УДК 004.4

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ХРАНЕНИЯ ПАРОЛЕЙ

Н. А. КАЗЫМОВ, Я. В. СМЫЧКОВ
Научный руководитель Е. А. ЗАЙЧЕНКО
Белорусско-Российский университет
Могилев, Беларусь

На сегодняшний день вопрос сохранения конфиденциальности информации стоит особенно остро. За 2021 г. произошло множество утечек пользовательских данных: от 533 млн записей базы пользователей Facebook до 1,75 млрд записей маркетплейса Hariexpress. Один из способов обеспечения безопасности данных – использование менеджера паролей.

Менеджер паролей – это специальное программное обеспечение, которое помогает работать с учётными данными различных сервисов и приложений.

В зависимости от места хранения базы паролей выделяют десктопные (место хранения – жёсткий диск компьютера), мобильные (место хранения – память смартфона, USB-накопитель) и сетевые (место хранения – хостинг сайта) менеджеры паролей.

Пользователь создаёт мастер-пароль, который используется как ключ шифрования хранилища паролей. Главное требование к ключу – высокая криптостойкость – устойчивость шифротекста к криптоанализу.

Шифрование – это процесс обратимого преобразования информации для сокрытия от третьих лиц. Важная особенность любого алгоритма шифрования – это использование ключа – информации для шифровки и дешифровки сообщения.

Проект «Программное обеспечение для хранения паролей» реализован на платформе .NETcore 3.1 в виде консольного приложения. Пользователю предоставляется возможность создавать локальные хранилища паролей в виде как зашифрованного, так и незашифрованного текстового файла. Учётные данные хранятся в формате «сервис»: «логин», «пароль».

В качестве алгоритма шифрования был использован симметричный шифр AES с длиной ключа 256 бит.

Для использования криптографических примитивов на платформе .NET применяется пространство имён System.Security.Cryptography. На высоком уровне данное пространство имён можно разделить на четыре основные части: алгоритмы шифрования (реализация симметричного и асимметричного шифрования, а также хеширования), вспомогательные классы (криптозащищённый генератор случайных чисел, взаимодействие с CryptoAPI, шифрование на основе потоковой модели), цифровые сертификаты и XML-подписи (цифровые подписи XML-документах).

Подводя итоги, следует отметить главное преимущество менеджеров паролей – сочетание удобства и безопасности хранения данных. Кроме того, менеджер паролей – обязательный отраслевой инструмент, позволяющий обеспечить надлежащий уровень безопасности данных и защиты от кибератак.