ПРОЕКТИРОВАНИЕ КРИПТОСИСТЕМЫ, ОСНОВАННОЙ НА АУТЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ЛИЦУ И ФЛЭШ КАРТЕ, С ИСПОЛЬЗОВАНИЕМ СЛУЖБЫ МЕЖПРОЦЕССНОГО ВЗАИМОДЕЙСТВИЯ

***Н.А. ГУРЕЦКИЙ*, О.В. ГОЛУБЕВА**

The practical way of creation of reliable cryptosystem with a non-standard way of storage of the password and authentication is presented in article. The purpose of work was writing of the program for protection of the user files with use a flash card as the password and authentication of the user on the person. The problem was solved by splitting the main program into libraries and auxiliary subprogrammes. The program is written in the C# programming language with use of Win32 API and library of recognition OpenCV

Ключевые слова: безопасность хранения информации, криптосистема, алгоритм шифрования, пароль, ключ, метод хранения пароля, аутентификация

Введение. В статье пойдёт речь о защите пользовательских файлов на персональном компьютере с применением шифрования и нестандартного метода хранения пароля, исключающего человеческий фактор. При этом подходе злоумышленник, даже завладев данными, воспользоваться ими без знания ключа и алгоритма шифрования не сможет.

Принцип разработанного алгоритма защиты информации и его функционал. В качестве алгоритма шифрования использован алгоритм Triple DES (3DES)[1]. Для генерации пароля и дальнейшей аутентификации, пользователю необходимо использовать USB флэш карту – первый уровень защиты. Также в настройке программы пользователю необходимо сделать фотографию своего лица для его дальнейшего распознавания – второй уровень защиты. Из логина и данных флэш карты получаем хеш длиной 1024 бит – он же и есть пароль для шифрования. Пользователю необходимо лишь один раз после полного включения компьютера вставить нужную флэш карту и сопоставить лицо и видеокамеру, после чего пароль будет храниться в стэке приложения.

Для удобства использования криптосистемы процесс аутентификации пользователя и хранение пароля вынесен в отдельную службу Windows [2]. Для общения службы с приложением дешифрования и открытия файлов используется межпроцессорное взаимодействие (англ. Inter-Process Communication, IPC [3]) – набор способов обмена данными между множеством потоков в одном или более процессах).

Аутентификация по лицу будет производиться с помощью технологии OpenCV [4]. OpenCV (англ. Open Source Computer Vision Library, библиотека компьютерного зрения с открытым исходным кодом).

Заключение. Авторами спроектирован программный продукт для надёжного хранения конфиденциальной, приватной, секретной информации на персональном компьютере, позволяющий пользователю комфортно проходить процедуру аутентификации. Для чего достаточно подключить нужную флэш-карту к компьютеру и показать лицо видеокамере. На данный момент ведутся работы по увеличению функционала программы.

Литература

1. Triple DES. [Электронный ресурс] – Режим доступа https://ru.wikipedia.org/wiki/Triple_DES . Дата обращения 08.12.2015.
2. Службы Windows. [Электронный ресурс] – Режим доступа https://ru.wikipedia.org/wiki/Службы_Windows. Дата обращения 19.12.2015.
3. Межпроцессное взаимодействие. [Электронный ресурс] – Режим доступа http://dic.academic.ru/dic.nsf/ruwiki/658474 . Дата обращения 10.01.2016.
4. OpenCV. [Электронный ресурс] – Режим доступа http://opencv.org . Дата обращения 12.01.2016.

МЕТОД КОНТРОЛЯ ПЛОТНОСТИ И ВЯЗКОСТИ УГЛЕВОДОРОДОВ В ПРОЦЕССЕ ОТБОРА ГЛУБИННОЙ ПРОБЫ

***Р.Е. ГУТМАН*, В.М. ТКАЧЕВ**

The present paper addresses the general problems which have to be faced with definition of properties of formation fluid. Physical properties of formation fluids play a major role in oil production industry. Physical properties of hydrocarbons in formation conditions are necessary for oil and gas deposits calculations, EOR and for aspects estimation of hydrocarbons fields, development and exploitation

Ключевые слова: углеводороды, контроль, вязкость

Данные о физико-химических свойствах углеводородов в пластовых условиях играют важную роль при разработке месторождений углеводородов. Физико-химические свойства углеводородов ис-