Программа полугодового курса
«Основы теории информации и криптографии»
для нового направления подготовки бакалавров ММФ НГУ
«Математика и компьютерные науки»

к.ф.-м.н. Н.Н.Токарева

Программа лекций

1. Введение в теорию информации. Источники информации, методы преобразования непрерывного сигнала в цифровую форму. Теорема дискретизации Котельникова.

2. Модели источников сообщений. Подходы к измерению сложности сообщения. Понятие энтропии, ее свойства.

3. Передача сообщений по каналу связи с искажением. Линейные коды. Оценки скорости кодирования. Коды Хэмминга. Циклические коды.

4. Теорема Шеннона о скорости кодирования. Коды с малой плотностью проверок на четность, достигающие оценку теоремы Шеннона.

5. Методы сжатия информации. Сжатие без потерь. Код Хаффмана. Арифметическое кодирование. Словарные методы. Сжатие с потерями. Формат JPEG. Обзор современных архиваторов.

6. Задачи хранения информации. Вопросы надежности и отказоустойчивости носителей информации. RAID-массивы.

7. Основные задачи криптографии. Вероятностная модель шифрсистемы. Полная избыточность языка сообщений и избыточность на букву сообщения. Теоремы Шеннона об избыточности языка сообщений, о числе ложных ключей, о совершенной секретности.

8. Блочные и поточные шифры. Сеть Фейстеля и SP-сети. Методы построения основных компонентов симметричных шифров.

9. Криптографические свойства булевых функций. Корреляционная и алгебраическая иммунность. Теоремы Зигенталера. Теоремы о максимально нелинейных функциях.

10. Псевдослучайные последовательности. Теорема о периоде линейной рекуррентной последовательности. Алгоритм Берлекэмпа-Месси. Оценка его эффективности.

11. Статистические методы криптоанализа. Линейный и дифференциальный методы. Теорема о надежности статистического метода криптоанализа шифра.

12. Методы асимметричной криптографии. Основные криптосистемы с открытым ключом (RSA, ElGamal и др.).

13. Задачи факторизации и проверки простоты числа. Методы криптоанализа асимметричных шифров.

14. Методы кодирования, хранения и передачи информации в цифровой сотовой связи и беспроводных сетях. Система безопасности GSM. Шифрование WEP и WPA. Методы представления, обработки и передачи информации на различных уровнях моделей сетевых протоколов OSI/ISO и TCP/IP.

Программа семинаров и лабораторных работ

1. Кодирование источников данных. Свойства энтропии. Определение избыточности языка сообщений. (Решение задач)

2. Кодирование и декодирование с помощью линейных кодов. Определение параметров кода. Свойства кода Хэмминга. Конструкции циклических кодов. Построение кодов с малой плотностью проверок на четность. (Решение задач)

3. Сжатие данных с помощью различных методов. Оценка стоимости кодирования. (Решение задач)

4. Реализация методов сжатия данных с потерями. Восстановление информации. (Лабораторная работа в компьютерном классе)

5. Вычисление расстояния единственности шифра. Оценка числа ложных ключей для конкретных шифров. Проверка шифра на совершенную секретность. (Решение задач)

6. Свойства булевых функций. Построение алгебраической нормальной формы булевой функции. Построение конечных полей характеристики 2. Свойства следа из поля в простое подполе. Решение задач, связанных с нахождением трейс-формы булевой функции. (Решение задач)

7. Определение корреляционной и алгебраической иммунности булевой функции. Свойства нелинейности булевой функции. (Решение задач)

8. Анализ и проверка последовательности на случайность. (Лабораторная работа в компьютерном классе)

9. Построение линейного генератора псевдослучайной последовательности с помощью алгоритма Берлекэмпа-Месси. (Лабораторная работа в компьютерном классе)

10. Реализация одного из методов симметричного шифрования. (Лабораторная работа в компьютерном классе)

11. Проведение линейного/дифференциального криптоанализа блочного шифра. (Решение теоретической задачи + лабораторная работа в компьютерном классе)

12. Криптосистемы RSA, ElGamal и др. Формирование электронной подписи. Решение теоретико-числовых задач, связанных с определением простоты числа и задачей факторизации. (Решение задач)

Программу семинаров можно расширить, как в пользу решения теоретических задач, так и в пользу практики в компьютерном классе.

Литература

В курсе используется литература, изданная, в основном, в недавнее время (2000-е годы).

- **Учебные пособия и монография автора по теме курса:**

1. Токарева Н.Н., *Симметричная криптография. Краткий курс*, Новосибирский государственный университет, Новосибирск, 2012, ISBN: 978-5-4437-0067-0, 234 с.

