АНАЛИЗ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ ОБЩЕГО ДОСТУПА С ПАРОЛЬНОЙ ЗАЩИТОЙ

В.В. Маликов, А.В. Макатерчик

Использование хеш-функций находит широкое применение в различных областях информационной безопасности. Однако, техническая осведомленность злоумышленников и их инструментарий постоянно растут и изменяются, поэтому в интересах защиты информации является жизненно необходимым знать реальное состояние дел с уровнем возможностей используемых технологий защиты информации. В ходе исследования авторами выполнен анализ возможностей программных средств анализа и расшифровки паролей, функционирующих на основе методов анализа значений хэш-функций.

На первом этапе исследования были выбраны для исследования следующие программные средства: скрипт определения хэш-функции hash-identifier, списки паролей RockYou, программа расшифровывания Hashcat. Проверены возможности проведения атаки прямым перебором и расшифровка по словарю. Исследование выполнялось по отдельности для каждого контрольного слова и с использованием различных хэш-функций.

Выявленные ограничения возможностей программных средств: атака прямым перебором для сложных паролей практически невозможен; обязательным условием расшифровки пароля по значению хэш-функции, является нахождение данного пароля в словаре либо как целое слово, либо как часть другого слова; поддерживается только латиница.

Результаты исследования позволяют утверждать, что реальные возможности существующих программных средств по расшифровке паролей на основе анализа значений хэш-функций достаточно ограничены. При этом стоит учитывать, что идентификация хэш-функции выполняется быстро и достоверно, что значительно повышает эффективность расшифровки паролей, но способ на скорость и качество расшифровки не влияет.