№ 3854

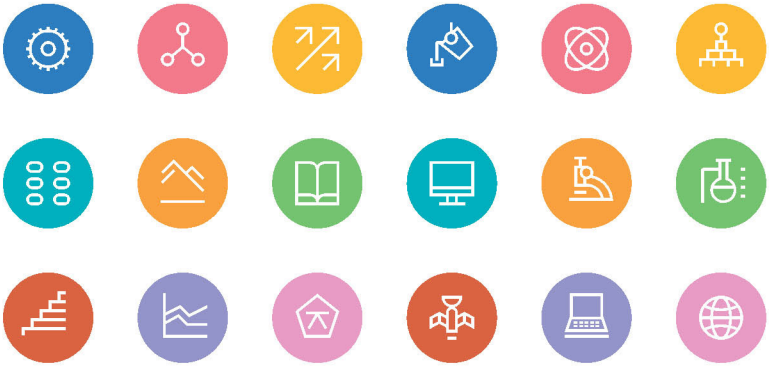
МИСиС
Национальный исследовательский технологический университет

Л.Е. Бахаров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

(разделы криптография и стеганография)

Практикум



STORE.MISIS.RU

УДК 621.38:004.056
Б30

Рецензент
канд. техн. наук, доц. *А.О. Аристов*

Бахаров Л.Е.

Б30 Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л.Е. Бахаров. – М. : Изд. Дом НИТУ «МИСиС», 2019. – 59 с.

ISBN 978-5-906953-94-0

В практикуме рассмотрены вопросы применения криптографических алгоритмов с открытым и секретным ключом, требования к криптографическим хэш-функциям и средствам формирования электронной подписи. Даются основы стеганографических алгоритмов применительно к вопросам защиты интеллектуальной собственности путем внедрения цифровых водяных знаков.

Предназначен для студентов, обучающихся по направлению подготовки 09.03.02 «Информационные системы и технологии», может быть использован студентами других направлений и специальностей.

УДК 621.38:004.056

ISBN 978-5-906953-94-0

СОДЕРЖАНИЕ

Практическая работа 1

ШИФР ВИЖЕНЕРА

Цель работы: изучение симметричных полиалфавитных шифров на примере шифра Виженера.

Шифр Виженера – это разновидность наиболее известных в криптографии шифров замены или подстановки, особенностью которых является замена символов (или слов, или других частей сообщения) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста. Различают *одноалфавитную* и *многоалфавитную* замену.

Одноалфавитные шифры достаточно легко вскрываются с помощью частотного анализа (учет частоты появления отдельных букв и их сочетаний в данном языке).

Примером многоалфавитного шифра замены является так называемая система Виженера. Система Виженера впервые была опубликована в 1586 г. и является одной из старейших и наиболее известных многоалфавитных систем. Впервые этот метод описал в своей книге Джован Баттиста Беллазо в 1553 г., однако в XIX в. получил имя Блеза Виженера, французского дипломата XVI в., который развивал и совершенствовал криптографические системы.

Система Виженера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Виженера. Каждая строка таблицы представляет собой символы используемого алфавита с циклическим сдвигом на n позиций. Таблица представляет собой квадратную матрицу размерностью $n \times n$, где n – число символов используемого алфавита. На рис. 1.1 показана таблица Виженера для русского языка (алфавит состоит из 32 букв и пробела). Первая строка содержит все символы алфавита. Каждая следующая строка получается из предыдущей циклическим сдвигом последней на символ влево.

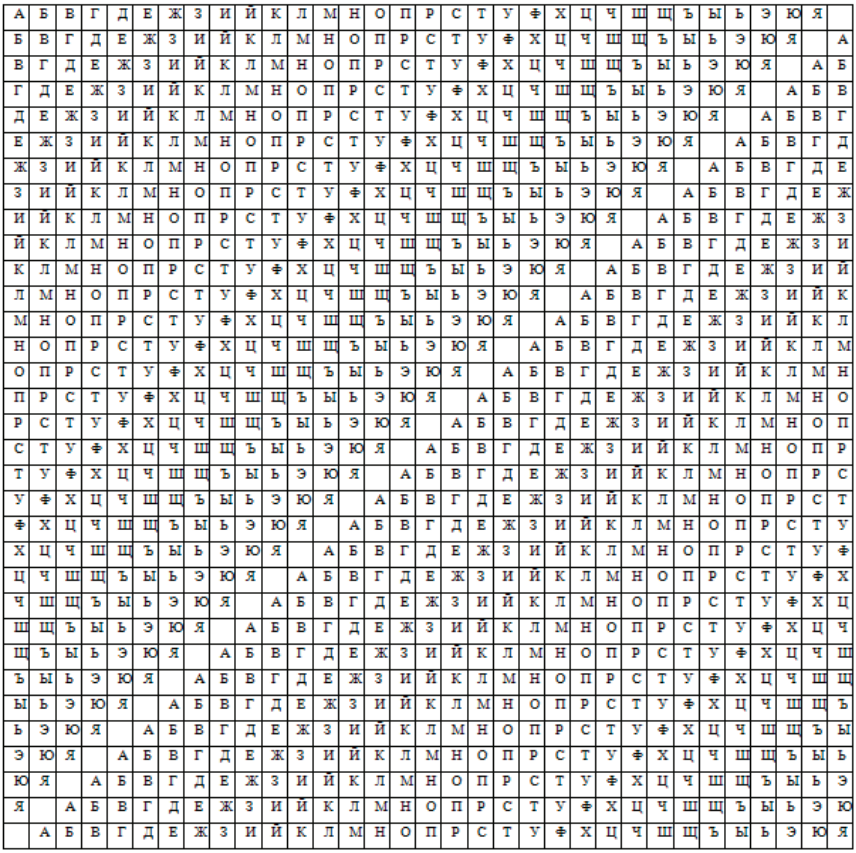


Рис. 1.1. Таблица Виженера

Пример. Используя шифр Виженера, зашифруем сообщение **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**. В качестве ключевого слова выберем имя **ИЛЬЯ**. Исходный текст: **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**.

Используем алфавит, содержащий 33 буквы, и пробел, стоящий после буквы Я: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ*пробел*

С помощью ключа **ИЛЬЯ** запишем строку исходного текста с расположенной под ней строкой с циклически повторяемым ключом (рис. 1.2).