«Математические основы защиты информации»
(на 72 часа)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Обеспечение информационной безопасности является одной из важнейших государственных задач наряду с развитием экономики, образования и здравоохранения.

Курс «Математические основы защиты информации» посвящен изучению ***информационной безопасности*** (науки, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере) и ***криптографии*** (науки, занимающейся разработкой методов преобразования информации с целью обеспечения ее конфиденциальности, целостности и аутентификации), теории сложности вычислений и математических основ криптографии.

Цели курса: формирование профессиональных навыков, связанных с организацией системы обеспечения информационной безопасности с помощью шифрования данных, изучение алгоритмов шифрования и дешифрования, общих подходов к криптоанализу зашифрованной информации; создание представления о современных методах обработки, преобразования и защиты информации в современных компьютерных системах; о современных способах борьбы с несанкционированным блокированием, доступом, копированием, изменением и сбором информации; развитие способностей к логическому и алгоритмическому мышлению, навыков использования методов и алгоритмов эксплуатации программных систем сбора, закрытия, восстановления и аутентификации информации.

Задачи курса: обучение студентов основам информационной безопасности и криптографии, теории сложности вычислений; изучение математических проблем, на базе которых построены основные криптосистемы; совершенствование у студентов навыков и умений разработки и реализации алгоритмов; развитие искусства работы в пакете Mathematica.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

№ п/п	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов
1	**Основы теории чисел и криптографии.** Элементы теории групп, колец и полей. Кольцо классов вычетов по модулю m. Числовые сравнения и их свойства. Функция Эйлера. Теоремы Эйлера и Ферма. Платформы шифрования. Модулярная арифметика. Простейшие шифры.	2л 2п
2	**Введение в теорию сложности вычислений и основные алгоритмы теории чисел.** Полиномиальный, субэкспоненциальный и экспоненциальный алгоритмы. Алгоритм Евклида, расширенный алгоритм Евклида, возведение в степень в кольце классов вычетов.	2л 2п

	Вычисление обратных элементов в мультипликативной группе Zn*.	
3	**Генерирование больших простых чисел.** Решето Эратосфена. Малая теорема Ферма. Псевдопростые числа. Числа Кармайкла. Свидетели простоты. Вероятностный тест на простоту Миллера-Рабина. Гипотеза Римана. Детерминированный полиномиальный алгоритм проверки простоты чисел. Детерминированный и недетерминированный алгоритмы. Алгоритмы с нулевой, односторонней и двусторонней ошибками.	2л 2п
4	**Факторизация чисел. Экспоненциальные и субэкспоненциальные алгоритмы.** Китайская теорема об остатках. Метод пробных делений. Ро-метод Полларда. Классы P и NP. Факторизация Ферма и факторные базы. Метод Диксона. Метод квадратичного решета.	2л 2п
5	**Криптосистемы с открытым ключом. Криптосистема RSA.** Криптосистемы с открытым ключом. Односторонние функции. Криптосистема RSA.	2л 2п
6	**Симметричные криптоалгоритмы.** Сети Фейстеля. Основные понятия криптоанализа, Линейный и дифференциальный криптоанализ. Алгоритмы DES и тройной DES. Советский и российский стандарт шифрования ГОСТ 28147-89 «Магма». Блочный шифр ГОСТ Р 34.12-2015 «Кузнечик».	2л 2п
7	**Рюкзачные криптосистемы.** Задача о рюкзаке. Задача о рюкзаке с быстрорастущим вектором. Рюкзачная криптосистема Меркля-Хеллмана. Алгоритм Шамира.	2л 1п
8	**Функции хеширования.** Хеш-функции. Коллизии. Алгоритм вычисления контрольной суммы. Криптографические хеш-функции. СТБ 34.101.312007.	2л 1п
9	**Дискретное логарифмирование.** Определение дискретного логарифма. Первообразный корень. Алгоритм больших и малых шагов. Алгоритм Полига-Хеллмана.	2л 2п
10	**Криптосистема Эль-Гамаля.** Криптосистема Эль-Гамаля. Обмен ключами Диффи-Хеллмана.	2л 1п
11	**Электронная цифровая подпись.** Электронная цифровая подпись. Подпись Эль-Гамаля. Аутентификация Шнорра. Электронная цифровая подпись Шнорра. Электронная цифровая подпись СТБ 1176.2-99.	2л 2п

12	**Криптосистема Рабина.** Криптосистема Рабина. Квадратичный вычет. Критерий Эйлера. Символ Лежандра. Алгоритм извлечения квадратного корня в кольце классов вычетов.	2л 1п
13	**Эллиптические кривые.** Основные понятия и определения. Теорема Хассе. Алгоритм вычисления произведения натуральных чисел с точками эллиптической кривой. Вычисление порядка группы точек эллиптической кривой над конечным полем.	2л 1п
14	**Криптография на эллиптических кривых.** Криптосистемы на эллиптических кривых. Электронная цифровая подпись ГОСТ Р 34.10-2001. Аналог ключевого обмена Диффи-Хеллмана.	2л 1п
15	**Введение в информационную безопасность.** Основные понятия информационной безопасности. Методы информационной безопасности. Сервисы информационной безопасности. Угрозы информационной безопасности. Каналы утечки информации. Неформальная модель нарушителя. Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности. Классификация криптографических методов защиты информации.	2л 1п
16	**Идентификация и аутентификация.** Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации. Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма. Протокол Kerberos. Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.	2л 2п
17	**Протоколирование и аудит**. Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге». Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.	2л 1п
18	**Компьютерные вирусы.** Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов. Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские	2л 1п

	кони, логические бомбы. Технологии маскировки вирусов. Тенденции современных компьютерных вирусов. Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов. Развертывание системы антивирусной защиты.	
19	**Средства защиты сети.** Межсетевые экраны. Виртуальные частные сети. Системы обнаружения вторжений. Анализ защищенности системы.	2л 1п
20	**Средства и методы противодействия угрозам доступности информации**. Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности. Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя. Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.	2л 1п
21	**Основные принципы построения систем защиты**. Меры противодействия угрозам безопасности. Принципы построения систем защиты. Понятие и назначение модели безопасности. Модель дискреционного доступа. Модель Белла-ла-Падулы. Ролевая модель контроля доступа. Системы разграничения доступа	2л 1п
	ИТОГО:	42л + 30п = 72 часа

Составитель: к.ф.-м.н., доц. Кайгородов Е. В.

Стоимость обучения:
72 часовой курс – 4500 р.*
42 часовой курс – 2500 р.*

*** При наборе группы не менее 10 человек.**