Департамент образования и науки города Москвы

Государственное бюджетное образовательное учреждение Школа №2109

**Проектная работа**

на тему:

«Генератор паролей»

**выполнил**: Романов Алексей Витальевич 11К

**научный руководитель**: учитель информатики

Бабушкин Сергей Владимирович

Москва, 2022

Оглавление

1. Введение…………………………………………………………………….2
   1. Историческая справка и теория по паролям…………….................2
   2. Практическая польза использования ГП…………………………..3
   3. Актуальность ГП………………………….........................................3
   4. Цель и задача проекта…………………….........................................3
2. Основная часть……………………………………………………………..3
   1. Способ реализации………………………………………………….3
   2. Как оценить сложность пароля и эффективность?..........................4
   3. Использование ГП…………………………………………………..8
   4. Обобщение проекта………………………........................................8
3. Заключение…………………………………………………………………9
   1. Итог…………………………………………………………………..9

**Введение**

В современном мире остро стоят задачи информационной безопасности. Каждый информационный ресурс требует соотнесения пользователя с уровнем его доступа, конфиденциальная информация не должна быть предоставлена лицам, не имеющим права на её получение. задачи авторизации и идентификации решают эти проблемы.

1. **Историческая справка и обзор литературы.**

**Пароль** (*parole* — слово) — условное словоили произвольный набор знаков, состоящий из букв, цифр и других символов, и предназначенный для подтверждения личности или полномочий. Если допустимо использование только цифр, то такую комбинацию иногда ПИН-КОДОМ (от английской аббревиатуры PIN — персональный идентификационный номер).

Пароли часто используются для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация «имя пользователя — пароль» используется для удостоверения пользователя.

Несмотря на происхождение термина, пароль не обязан быть, собственно, словом. Комбинацию, не являющуюся словом, сложнее угадать или подобрать, поэтому такие пароли более предпочтительны. Для дополнительной защиты иногда используют пароли, состоящие из многих слов; такой пароль иногда называют «парольной фразой». *Запомните это, мы еще вернемся к этому.*

* 1. Практическая польза ГП

Большинство людей используют несложные комбинации, которые, возможно, имеются в базе данных “Украденных паролей”, поэтому становится весьма опасно пользоваться данными паролями. Допустим вы использовали несложный пароль для личной почты, злоумышленник беспрепятственно получает доступ к информации на ней и распоряжается ей как ему угодно. Согласитесь в этом мало приятного. И так, чтобы избежать неприятностей нужно придумывать сложные пароли. Но почему люди так не делают? – Есть три основные причины: человеку лень его придумывать и он использует, возможно, свое имя и пару цифр, или у человека нету времени придумывать пароль, или человек не хочет заморачиваться, используя сложный пароль. Если причина по которой вы не используете сложный пароль третья, то вам следует переосмыслить использование паролей.

* 1. Актуальность ГП

Имеем картину, что ГП в настоящий момент более чем актуален. Поэтому я буду реализовать этот проект.

* 1. Цель и задача проекта

И так, вы поняли, что использование сложных и хороших паролей - это залог вашей безопасности. Также вы узнали, что имеются два основных типа паролей – набор символов (Трудно запоминаемый и потому требует записи, например, на бумажный носитель) и фразовый пароль (Состоит из фраз, которые можно легко держать у себя в голове). Моя задача состоит в реализации функциональности и того, и того типа паролей в одном месте.

**2. Описание проекта.**

2.1 СПОСОБ РЕАЛИЗАЦИИ

Для решения поставленной задачи есть разные пути решения:

* Консольная программа (При таком варианте пользователь должен уметь взаимодействовать с консолью и в целом разбираться с базовыми принципами компьютера)
* Приложение в виде исполняемого файла (уже более благоприятный вариант для конечного пользователя )
* Веб сайт – самое простое и понятное для пользователя решение. Просто зайти на сайт и сгенерировать пароль.

Последний вариант и есть результат этого проекта.

2.2 Как оценить сложность и эффективность пароля?

Сложность пароля – это то, насколько сложно пароль отгадать.

Сложность пароля зависит от мощности алфавита пароля и длины пароля. И так, чтобы сделать пароль сложнее мы должны увеличивать алфавит и длину. Но оказывается имея, допустим, алфавит длиной в английский алфавит будет разумнее добавить пару букв, чем расширять алфавит. Вот пример: A) Исходный алфавит - длина 6 букв, мощность алфавита 26 букв

Б) Алфавит с расширенной мощностью алфавита и нетронутой длиной. А именно мощность алфавита увеличили на 10 знаков (добавили цифры от 0 до 9)

В) Алфавит с расширенной длиной и нетронутой мощностью алфавита. А именно увеличили длину пароля на 4 символа (примерно одно слово).

