УДК 004

Прохорова Мария Сергеевна,
студентка ИВТ-19-1, Ангарский государственный технический университет,
e-mail: mash.prohorowa.01@mail.ru
Сенотова Светлана Анатольевна,
к.т.н., доцент, Ангарский государственный технический университет,
e-mail: sveta-senotova@mail.ru

РАЗРАБОТКА ИНТЕРАКТИВНОГО ТРЕНАЖЕРА КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Prohorova M.S., Senotova S.A.

DEVELOPMENT OF INTERACTIVE CRYPTOGRAPHIC SYSTEMS SIMULATOR

Аннотация. Разработка интерактивного тренажера криптографических систем для изучения материалов по защите информации.

Ключевые слова: шифрование, методы шифрования, тренажер, криптографическая защита информации.

Abstract. Development of an interactive simulator of cryptographic systems for studying information security.

Keywords: encryption, encryption methods, simulator, cryptographic protection of information.

На данном этапе развития технологий большая часть информации, в том числе и конфиденциальной, хранится в электронном виде. Одним из незаменимых способов защиты информации (безопасности данных [1]) является шифрование, например, электронная цифровая подпись, хэш-функция [2] и т.п.

Шифры появились задолго до появления первых вычислительных машин. В настоящее время шифрование настолько важно, что пронизывает все сферы деятельности, и им занимаются специалисты по защите информации.

Для того чтобы понимать принципы современных методов шифрования, необходимо начинать изучение этой области с самых примитивных шифров. Специалист должен не только понимать принцип работы метода шифрования, но и уметь правильно реализовать его программно.

В Университете тема защиты информации изучается в различных дисциплинах студентами кафедры Вычислительных машин и комплексов.

В данной статье рассматривается криптографическая защита информации – это защита информации с помощью ее криптографического преобразования [3].

В процессе обучения студенты сталкиваются с необходимостью поиска материалов о шифрах на различных ресурсах сети Интернет, где информация может быть не структурированной и недостоверной.

Для упрощения этого процесса было решено разработать интерактивный тренажёр криптографических систем, который позволит изучить теорию и способы программной реализации шифров на языках программирования высокого уровня. Интерактивный тренажёр находится на стадии разработки, на рисунке 1

представлен фрагмент теоретической части тренажера, а на рисунке 2 пример работы шифра Атбаш.

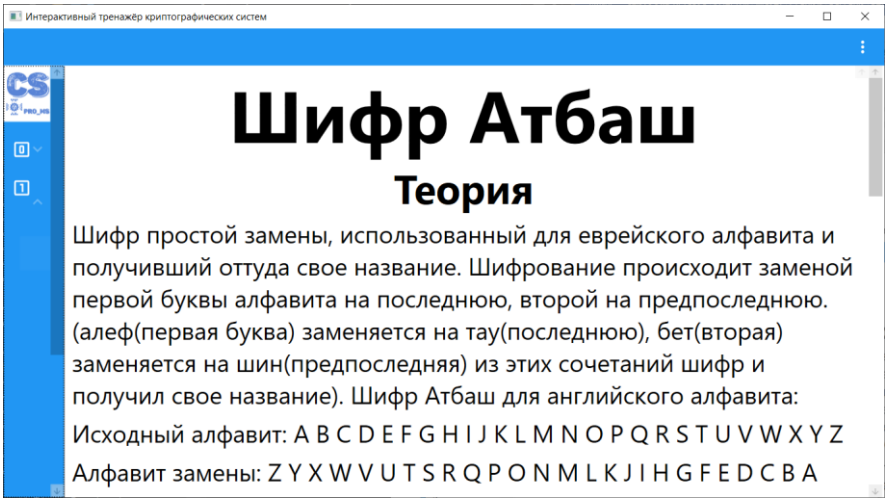

Рисунок 1 – Теоретическая часть интерактивного тренажера

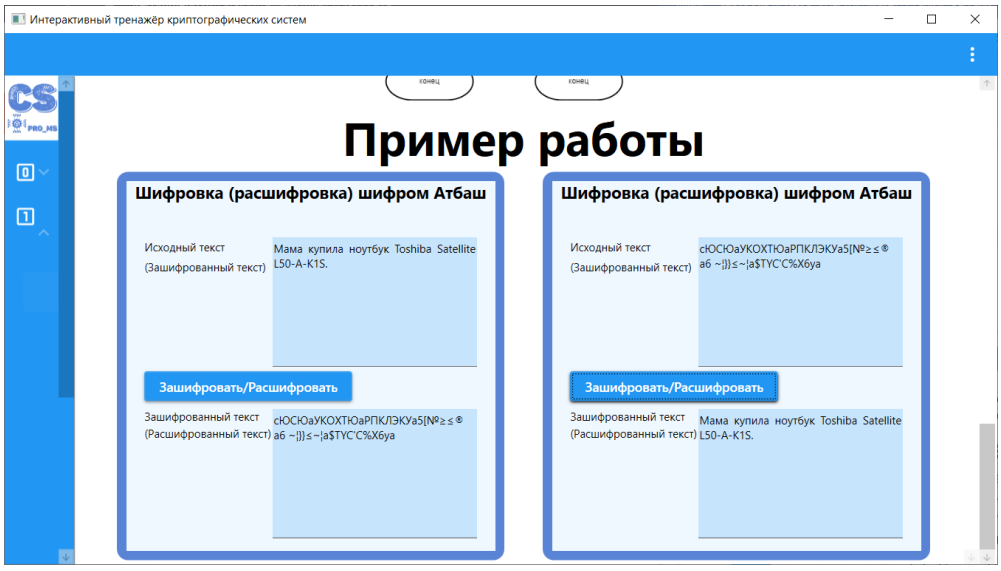

Рисунок 2 – Пример работы шифра Атбаш

ЛИТЕРАТУРА

1. ГОСТ Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации [Электронный документ] URL: https://internet-law.ru/stroyka/doc/45674/ (Дата обращения: 20.02.23).
2. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный документ] URL: https://docs.cntd.ru/document/1200095034 (Дата обращения: 25.02.23).
3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения [Электронный документ] URL: https://internet-law.ru/gosts/gost/5737/ (Дата обращения: 01.03.23).