

Министерство образования Республики Беларусь

Учреждение образования
"БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ"

УТВЕРЖДАЮ
Проректор по учебной работе
и социальным вопросам
_____ А.А. Хмыль
" _19_ " _____ 05 _____ 2014 г.

ПРОГРАММА

вступительного экзамена в магистратуру по специальности
1-98 80 03 «Аппаратное и программно-техническое обеспечение
информационной безопасности»

Минск 2014

Программа составлена на основании типовых учебных программ дисциплин «Цифровая обработка сигналов», «Цифровые и микропроцессорные устройства», «Теория кодирования и основы криптологии», «Методы и устройства приема и обработки сигналов» специальности I 39 01 04 «Радиоэлектронная защита информации» и дисциплины «Структурная и функциональная организация вычислительных машин» специальности I 40 02 01 «Вычислительные машины, системы и сети».

СОСТАВИТЕЛИ:

Малевич Игорь Юрьевич – доктор технических наук, профессор, заведующий кафедрой радиотехнических систем БГУИР;

Левкович Василий Николаевич – кандидат технических наук, доцент, доцент кафедры радиотехнических систем БГУИР.

Программа рассмотрена и рекомендована к утверждению на заседании кафедры радиотехнических систем Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники (протокол № 9 от 19.05.2014 г.)

Заведующий кафедры РТС

И.Ю. Малевич

СОДЕРЖАНИЕ ПРОГРАММЫ

В основу программы положены следующие вузовские дисциплины: «Цифровая обработка сигналов», «Цифровые и микропроцессорные устройства», «Теория кодирования и основы криптологии», «Методы и устройства приема и обработки сигналов», «Структурная и функциональная организация вычислительных машин».

Раздел 1. ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ

Общая структура системы цифровой обработки сигналов (ЦОС). Области применения и возможности ЦОС. Дискретные, цифровые сигналы и системы. Методы описания дискретных сигналов и систем. Разновидности дискретных систем. Преобразование сигналов в системах цифровой обработки. Дискретные преобразования: Фурье, Уолша, Карунена-Лоэва. Многоскоростные преобразования сигналов. Методы и алгоритмы вычисления дискретных сверток. Спектральный и корреляционный анализ дискретных сигналов и процессов. Анализ случайных дискретных сигналов. Спектральный анализ нестационарных сигналов. Методы и алгоритмы фильтровой цифровой обработки сигналов. Цифровые частотные фильтры. Цифровая обработка сигналов на основе модели случайного процесса. Оптимальные фильтры обработки цифровых сигналов. Адаптивная цифровая фильтрация сигналов. Слепая обработка сигналов в системах идентификации. Цифровые системы распознавания объектов и явлений.

Раздел 2. ЦИФРОВЫЕ И МИКРОПРОЦЕССОРНЫЕ УСТРОЙСТВА

Законы, аксиомы и правила алгебры логики. Электронные ключи на транзисторах. Логические элементы. Цифровые устройства комбинационного типа. Формирователи импульсов. Автоколебательные и ждущие мультивибраторы. Генераторы пилообразного напряжения. Системы счисления. Кодирование чисел. Типовая структура микрокомпьютера. Назначение функциональных блоков микропроцессора. Организация чтения/записи, ввода/вывода информации в микрокомпьютере. Циклы работы микропроцессора. Структура и формат команды. Понятие алгоритма. Этапы программирования. Методы цифроаналогового преобразования. Аналого-цифровые преобразователи. сигналов. Отображение информации в микропроцессорных системах. Схемотехника программируемых логических интегральных схем (ПЛИС), архитектура, организация ввода-вывода, программирование и конфигурирование. Проектирование блоков цифровых устройств в ПЛИС. Комбинационная логика, элементы цифровой техники, память. Интерфейсные решения. HDL-проектирование и моделирование схем цифровых устройств. VHDL-описание и реализация схем цифровых устройств. Моделирование с помощью VHDL-описаний. Функциональные тесты. Схемы программирования и конфигурирования ПЛИС.

