

Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

ОТЧЁТ

к лабораторной работе №1

по дисциплине «Средства и методы защиты информации в
интеллектуальных системах»

Студент:

Д.С.Батук

Группа:

321703

Проверил:

Д. А.Сальников

Минск 2025

Тема: генерация паролей

Задание:

- 1) Разработать программу на языке C++, реализующую следующие функции:
 - генерация строки с заданной пользователем длиной, состоящей из символов алфавита в соответствии с вариантом задания (использовать функции `rand()`, `srand()` и инициализацию от таймера);
 - проверка равномерности распределения символов путем визуализации частотного распределения;
 - вычисление среднего времени подбора пароля, выбираемого из сгенерированной строки.
- 2) Построить график зависимости среднего времени подбора пароля от его длины.
- 3) Дать практические рекомендации по выбору пароля исходя из предположений об алфавите пароля; ценности информации, доступ к которой защищается с помощью этого пароля; производительности вычислительного средства атакующего и времени атаки.

Вариант алфавита для генерации пароля:

- 2) Латиница строчные и прописные.

Цель: изучить базовые принципы и способы организации безопасности в информационной среде, основные типы объектов и терминов, в частности, понятие пароля, его классификации и особенности составления и подбора. Также закрепить полученные знания, выполнив задание с программной реализацией механизмов составления и подбора пароля.