Для вычисления сложности пароля можно воспользоваться следующей формулой: мощность алфавита^длина пароля

Для пароля Б имеем: 36^6 = 2176782336.

Для пароля В имеем: 26^10 = 141167095653376

Пароль “В” в 64851.26846 раза защищеннее!

Получается добавив к совей фразе 1 слово можно добиться сильного увеличения резистентности ко взлому. И это так.

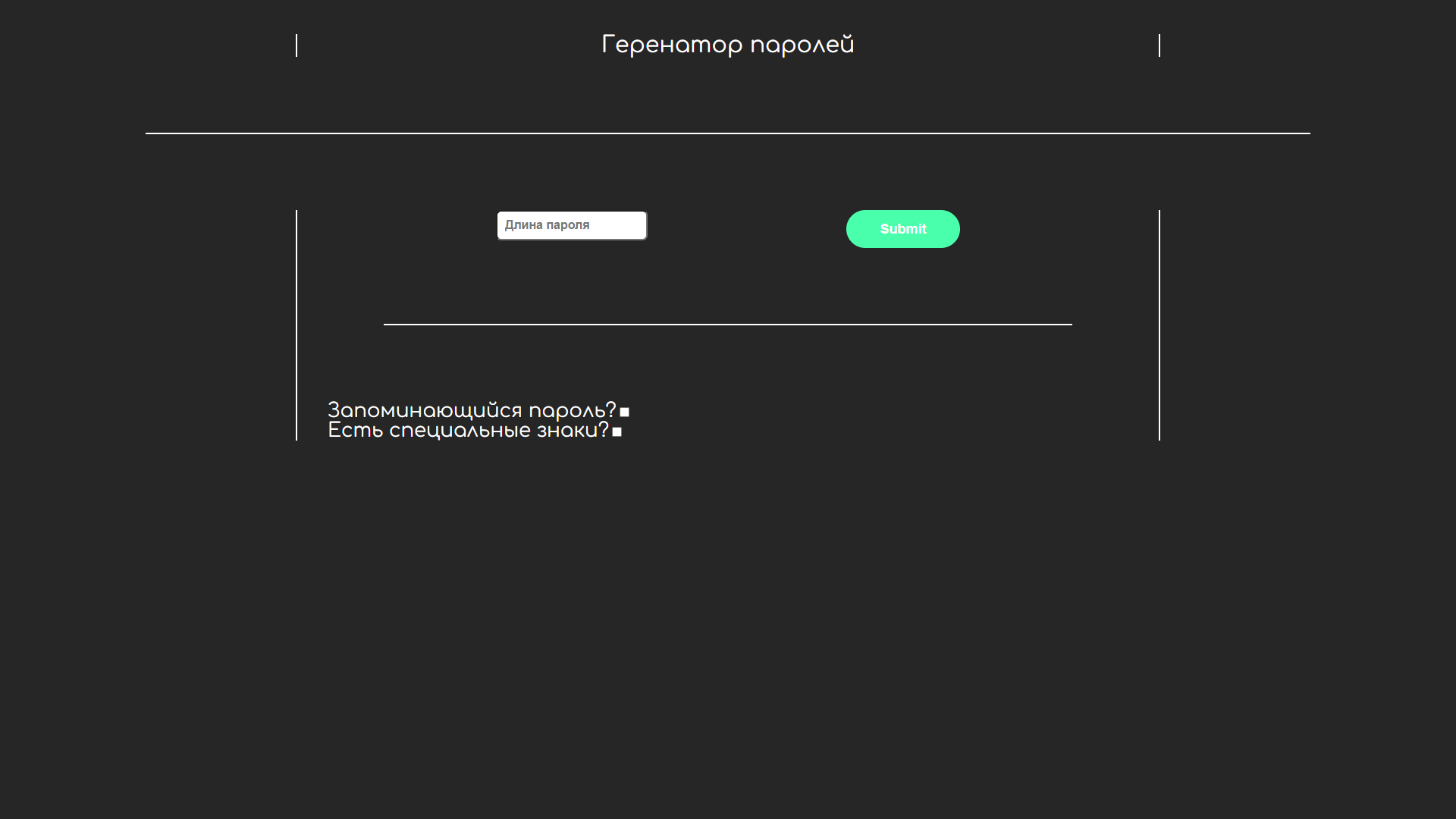
2.3 Использование ГП

У ГП, как замечалось ранее, имеется два типа работы – генерация набора символов и фразовый пароль.