Раздел 3. ТЕОРИЯ КОДИРОВАНИЯ И ОСНОВЫ КРИПТОЛОГИИ

Задачи кодирования и защиты информации в системах и устройствах. Кодирование источников информации. Теоремы Шеннона. Алгоритмы эффективного кодирования. Помехоустойчивое кодирование информации. Модели каналов передачи информации при наличии помех. Линейные коды: методы кодирования и декодирования. Циклические коды: методы кодирования и декодирования. Кодирование и исправление ошибок на основе алгебры конечных полей. Сверточные и турбо-коды. Прикладные коды: итеративно декодируемые коды, корреляционные коды, комбинирование кодов и цифровой модуляции. Базовые концепции безопасности электронных систем. Криптографические модели защиты. Криптографические системы. Поточные криптосистемы. Блочные криптосистемы. Методы криптоанализа блочных криптосистем. Асимметричные криптосистемы с открытым ключом. Криптоанализ асимметричных систем защиты информации. Защита электронного взаимодействия. Электронная цифровая подпись, сигнатуры и аутентификация сообщений. Криптографические протоколы. Системы управления криптографическими ключами. Стеганографические методы скрытой передачи или хранения информации. Методология построения систем защиты информации.

Раздел 4. МЕТОДЫ И УСТРОЙСТВА ПРИЕМА И ОБРАБОТКИ СИГНАЛОВ

Радиоприемные тракты, основные параметры. Общие сведения о радиоприемных трактах. Помехи радиоприему и методы борьбы с ними. Устройства согласования и предварительной селекции в радиоприемных трактах. Усилители радиосигналов. Преобразователи частоты. Демодуляторы приемных трактов. Устройства управления и регулирования в радиоприемных трактах. Особенности построения радиоприемных трактов различного назначения. Характеристики и параметры ЭМС радиоприемных устройств. Адаптация в интересах обеспечения ЭМС.

Раздел 5. СТРУКТУРНАЯ И ФУНКЦИОНАЛЬНАЯ ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, СИСТЕМ И СЕТЕЙ

Понятие об архитектуре вычислительной машины. Классификация микропроцессоров по назначению. Сигнальные микропроцессоры: области применения, особенности архитектуры, системы команд, портов ввода-вывода, основные характеристики. ПС-контроллеры: области применения, особенности архитектуры, системы команд, портов ввода-вывода, основные характеристики. Проблемы и методы организации подсистем ввода-вывода. Понятие о многомашинных и многопроцессорных вычислительных системах и комплексах. Особенности организации отказоустойчивых многопроцессорных вычислительных комплексов. Типы структур многопроцессорных вычислительных систем, ориентированных на достижение сверхвысокой производительности. Конвейерно-векторные суперЭВМ. Концепция

вычислительной системы с управлением потоком данных. Классификация вычислительных сетей. Методы передачи данных по каналам связи. Коммутация каналов, сообщений и пакетов. Эталонная логическая модель вычислительной сети и иерархия протоколов. Элементы протоколов. Протоколы управления физическим и информационным каналами и сетью передачи данных. Локальные вычислительные сети. Особенности организации передачи информации в локальных сетях. Методы доступа к моноканалу. Информационно-управляющие локальные сети.

