Номер модуля	**Название модуля**	**Доцент(ы)**
PTI 812	Основы информатики	КГФИ, Г.Сабирова, М.Борубаев

Направление: Информатика (бакалавр) **Специальность:** Все	**Семестр:** 1 семестр(зим.сем.) с продолжением на 2 семестре (летн. сем.) **Кредиты ECTS:** 8 **Рабочая нагрузка в ч.:** 240 **Учебные формы и формы обучения в ч:** Лекция 120 (8 СНЧ) Подготовка и обработка материала/ Самостоятельная работа 120

Цели обучения

Получение знаний по математическим основам числовых форматов, информационной теории и кодировании. Студенты должны знать существенные риски, которым подвергаются системы информационной технологии и возможности их предотвращения.

Математические основы информатики: Студенты обладают важнейшими математическими основами представления числовых форматов, а так же методов кодирования. Они в состоянии оценить технические кодирования относительно их применения. При компьютерных расчетах правильно распределять вытекающие проблемы точности на основе теоретических знаний цифровых систем.

Логика: Студенты обучаются распознавать, что наряду с решением проблемы путем программирования в некоторых случаях возможны так же схемные решения.
Они будут знакомы с логическими функциями и смогут их применять. Благодаря знаниям о действующих для логических ценностях правилах вычисления, они смогут правильно переформулировать логические выражения. Они смогут использовать существующие аналогии между логическими выражениями и схемными представлениями для преобразования.
Они ознакомятся с принципом, сначала найти предварительную реализацию и применить метод для улучшения этой реализации.

Защита информации: Студенты должны знать информационно-техническую угрозу безопасности и с помощью современных методов кодирования и цифровых сигнатур должны уметь применять для защиты информации предназначенные криптографические методы.

Содержание обучения

Математические основы информатики (Лекция: 30 ч., Подготовка и обработка материала: 30 ч., Самостоятельная работа: 30 ч.)

- Основы теории информации, элементарный запас, решающая вместимость, энтропия, избыточность.
- Кодирование и ее технически-практическая реализация
- Одно и многошаговые коды
- Защита кода, коды, определяющие ошибки, и коды, исправляющие ошибки
- Геометрическая интерпретация кодового пространства, дистанции разрядов
- Оптимизация кода
- Системы счисления, представление чисел, системы позиционных значений
- Конверсия чисел, арифметические операции, отрицательное представление чисел
- Представление фиксированной запятой, представление плавающей запятой

- Проблема точности, ошибки округления

Логика (лекции: 30 h, практика: 15 h, подготовка и обработка материала: 60 h, самостоятельная работа: 15 h)

- Булева алгебра
- Однозначные функции, двузначные функции, многозначные функции, правила вычисления для работы с булевыми переменными
- Дизъюнктивные нормальные формы, комбинаторные схемы и их минимизация
- Минимизация с использованием KV-представления, минимизация по Quine / Mc Cluskey, учет don't care-условий, замечания к минимизации коньюнктивных нормальных форм
- Контактные схемы
- Примеры о комбинаторных схемах
- Последовательные схемы
- Тригерный каскад
- Анализ и синтез последовательных схем
- Числитель и регистр

Защита информации (лекция: 30 ч., подготовка и обработка материала: 30 ч., самостоятельная работа: 30 ч.)

- Основы, понятия, виды нападения, угрозы
- Кодирование, классические методы, блочные и электрические шифры
- Симметричное кодирование, DES, AES, выработка кодирования, способы производства
- Асимметричное кодирование, проблема кодового распределения, RSA, метод Diffie Hellman
- Hash-функции, MD5, SHA-1, MAC
- Цифровые сигнатуры, сертификаты
- Pretty Good Privacy
- Кодовое управление, уничтожение
- Аутентификация, классы служб аутентификации, Challenge- Response-метод, методы стандартного пароля, One-Time-Pad-методы

Литература

Лысенко В.В., Малинин Л.А., Беляев М.А, Основы информатики: Учебник для вузов, Неоглори, 2006,294
Кузнецов А.А., Алатова Х.В. Основы информатики, Дрофа, 2002,176
Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии.- М: Горячая линия — а Телеком, 2002.-175
Герасименко В.А. Защита информации в автоматических системах обработки данных, М: Энергоатомиздат,1994
Козлова М. Основы криптографически защищенной системы менеджмента информации. М: МО,1996
Конхейм А.Г. Основы криптографи. М: Радио и коммуникация, 1987

Предварительные знания
Никакие

Контроль успеваемости:
Вид: Контрольная работа **Продолжительность:** 90 мин.

Оценивается по: Матем. основы 50%

	Защита информ.	50%
Logik	40%	
	Mathematische Grundlagen	30%
	Informationssicherheit	30%

Предварительные работы: никакие

Разработано: 17.01.09/01.04.10 Проф.Шварц

Проф. Ленк / КГФИ