МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИМ. В.Н.ТАТИЩЕВА

Факультет цифровых технологий и кибербезопасности

Кафедра информационных технологий

Форма обучения очная

**БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ**

**ЛАБОРАТОРНАЯ РАБОТА №2**

***Реализация простейшего генератора паролей***

|  |  |  |
| --- | --- | --- |
| Исполнитель:  студент группы ДПИ-25  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мартынов В.А.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.    Преподаватель:  Кафедра информационных технологий  Кандидат технических наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мартьянова А.Е.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г. |  |  |

Астрахань – 2025

1. **Практическая часть**

Для выполнения задания был выбран вариант №10:

* Пользователь вводит идентификатор длины *N*.
* Длина пароля фиксирована — 10 символов *b*1,*b*2,...,*b*10.
* *Q*=*N*mod6.
* Последние *Q*+1 символов пароля (с *b*10−*Q* по *b*10) — случайные цифры.
* Первые два символа *b*1,*b*2 — случайные заглавные буквы русского алфавита.
* Символы с *b*3 по *b*10−*Q*−1 — случайные строчные буквы русского алфавита.

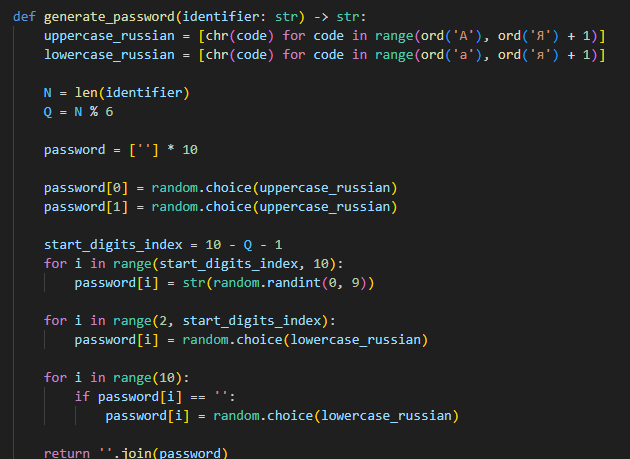


Рисунок 1 – Генератор паролей

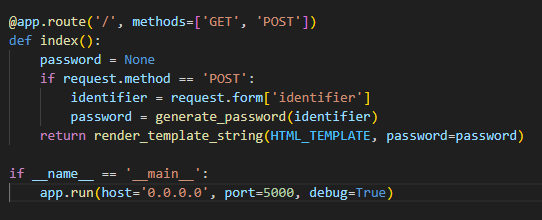


Рисунок 2 – Взаимодействие frontend и backend

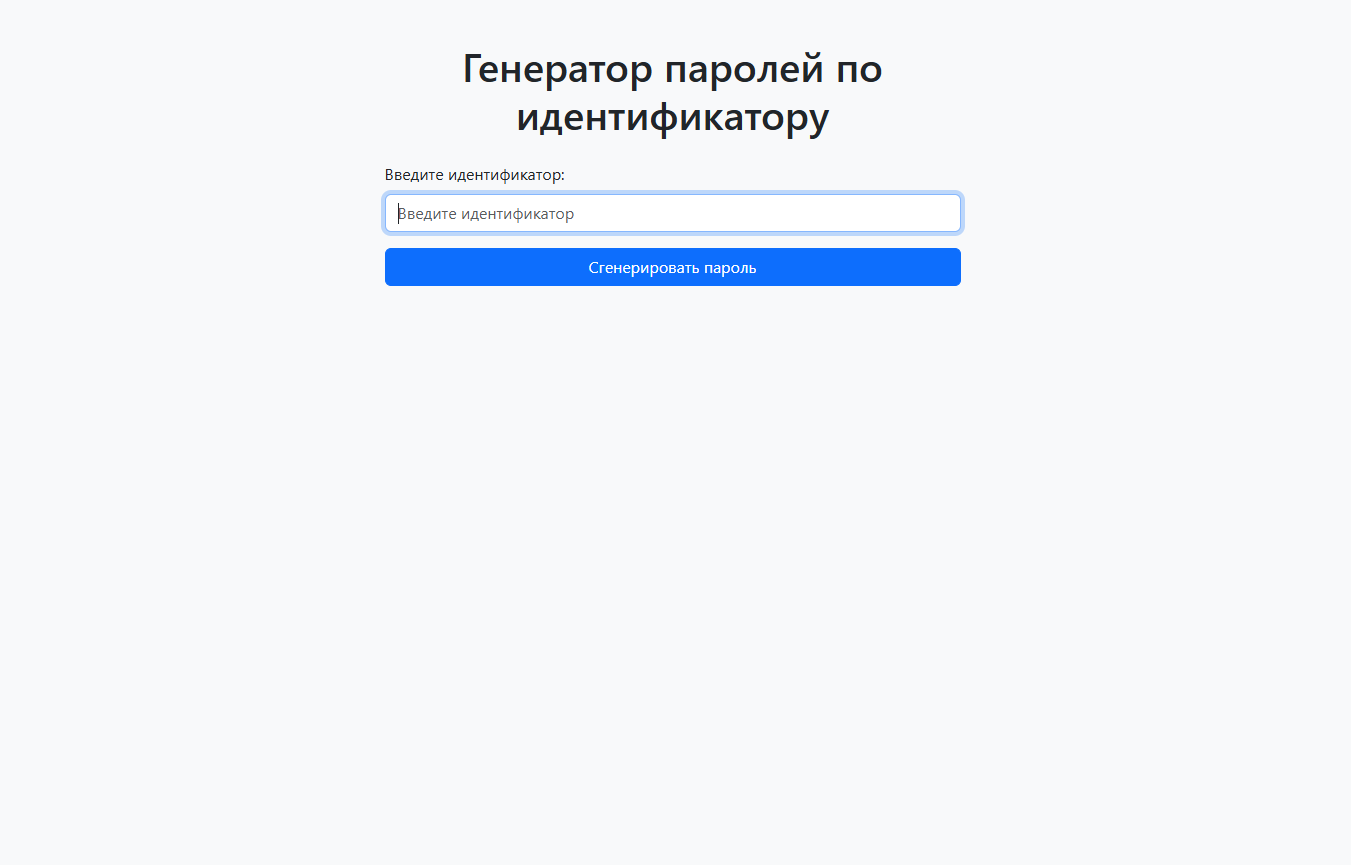


Рисунок 3 – Окно программы в WEB-интерфейсе

