**УДК 004.056.52**

**Мухаметчин Артём Викторович, 8 класс**

**РАНДОМАЙЗЕР ПАРОЛЕЙ**

*МАУ ДО "Центр дополнительного образования» г.Мирный*

*Моякулова Екатерина Николаевна, педагог дополнительного образования*

**Аннотация:** Научная работа посвящена разработке генератора паролей на Python с использованием графического интерфейса Tkinter и метода брутфорс для подбора паролей. Исследованы теоретические аспекты безопасности паролей и созданы две прикладные программы.

**Ключевые слова**: Python, генератор паролей, Tkinter, безопасность, брутфорс, криптография.

1. **Введение:**

**Цель:** Разработка программного обеспечения для безопасного управления паролями пользователей с применением методов генерации случайных паролей и анализа их стойкости к атаке методом перебора.

**Задачи:**

1. Разработать алгоритм для генерации сложных паролей.

2. Реализовать интерфейс для взаимодействия пользователя с программой.

3. Реализовать механизм сохранения зашифрованных паролей, чтение с дешифровкой.

3. Провести исследование на стойкость паролей методом полного перебора (брутфорс).

4. Оценить эффективность.

**Методы исследования:**

Теоретические методы: изучение современных подходов к созданию и оценке безопасности паролей, обзор существующих алгоритмов генерации и атаки на пароли [1].

Практические методы: разработка двух программ — генератора паролей и утилиты для подбора паролей методом брутфорс, тестирование созданных приложений на реальных данных.

**Объект исследования:**

Программное обеспечение для работы с паролями, включающее генераторы и средства проверки их надежности.

**Предмет исследования:**

Алгоритмы генерации паролей и методики их защиты от несанкционированного доступа через атаку полным перебором.

**Практическая значимость:**

Разработанные программы позволяют пользователям создавать надежные пароли, защищая личные данные от потенциальных угроз взлома. Внедрение генератора паролей упрощает процесс создания уникальных комбинаций символов, минимизируя риск использования легкоугадываемых или повторяющихся паролей. Анализ стойкости паролей помогает лучше понимать уязвимости системы безопасности**.**

1. **Основная часть**

**Генерация паролей:**

Программа написана на языке программирования Python с использованием библиотеки Tkinter для реализации графического интерфейса. Основной задачей является создание сложного пароля длиной от 8 до 16 символов, состоящего из букв верхнего и нижнего регистра, цифр и специальных символов. Для обеспечения максимальной случайности используется функция `random.choice`, выбирающая элементы из множества возможных символов [2].

Пример генерируемого пароля: P-sрЕw0rd\*3!

**Атака методом брутфорс:**

Вторая программа реализует метод полного перебора (брутфорс) для подбора пароля заданной длины. Алгоритм последовательно проверяет все возможные комбинации символов до тех пор, пока не будет найдено совпадение с целевым паролем. Это позволяет оценить стойкость пароля к подобным атакам.

Результат подбора пароля S;be% при длине 5 символа, не так быстро взламывается как из 3-х или 4-х символов:

Пароль найден: S;be% (попыток: 1048576).

**Результаты тестирования**

Тестирование показало, что использование специальных символов, заглавных и строчных букв значительно увеличивает сложность подбора пароля. Однако, даже короткие пароли требуют значительных вычислительных ресурсов для успешного подбора методом брутфорс [3].

**Выводы**

Проведенное исследование позволило разработать эффективные инструменты для генерации и оценки безопасности паролей. Программы продемонстрировали высокую практическую ценность благодаря простоте использования и способности создавать уникальные и устойчивые к взлому пароли. Важно отметить, что даже самые сложные пароли остаются уязвимыми перед методами социальной инженерии и фишинга, поэтому наряду с техническими мерами рекомендуется использовать дополнительные способы защиты, такие как двухфакторная аутентификация.

**Библиографический список**

1. Типы атак на пароли // Keeper Security Blog. — URL: https://www.keepersecurity.com/blog/ru/2024/01/12/types-of-password-attacks/ (дата обращения: 10.03.2025).

2. Мэтью Э: Изучаем Python. Программирование игр, визуализация данных, веб-приложения. — СПб.: Питер, 2017. — 496 с.: ил. — (Серия «Библиотека программиста»).

2. Что такое Brute Force? // SkillFactory Blog. — URL: https://blog.skillfactory.ru/glossary/brute-force/ (дата обращения: 10.03.2025)..