2. Токарева Н.Н., *Нелинейные булевы функции: бент-функции и их обобщения*, LAP LAMBERT Academic Publishing, Saarbrucken, Germany, 2011, ISBN: 978-3-8433-0904-2, 180 с.

3. Городилова А.А., Токарева Н.Н., Шушуев Г.И. *Криптография и криптоанализ. Сборник задач*, Новосибирский государственный университет, Новосибирск, 2014, 325 с.

- **Основные источники:**

1) Материалы международных конференций по теории информации и криптографии: ISIT, EUROCRYPT, CRYPTO, FSE, ASIACRYPT, SIBECRYPT, BFCA и др.
2) Агибалов Г.П. *Избранные теоремы начального курса криптографии* // учеб. пособие, Томск: Томский государственный университет, 2005.
3) Айфичер Э., Джервис Б. *Цифровая обработка сигналов: практический подход* // М.:Вильямс, 2004. 992 с. ISBN 5-8459-0710-1.
4) Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. *Основы криптографии: Учебное пособие* // М.: Гелиос АРВ, 2005. 480 с.
5) Ватолин Д., Ратушняк А., Смирнов М., Юкин В. *Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео* // М.: ДИАЛОГ-МИФИ, 2002. 384 с.
6) Колесник В., Полтырев Г. *Курс теории информации* // М.: Наука, 1982.
7) Логачёв О. А., Сальников А. А., Ященко В. В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2004. 470 с. ISBN 5-94057-117-4.
8) Moon T. K., *Error Correction Coding, Mathematical Methods and Algorithms*. Wiley, ISBN 0-471-64800-0. 2005.
9) Маховенко Е. Б. *Теоретико-числовые методы в криптографии* // М.: Гелиос АРВ, 2006. 320 с. ISBN 5-85438-143-5.
10) Рябко Б. Я., Фионов А. Н. *Основы современной криптографии и стеганографии* // М.: Горячая линия-Телеком, 2010. 232 с. ISBN 978-5-9912-0150-6.
11) Скляр Б. *Цифровая связь. Теоретические основы и практическое применение* // М.:Вильямс, 2007. 1104 с. ISBN 978-5-8459-0497-3
12) Сэломон Д. *Сжатие данных, изображений и звука* // М.: Техносфера. 2004. 368 с. ISBN 5-94836-027-X.
13) Фомичёв В. М. *Дискретная математика и криптология. Курс лекций* // М.: Диалог-МИФИ, 2003. 400 с. ISBN 5-86404-185-8.
14) Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. *Математические и компьютерные основы криптологии: Учебное пособие* // Минск: Новое знание, 2003. 382 с. ISBN 985-475-016-7.
15) Черемушкин А. В. *Лекции по арифметическим алгоритмам в криптографии* // М.: МЦНМО, 2002. 104 с. ISBN 5-94057-060-7.
16) Шеннон К. *Работы по теории информации и кибернетике* // М.: Издательство иностранной литературы, 1963. 832 с.

Аннотация полугодового курса
«Основы теории информации и криптографии»
для нового направления подготовки бакалавров ММФ НГУ
«Математика и компьютерные науки»

к.ф.-м.н. Н.Н.Токарева

Курс посвящен основам современной теории информации и криптографии. В него входят такие направления, как

- обработка непрерывной информации; методы дискретизации;
- основы теории информации (измерения количества информации, сложности сообщений, особенности источников данных);
- методы помехоустойчивого кодирования (особенно исследующиеся в последние, 2000-е, годы методы линейного кодирования, достигающие оптимальной оценки по скорости);
- методы сжатия информации (без потерь и с потерями; изложение теоретических основ и разбор современных архиваторов);
- задачи хранения информации (надежность и отказоустойчивость, RAID-массивы);
- криптография и криптоанализ (теоретические и практические результаты, новые направления исследований последнего десятилетия);
- псевдослучайные последовательности; статистические методы их анализа;
- методы хранения, обработки и передачи информации в цифровой сотовой связи, беспроводных сетях; представление информации на различных уровнях сетевых протоколов.

Курс совмещает изложение строгих математических результатов (и их доказательств) с практическими результатами внедрения методов теории информации в конкретные системы и протоколы. Цель курса – дать студентам базовые знания по основным направлениям современной теории информации. В состав курса кроме лекций входят семинарские занятия (с решением теоретических задач) и лабораторные работы в компьютерном классе. Будет сформулирован также ряд исследовательских задач студентам, интересующимся специализацией в данной области.

Подобрана группа семинаристов. Все они имеют успешный опыт преподавания, публикации, ведут научные исследования в области теории информации и криптографии, в том числе совместные исследования с лабораторией компьютерной безопасности и криптографии COSIC (Бельгия), широко известной по разработке многих мировых криптографических стандартов.