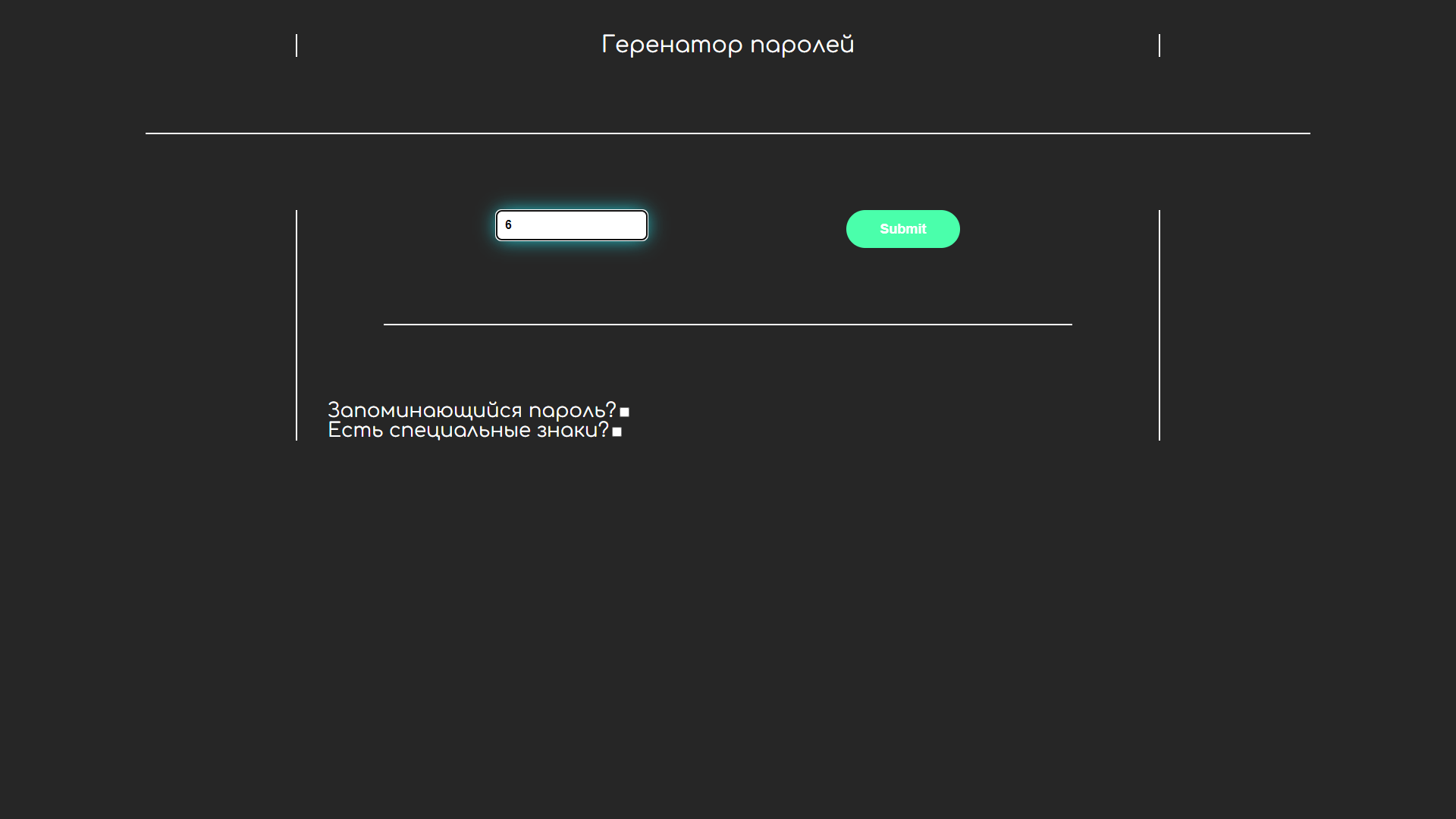
Для того, чтобы протестировать как работают эти режимы работы, перейдите на сайт https://romanovalexey.online/gen/index\_ru/ и используя понятный интерфейс сгенерируйте нужный пароль!

Начнем с генерации набора символов.

