СПИСОК ЛИТЕРАТУРЫ:

1. *Брейсуэлл Р.* Преобразование Хартли. М.: Мир, 1990.
2. *Иваненко В. Г.* Интерполяция цифровых сигналов на основе сдвинутого дискретного преобразования Хартли. М. Препринт МИФИ 005-89. 1989.

REFERENCES:

1. *Braycuell R.* Preobrazovanie Khartli. M.: Mir, 1990.
2. *Ivanenko V. G.* Interpolyatsiya tsifrovyh signalov na osnove sdvinutogo diskretnogo preobrazovaniya Khartli. M. Preprint MEPhI 005-89. 1989.

A. V. Epishkina

History of Cryptology for Students

Key words: cryptology, history, subject matter

The purpose of the work was to show the main aspects of the subject matter named "History of Cryptology" lectured to the first term students of the Cybernetics and Information Security Department of National Research Nuclear University "MEPhI". The major problems that arose in face of the lecturer were described. The general topics of the curriculum were demonstrated in the article.

А. В. Епишкина

О ПРОГРАММЕ ДИСЦИПЛИНЫ «ИСТОРИЯ КРИПТОЛОГИИ»

На факультете «Кибернетика и информационная безопасность» Национального исследовательского ядерного университета «МИФИ» для студентов 1-го курса, специализирующихся по кафедре «Криптология и дискретная математика», с 2013/2014 учебного года введена дисциплина «История криптологии». Автором разработана учебная программа, проводятся лекционные занятия.

Задачами изучения данной дисциплины первоначально являлись ознакомление студентов с историей науки, которой им предстоит заниматься, наглядная демонстрация применения криптографических примитивов, а также роли успешного криптографического анализа в исторических событиях [1—3]. Однако практика показала, что одного экскурса в историю недостаточно. Для формирования у студентов, вчерашних выпускников школ, целостного взгляда на изучаемую науку необходимо привлечение математических основ криптологии. По вопросам, которые задают слушатели, становится ясно, что их интересует не столько цель, достигаемая при помощи криптографических методов, сколько сущность применяемых методов, интересен ответ на вопрос, как же удается достичь тех или иных результатов. И здесь возникает непростая задача, которую должен решить преподаватель. С одной стороны, исторический обзор, безусловно, должен читаться на 1-м курсе, дабы с самого начала обучения построить необходимую основу, на которую будут опираться все дальнейшие знания. С другой стороны, студенты не обладают требуемой математической подготовкой, позволяющей разобраться с конструкцией тех или иных криптографических примитивов.

В большей степени всё вышесказанное относится к асимметричной криптографии, так как для ее изучения необходимо знать определения и свойства основных алгебраических объектов.

Однако проблема с недостаточностью квалификации студентов возникает не только в области математических дисциплин. В частности, при изложении раздела, связанного с квантовой криптографией, преподаватель сталкивается с тем, что и знаний по физике у слушателей недостаточно.

Автор считает, что, несмотря на упомянутые сложности, возникающие при изложении материала, нельзя сужать рассматриваемую область и при необходимости следует восполнять недостающие сведения.

Далее кратко охарактеризуем основные разделы дисциплины «История криптологии».

Раздел 1. Криптология и защита информации. Криптология: понятие, содержание, этимология. Основные задачи, решаемые криптографией: обеспечение конфиденциальности информации, целостности информации, аутентификации информации и неотказуемости от авторства. Строгие математические определения шифра, зашифрования, расшифрования и дешифрования. Шифры замены и перестановки. Краткая историческая ретроспектива развития способов защиты тайных посланий: физическая, стеганографическая и криптографическая защита информации. Организация секретной связи на основе симметричной шифрсистемы. Организация секретной связи на основе асимметричной шифрсистемы.

Раздел 2. Донаучная криптография. Возникновение криптографии. Способы составления шифрованного письма в древних цивилизациях Индии, Египта и Месопотамии. Развитие криптографических методов в Древней Греции и Спарте. Приборы для шифрования: сцитала и таблица Энея. Шифр Цезаря и квадрат Полибия. Криптография в период расцвета арабских государств. Происхождение слова «шифр». Зарождение методов частотного анализа встречаемости букв текста. Криптография в эпоху Возрождения. Шифровальный диск Альберти и его особенности. Методы усложнения шифров, работы Белазо и Арженти. Решетка Кардано. Таблица Вижинера. Книжные шифры. Эпоха «черных кабинетов» и ее влияние на развитие криптографии. Номенклаторы. Шифратор Джефферсона. Шифровальные устройства Уодсворта и Уитстона. Колесные шифраторы: шифрующие диски Хеберна, Коха, Шербиуса и Дамма. «Энигма»: особенности устройства и роль в исторический событиях Второй мировой войны.