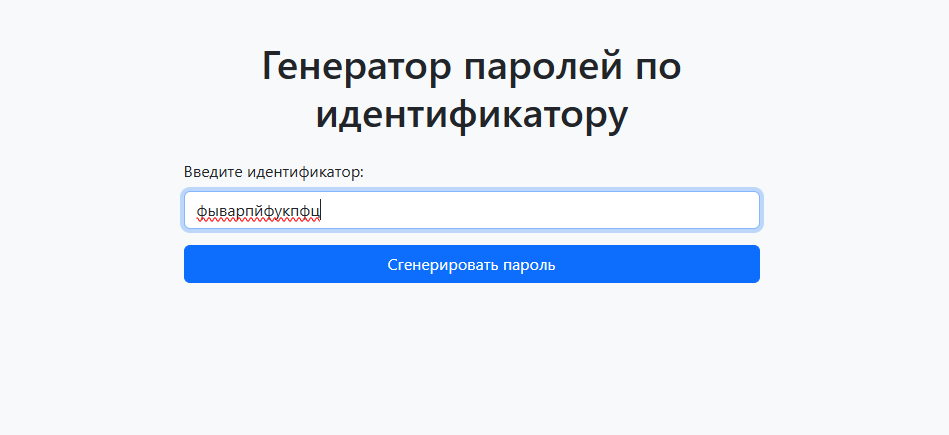


Рисунок 4 – Пример запроса

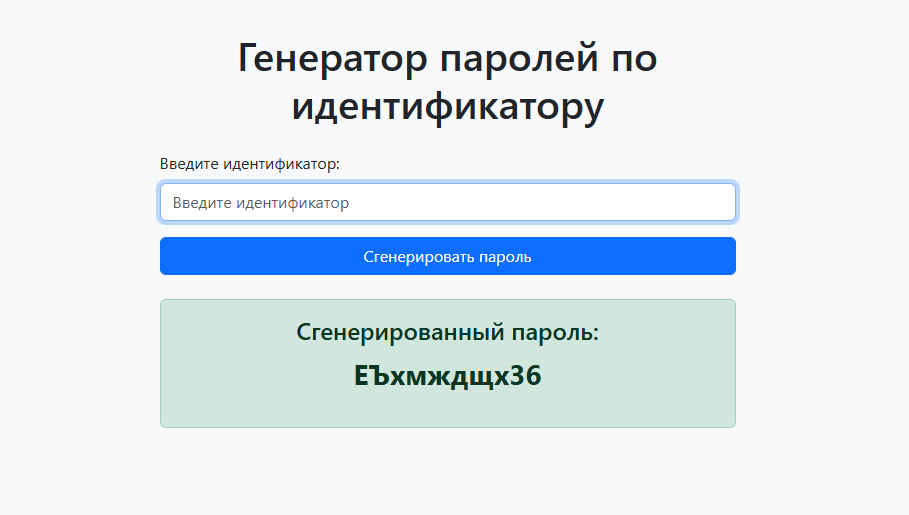


Рисунок 5 – Пример ответа

1. **Ответы на контрольные вопросы**
2. Определение стойкости пароля к взлому и формула

Стойкость пароля — показатель, характеризующий сложность и время, необходимое для его взлома методом перебора всех возможных комбинаций. Чем выше стойкость, тем сложнее подобрать пароль.

Формула числа всех возможных паролей:

где,

где S — общее число вариантов,

R — мощность алфавита (количество различных символов),

L — длина пароля.

1. Определение мощности алфавита паролей

Мощность алфавита — количество различных символов, используемых для формирования пароля (например, цифры, заглавные и строчные буквы, специальные символы).

1. Основные задачи, решаемые с использованием определения стойкости пароля

* Оценка времени и ресурсов, необходимых для взлома пароля.
* Разработка требований к сложности и длине пароля.
* Поддержание безопасности информационных систем через подбор надежных паролей.
* Анализ и улучшение политики безопасности пользователей.

1. Основные требования к выбору пароля

* Достаточная длина (рекомендуется не менее 8-12 символов).
* Использование символов разного типа (строчные и заглавные буквы, цифры, спецсимволы).
* Отсутствие предсказуемых последовательностей и слов из словаря.
* Уникальность пароля для каждого ресурса.
* Периодическая смена паролей при необходимости.