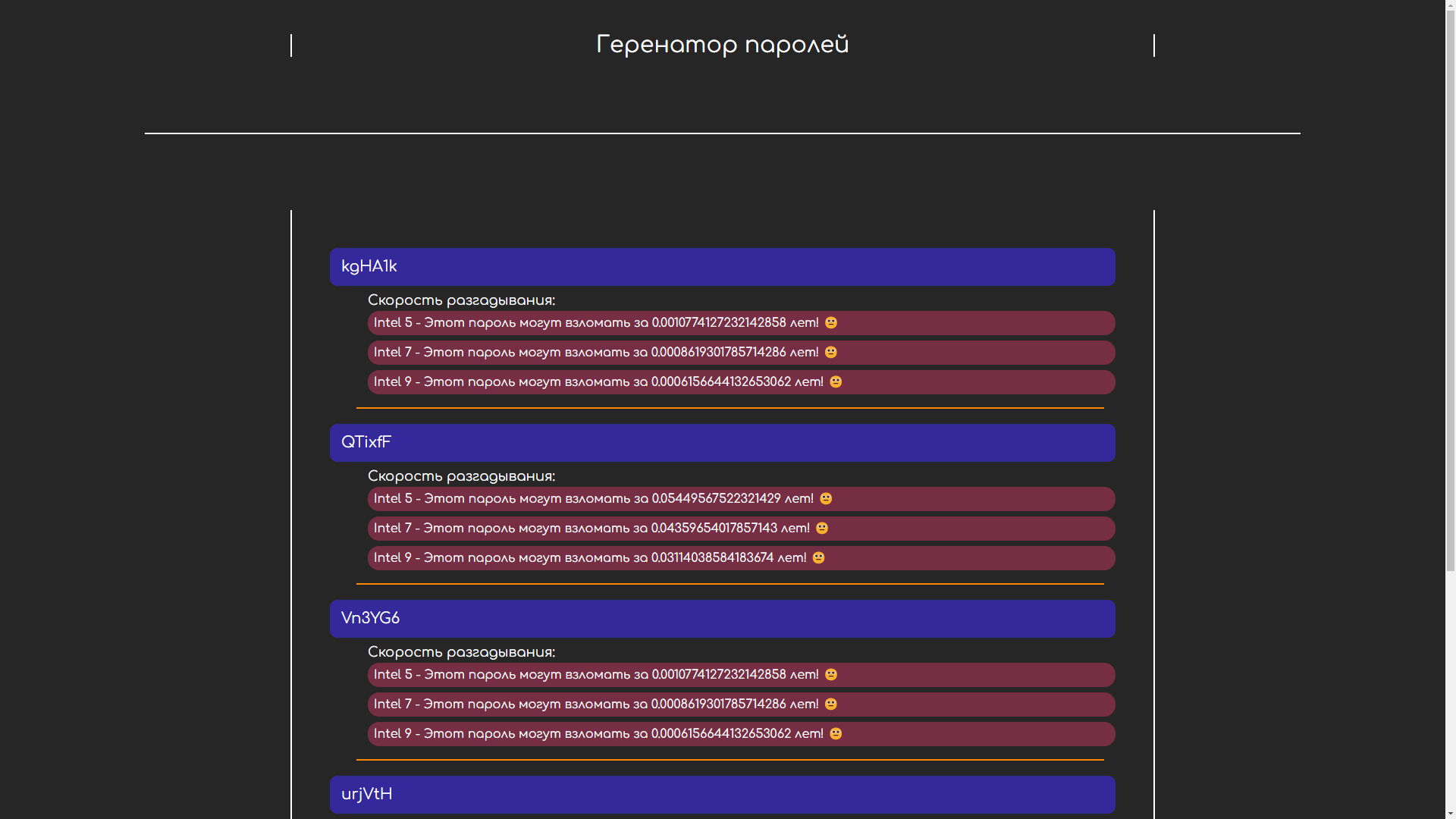
На главной странице нас встречает следующий интерфейс:



Давайте заполним поля конфигурации и создадим пароль.