Раздел 3. Криптография в России. Азбуки, лежащие в основе отечественного шифрования. Шифры XVII в.: «простая литорея», «мудрая литорея» и «тайнопись в квадратах». Тарабарский язык. Посольские приказы и развитие криптографии. Шифры, используемые Петром I и Екатериной I. Агентурные шифры простой замены. Шифры 30-х годов XVIII в.: алфавит, слоги, суплемент, счеты и месяцы. «Черные кабинеты» в России и успехи дешифровальщиков. Цифирные азбуки. Биграммные и биклавный шифры.

Раздел 4. Криптография и совершенные шифры. Доклад Шеннона «Математическая теория криптографии». Концепции теоретической и практической стойкости. Моделирование языка открытых сообщений. Избыточная информация. Понятия совершенной секретности и рабочей характеристики шифра. Вклад Колмогорова и Маркова в развитие криптографии. Шифр Вернама и его свойства. Первый стандарт шифрования данных DES (Data Encryption Standard). Принцип Керкгоффса.

Раздел 5. Асимметричная криптография. Работа Диффи и Хеллмана «Новые направления в криптографии». Криптография с открытым ключом. Однонаправленные функции и однонаправленные функции с секретом. Криптосистема RSA. Шифрсистема Эль Гамаля.

Раздел 6. Современные криптографические алгоритмы. Шифр «Люцифер». Шифр DES. Сеть Фейстеля. Российский стандарт на алгоритм шифрования ГОСТ 28147-89. Стандарт шифрования США AES (Advanced Encryption Standard). Электронная подпись: определение и особенности применения. Схема электронной подписи Эль Гамаля. Случайные числа и их применение в криптографии.

Раздел 7. Квантовая криптография. Принцип неопределенности Гейзенберга. Квантовые каналы связи. Задачи квантовой криптографии. Протокол открытого распределения ключей по квантовому каналу и его анализ.

Приведенная программа дисциплины «История криптологии», с одной стороны, достаточно полно охватывает основные исторические факты, позволяющие говорить о становлении криптологии как науки, с другой стороны, дает базовые математические основы для дальнейшего изучения криптографических примитивов и протоколов и отражает современный уровень развития криптологии.

СПИСОК ЛИТЕРАТУРЫ:

1. *Бабаш А. В., Шанкин Г. П.* История криптографии. Ч. I. М.: Гелиос АРВ, 2002.
2. *Русецкая И. А.* История криптографии в Западной Европе в раннее Новое время. СПб.: Центр гуманитарных инициатив. Университетская книга — СПб., 2014.
3. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2001.

REFERENCES:

1. *Babash A. V., Shankin G. P.* Istoriya kriptografii. Chast' I. M.: Gelios ARV, 2002.
2. *Rusetskaya I. A.* Istoriya criptographii v Zapadnoi Evrope v rannee Novoe vremya. SPb.: Centr gumanitarnyh initsiativ. Universitetskaya kniga — SPb., 2014.
3. *Alferov A. P., Zubov A. U., Kuz'min A. S., Cheremushkin A. V.* Osnovy kriptorgafii: Uchebnoe posobie. M.: Gelios ARV, 2001.

A. V. Epishkina, S. A. Kiryakina

The Possibility of Using Simulation Systems for the Development of a High-speed Encipherer

Key words: encipherer, model, simulation modelling

The paper presents the investigation of a possibility of using simulation systems for the development of a high-speed encipherer. The systematization of methods for constructing a high-speed encipherers and techniques to simulate network processes was done and the choice of General Purpose Simulation System (GPSS) as the modeling system was established. The main result of the work was the conclusion allowed to utilize simulation modelling to construct a high-speed encipherer.

А. В. Епишкина, С. А. Кирякина

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СИСТЕМ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ РАЗРАБОТКИ ВЫСОКОСКОРОСТНОГО ШИФРАТОРА

Жизнь современного общества трудно представить без повсеместного применения информационных технологий. Массовое использование компьютеров позволяет решать задачу автоматизации обработки