А. А. Семенюк

РАЗРАБОТКА АНАЛИЗАТОРА НАДЁЖНОСТИ ПАРОЛЕЙ НА ОСНОВЕ МНОГОФАКТОРНОГО АЛГОРИТМА ОЦЕНКИ И ГЕНЕРАЦИИ

Рассматривается программная реализация анализатора надёжности паролей с расширенной системой оценки защищённости. Предлагается комплексный подход, включающий оценку сложности, генерацию сильных паролей и безопасное хранилище. Программа предназначена для повышения осведомлённости пользователей о криптографической стойкости паролей.

Введение

В современном цифровом мире выбор надёжного пароля является ключевым фактором информационной безопасности. Для решения задачи оценки и улучшения качества паролей разработан консольный анализатор, основанный на достоверном алгоритме многофакторной оценки. В ходе работы реализованы функции генерации, хранения и сравнения паролей. Предлагается использовать модифицированную схему оценки, учитывающую длину, разнообразие символов и наличие распространённых слабых паттернов.

I. Алгоритм оценки пароля

Классическая оценка пароля представляет собой многофакторный анализ с присвоением баллов за положительные характеристики и штрафами за слабые места. Алгоритм evaluatePasswordAdvanced учитывает 15-балльную шкалу.

На входе — строка пароля. На выходе — числовой балл (0–15) и текстовое описание силы («ОТЛИЧНЫЙ», «ХОРОШИЙ» и т.д.).

II. Функции генерации и хранения

Генератор паролей гарантирует наличие минимум одного символа каждого типа и производит финальное перемешивание. Хранилище passwordVault сохраняет пароль, название, дату, балл и статус в файл password_vault.txt. Поддерживается просмотр, сравнение и безопасное удаление записей.

III. Заключение

Предлагаемый анализатор точно характеризует надёжность пароля, даёт конкретные рекомендации по улучшению и предоставляет удобный интерфейс управления хранилищем. Реализация на C++ обеспечивает высокую производительность и простоту расширения. Использование данного инструмента повышает культуру информационной безопасности конечных пользователей.

Список литературы

1. OWASP. Руководство по безопасному выбору паролей. –2025. – 32 с.
2. Рябцев Д. К. Анализ современных методов хранения паролей // Безопасность цифровых технологий. – 2024. –№1 (112). – С. 74–89.
3. Янг С., Айтел Д. The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks. – Бока-Ратон: CRC Press, 2004. – 896 с.

Семенюк Артём Алексеевич, студент 1курса факультета информационной безопасности Белорусского государственного университета информатики и радиоэлекстроники, artemsemianiuk07@gmail.com.

Научный руководитель: Кукин Дмитрий Петрович, Заведующий кафедрой вычислительных методов и программирования. Белорусского государственного университета информатики и радиоэлектроники, кандидат технических наук, доцент.kukin@bsuir.by