Пример работы

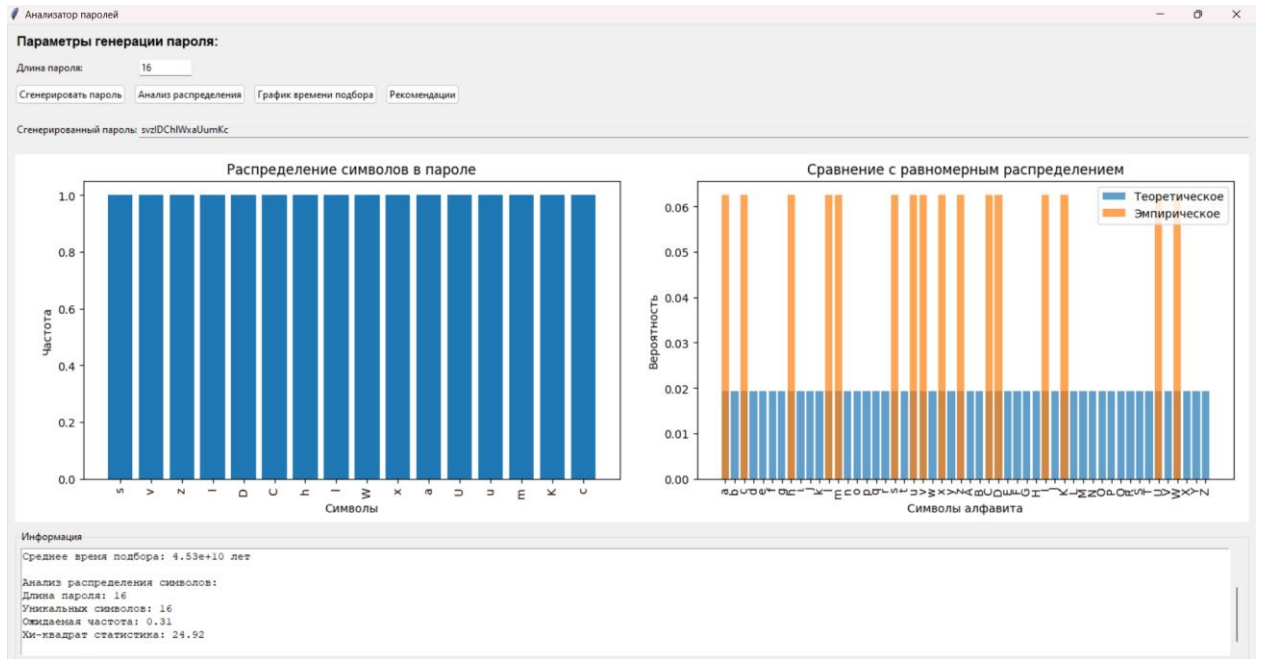
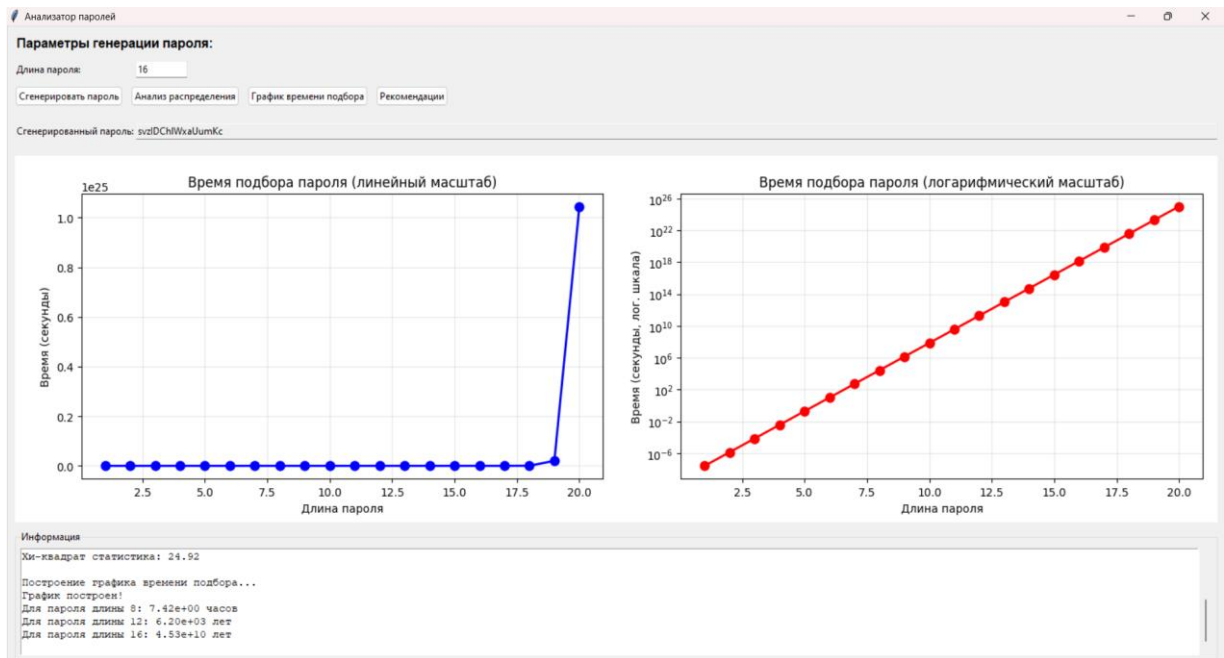


График зависимости среднего времени подбора пароля от его длины



Рекомендации по выбору пароля

1. **Не используйте словарные слова, имена, даты** — они уязвимы к словарным атакам.
2. **Используйте максимально возможный алфавит** — буквы (верх/нижний регистр), цифры, спецсимволы.

3. **Длина важнее сложности** — 16 символов из букв и цифр надёжнее, чем 8 с символами.
4. **Используйте генераторы случайных паролей** — например, pwgen, KeePass, 1Password.
5. **Для высокой безопасности** — используйте **passphrases** (случайные слова).
6. **Никогда не повторяйте пароли** между разными сервисами.
7. **Используйте менеджер паролей** — чтобы не запоминать, а хранить надёжно.

Итог: в ходе выполнения лабораторной работы были изучены основные принципы генерации паролей, а также факторы, влияющие на их стойкость к подбору. Была реализована программа, составляющая и подбирающая пароль, в результате разработки которой были закреплены полученные знания. Также был построен график, визуализирующий зависимость среднего времени подбора пароля от его длины и были сформулированы базовые рекомендации по выбору пароля.