Нажмем зеленую кнопку отправить

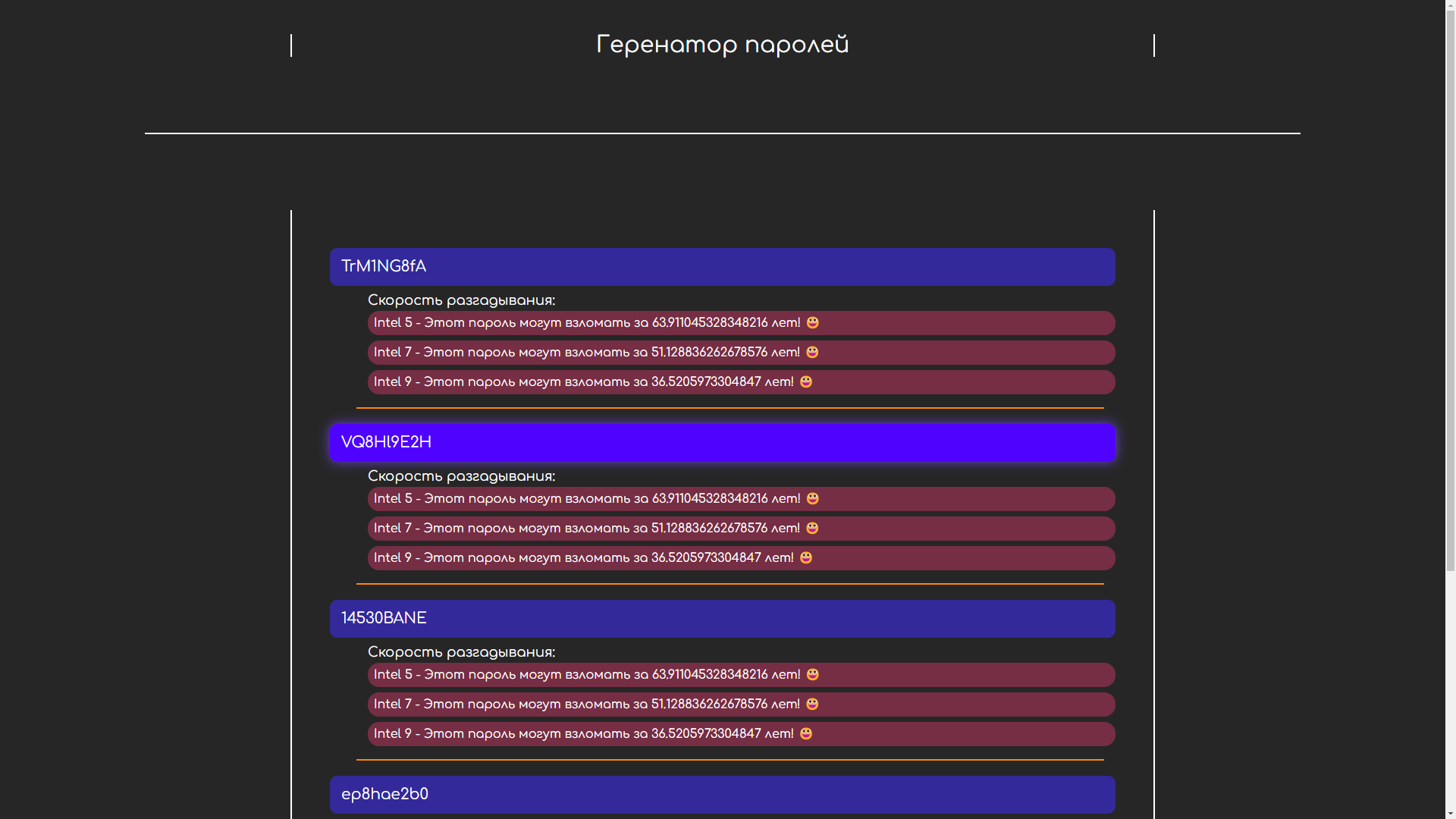


И вот наш результат!

Судя по грустным смайликам пароль не очень надежный.



Увеличив длину пароля на 3 символа (в сумме 9) получим более надежный пароль и смайлик будет счастливым.



На последок создадим запоминающийся пароль – самый удобный и как оказалось безопасный.

На странице конфигурации выберем длину 4 слова и отметил галочку “запоминающийся пароль”.

Получим:



2.4 Обобщение проекта

В общей сумме имеем удобный и полезный инструмент для создания гибких и настраиваемых паролей, которые можно использовать в различных целях.

3.0 **Заключение**

Подводя итог по проекту мы узнали об теории паролей, об их истории, об их типах и о об их теории сложности. Мы подробно разобрались какой пароль сложнее и как эффективно улучшать его сложность, попробовали создать своими руками пару паролей и увидели приблизительную скорость взлома.

Как практичный совет запомните – используйте пароли длиной не менее 8 символов из знаков, допустим, латинского алфавита, но лучше всего придумать фразовый пароль из 4 и более слов и быть спокойным за свои данные.