М. В. Павлюк
(ГГУ им. Ф. Скорины, Гомель)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ШИФРОВАНИЯ И ХРАНЕНИЯ АУТЕНТИФИКАЦИОННЫХ ДАННЫХ МНОГИХ ПОЛЬЗОВАТЕЛЕЙ

Аутентификационные данные пользователя, как хранящийся набор данных, представляют собой совокупность адресных имен сайтов и названий приложений вместе с соответствующими логинами и паролями, которые необходимы для успешной авторизации пользователя. Эта информация является конфиденциальной и крайне нежелательно попадание ее в руки сторонних лиц. Возникает необходимость удобного и надежного способа ее хранения с предотвращением доступа к ней злоумышленников.

В настоящей работе для непосредственного хранения аутентификационных данных многих пользователей в зашифрованном виде применяется симметричный алгоритм 64-битного блочного шифра с ключом переменной длины «Blowfish», представляющий собой сеть Фейстеля, но с некоторыми особенностями генерации и использования раундовых ключей. Для авторизации пользователей и защиты паролей доступа применяется однонаправленная хеш-функция «SHA-256» с добавлением к хешируемому паролю автоматически генерируемой криптографической соли.

Кроме надежного хранения аутентификационных данных многих пользователей, необходим простой и удобный способ непосредственного доступа к ним авторизированных лиц. Это было достигнуто посредством реализации простого и интуитивно понятного интерфейса программного обеспечения. Разработка программного обеспечения осуществлялась в среде «Embarcadero C++ Builder XE4».

Использование вышеперечисленных криптографических алгоритмов защиты аутентификационных данных многих пользователей в совокупности с интуитивно понятным интерфейсом, обеспечивает достаточно надежный и удобный способ их хранения, предотвращающий доступ к ним сторонних лиц.

ЛИТЕРАТУРА

1 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер; под ред. А. Б. Васильева. – М.: Триумф, 2002. – 816 с.

2 Венбо, М. Современная криптография. Теория и практика / М. Венбо. – М.: Вильямс, 2005. – 768 с.

3 Теллес, М. Н. Borland C++ Builder. Библиотека программиста / М. Н. Теллес. – СПб.: БХВ-Петербург, 2004. – 461 с.