Литература

1. Оппенгейм, А. Цифровая обработка сигналов/ А. Оппенгейм, Р. Шафер. -М.: Техносфера, 2006.
2. Основы цифровой обработки сигналов: Курс лекций/Авторы: А.И. Солонина, Д.А. Улахович, С.М. Арбузо, Е.Б. Соловьева, И.И. Гук. - СПб.: БХВ - Петербург, 2003.
3. Солонина, А.И. Цифровая обработка сигналов. Моделирование в MATLAB/А. И. Солонина, С. М. Арбузов. – СПб.: БХВ-Петербург, 2008. –816с.
4. Айфичер, Э. С. Цифровая обработка сигналов: практический подход/ Э. С. Айфичер, Б. У. Джервис. – М.: Вильямс, 2008.
5. Лайонс, Р. Цифровая обработка сигналов/ Р Лайонс.. М.: ООО «Бином-Пресс», 2006.г.
6. Глинченко, А.С. Цифровая обработка сигналов: Учеб. пособие в 2 Ч/ А.С. Глинченко.-Красноярск.: Изд-во КГТУ, 2001. -199 с.
7. Методы цифровой обработки сигналов/ Под ред. Ю.В. Гуляева, В.Ф. Кравченко .- М.: Радиотехника, 2003.
8. Куприянов, М.С., Матюшкин Б.Д. Цифровая обработка сигналов: процессы, алгоритмы, средства проектирования. – СПб.: Политехника, 2002.
9. Шахтарин, Б.И. Случайные процессы в радиотехнике. Т.1. Линейные преобразования.-М.:Гелиос АРВ,2006.
10. Цифровая обработка сигналов и изображений в радиофизических приложениях/Под ред В.Ф.Кравченко. – М.: ФИЗМАТЛИТ, 2007. – 544 с.
11. Угрюмов Е.П. Цифровая схемотехника: Учеб. пособие для вузов. - СПб: ХВ-Петербург, 2004. – 528с.
12. Новиков Ю.В. Основы цифровой схемотехники. М.: Мир, 2001. – 379 с. Электроника /Под ред. Ю.А. Быстрова – СПб.: Энергоатомиздат, 1996.
13. Сергеев Н.Р., Вашкевич Н.Р. Основы вычислительной техники: Учеб. пособие для вузов. - М.: Высш. шк., 1988. – 311 с.
14. Гусев В.Г. Электроника и микропроцессорная техника: Учебник для вузов.-М.:Высш.шк., 2004.-790 с.
15. Сташин В.В. и др. Проектирование цифровых устройств на однокристалльных микроконтроллерах/ В.В. Сташин, А.В. Урусов, О.Ф. Мологонцева. - М.: Энергоатомиздат, 1990.

16. Соловьев В.В. Проектирование цифровых устройств на основе программируемых логических интегральных схем. – М.: Горячая линия-Телеком, 2001. – 636 с.
17. Суворова Е.А., Шейнин Ю.Е. Проектирование цифровых систем на VHDL. СПб, БХВ-С.-Петербург, 2003, 576 с.
18. Угрюмов Е. П. Цифровая схемотехника. СПб.: БХВ, 2000, 528 с.
19. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2006. – 288 с.
20. Морелос–Сарагоса Р. Искусство помехоустойчивого кодирования. Методы алгоритмы, применение. Учебное пособие. - – М.: Техносфера, 2005. – 320 с.
21. Теория информации и кодирование/ Самсонов Б.Б., Плохов Е.М., Филоненков А.И., Кречет Т.В. Учеб пособие – Ростов на Дону : Феникс,2002.- 208 с.
22. Фомичев. В. М. Дискретная математика и криптология. – М.: Диалог – МИФИ, 2003
23. Куприянов, А. И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений/ А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М. : Издательский центр «Академия», 2006.
24. Румянцев К. Е. Прием и обработка сигналов. –М.: Издательский центр «Академия», 2004. - 528 с.
25. Чердынцев В.А., И.Ю. Малевич, А.Е. Курочкин. Методы и устройства приема и обработки радиосигналов. – Мн: БГУИР, 2010.
26. Пятибратов А.П. и др. Вычислительные машины, сети и телекоммуникации. - М.: Финансы и статистика, 2001.
27. Гук М. Аппаратные средства IBM PC: Энциклопедия. – СПб.: Питер, 2000.
28. Эрглис К.Э. Интерфейсы открытых систем.– М.: Горячая линия – Телеком, 2000.
29. Нанс Б. Компьютерные сети: Пер. с англ. - М.: Бином. 1995.