Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных систем и технологий

Кафедра «Информационные системы»

Дисциплина «Информационная безопасность»

Лабораторная работа №1

Выполнил:

студент гр. ПИбд-41

Барсуков П. О.

Проверил:  
Мытарев П. В.

Ульяновск, 2025г.

**Индивидуальное задание**

Ограничение на выбираемые пароли: Наличие цифр, знаков препинания и знаков арифметических операций.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Используемый режим шифрования алгоритма DES для шифрования файла | Добавление к ключу случайного значения | Используемый алгоритм хеширования пароля |
| 5 | ECB | Да | MD5 |

Реализованное приложение: <https://github.com/frogg24/InfSec>

**Описание структуры БД**

Таблица Users:

* Id – уникальный индификатор пользователя
* Username – имя пользователя
* Password\_hash – пароль пользователя в виде кэша
* Blocked – флаг блокировки
* Restrictions\_enabled – флаг наличия ограничений
* Min\_length – минимальная длина пароля
* Expiry\_months – срок действия пароля в месяцах

**Описание функций связанных с хэшированием и шифрованием**

Для шифрования файла БД используется алгоритм DES из System.Security.Cryptography в режиме ECB.. Используется добавление случайного значения размером 8 байт, которое генерируется с помощью RandomNumberGenerator.Create(). Ключ получается путем объединения случайного значения и байтов UTF-8 парольной фразы, которые хэшируются и усекаются до первых 8 байтов, которые и становятся ключом.

Для хэширования паролей используется алгоритм MD5 из System.Security.Cryptography.