обратное преобразования Фурье.
6. Прямое и обратное дискретные преобразования Фурье.

7. Спектры аналоговых и дискретных сигналов.
8. Спектры периодических и непериодических сигналов.
9. Свойства спектров сигналов. Эффект наложения спектров.
10. Низкочастотная дискретизация финитных сигналов.
11. Z-преобразование. Свойства Z-преобразования.
12. Импульсная характеристика системы. Свертка дискретных сигналов.
13. Фильтр с конечной импульсной характеристикой (КИХ).
14. Фильтр с бесконечной импульсной характеристикой (БИХ).
15. Структурные схемы рекурсивных и нерекурсивных фильтров.
16. Расчет рекурсивного ФНЧ Бесселя 2-го порядка.
17. Проектирование нерекурсивных цифровых фильтров.
18. Преобразование Гильберта.
19. Синтезаторы частот с прямым и косвенным синтезом.
20. Прямой цифровой синтез частот (DDS). Структуры DDS.
21. Методы защиты данных при случайных воздействиях. Коды Хэмминга. Линейные коды.
22. Циклические коды.
23. Сверточное кодирование.
24. Методы защиты данных при преднамеренных воздействиях.
25. Модель криптосистемы с секретными ключами.
26. Симметричное шифрование. Алгоритм шифрования DES.
27. Симметричное шифрование. Алгоритм шифрования AES.
28. Области применения симметричного шифрования.
29. Назначение программного обеспечения "TryeCrypt".
30. Несимметричное шифрование. Шифрование с открытыми ключами.
31. Односторонние функции и открытое распространение ключей. Алгоритм Диффи-Хеллмана.
32. Алгоритм шифрования RSA.
33. Области применения криптосистемы RSA.
34. Назначение программного обеспечения "PGP" и "GnuPG".
35. Криптосистема Эль-Гамаля.
36. Управление ключами.
37. Аутентификация сообщений.
38. Управление сертификатами.

14. Образовательные технологии

По курсу «Цифровая обработка сигналов и защита информации» при выполнении лабораторных работ используется программное обеспечение: NI "LabVIEW" совместно с лабораторными станциями "NI ELVIS II+".

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Рябко, Б. Я. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / Рябко Б. Я. - Москва : Горячая линия - Телеком, 2012. - 229 с.
   Режим доступа: http://www.iprbookshop.ru/11994
2. Аверченков, В. И. Методы и средства инженерно-технической защиты информации [Электронный ресурс] : учебное пособие / Аверченков В. И. - Брянск : Брянский государственный технический университет, 2012. - 187 с.
   Режим доступа: http://www.iprbookshop.ru/7000
3. Рябко, Б. Я. Основы современной криптографии и стеганографии [Текст] : монография / Рябко Б. Я. - Москва: Горячая линия - Телеком, 2010. - 232с.
   Режим доступа: http://www.iprbookshop.ru/12018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Оппенгейм А. Цифровая обработка сигналов [Электронный ресурс] : учебное пособие / Алан Оппенгейм. - Москва : Техносфера, 2012. - 1048 с.
   Режим доступа: http://www.iprbookshop.ru/26906
5. Дворкович, В. П. Оконные функции для гармонического анализа сигналов [Текст] / Дворкович В. П. - Москва : Техносфера, 2014. - 112 с.
   Режим доступа: http://www.iprbookshop.ru/31874
6. Радиотехнические цепи и сигналы. Том 2 [Электронный ресурс] : учебное пособие. - Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2010 - .Радиотехнические цепи и сигналы. Том 2 / Астайкин А. И. - 2010. - 360 с.
   Режим доступа: http://www.iprbookshop.ru/18445

16. Материально-техническое обеспечение

Межфакультетская научно-образовательная лаборатория информационно-коммуникационных систем (лаб. 2/211а). В лаборатории имеется специализированная учебная мебель, мультимедиа, 15 ПК с выходом в Интернет.

Информационное и учебно-методическое обеспечение – электронная библиотека вуза, электронная информационно – образовательная среда.

Лицензионное программное обеспечение: NI "Circuit Design Suite", NI "LabVIEW" для лабораторных станций "NI ELVIS II+".

Студенты проводят расчеты на ЭВМ при обработке результатов лабораторных и практических занятий, выполнении самостоятельной работы.