УДК 004.021

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

Н.А. ГУРЕЦКИЙ
(Представлено: канд. физ.-мат. наук, доц. О.В. ГОЛУБЕВА)

Представлен практический способ создания интерфейса для криптосистемы с использованием флэш-карты как пароля и распознаванием лиц. Целью работы явилось написание программы для защиты пользовательских файлов с использованием флэш карты в качестве пароля и аутентификации пользователя по лицу, а также создание интуитивно понятного пользовательского интерфейса. Задача реализации интерфейса решалась с использованием Windows Form и языка программирования C#.

В настоящий момент самым распространённым способом хранения информации является запись её на цифровые носители. Часть сохраняемой информации может быть конфиденциальной, приватной, секретной и нуждаться в защите. У такой информации есть законные пользователи. Но всегда существует вероятность появления пользователей незаконных, стремящихся захватить секретную информацию с целью обращения её себе во благо. Хакеры ежедневно воруют номера кредитных карт, банковские счета и даже личность человека. Опасаясь этого, законные пользователи принимают меры по защите информации.

На сегодняшний день известны несколько подходов к проблеме защиты информации, хранящейся в персональном компьютере. Один из них – шифрование данных.

Принцип разработанного алгоритма защиты информации и его функционал. В качестве алгоритма шифрования использован алгоритм Triple DES (3DES). Этот алгоритм, созданный Уитфилдом Диффи, Мартином Хеллманом и Уолтом Тачманном в 1978 году на основе алгоритма DES, представляет собой симметричный блочный шифр. Цель создания Triple DES – устранение главного недостатка алгоритма DES: недостаточной длины ключа (56 бит), который можно взломать полным перебором. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше. Время, требуемое для криптоанализа 3DES, может быть в миллиард раз больше, чем время, нужное для вскрытия DES [1].

Для генерации пароля, а затем и для дальнейшей аутентификации пользователю необходимо использовать USB флэш-карту – первый уровень защиты. Также в первоначальной настройке программы пользователю необходимо сделать фотографию своего лица для его дальнейшего распознавания – второй уровень защиты. Из логина и данных флэш-карты (каждая флэш-карта обладает уникальным сочетанием данных, вшитых в плату) получаем хеш длиной 1024 бит – он же и есть пароль для шифрования. В алгоритме 3DES в качестве пароля используется лишь 192 бит, поэтому хеш специальным алгоритмом урезаем до 192 бит. При аутентификации сверяться будут не пароли, а одно и то же слово, зашифрованное ими, причем правильный вариант будет храниться в защищенном разделе реестра. Пользователю необходимо лишь один раз после полного включения компьютера вставить нужную флэш-карту и поставить в соответствие лицо и видеокамеру, после чего пароль будет храниться в стэке приложения.

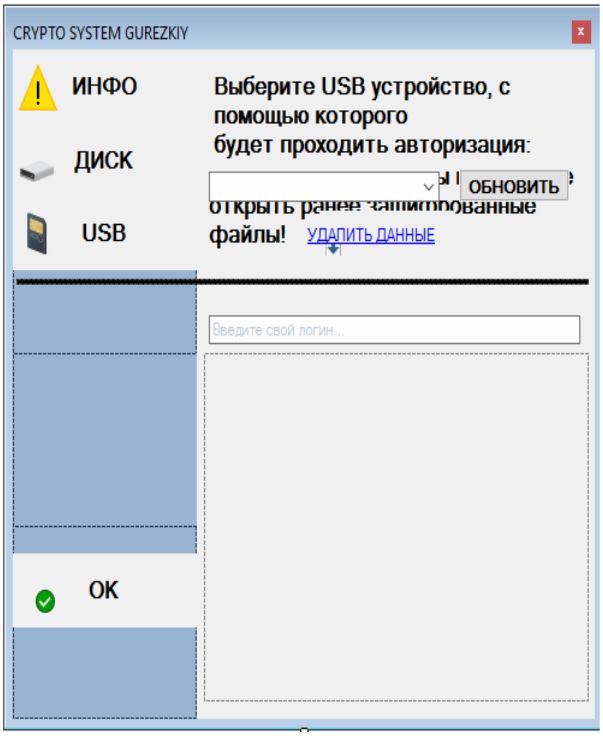

Рисунок 1. – Создание интерфейса CryproSystem.exe

Интерфейс программы CryptoSystem.exe создан с помощью Windows Form на языке программирования C# (рис. 1). На первый взгляд интерфейс кажется непонятным, однако не все эти элементы будут отображаться сразу. После некоторых настроек интерфейс будет выглядеть, как показано на рисунках 2–5. После настройки программы нужно нажать «OK». Изменения программы вступят в силу после перезагрузки компьютера. Если пользователь уже однажды настраивал эту программу, то перед настройкой необходимо удалить данные, нажав на строку «Удалить данные на вкладке ИНФО».

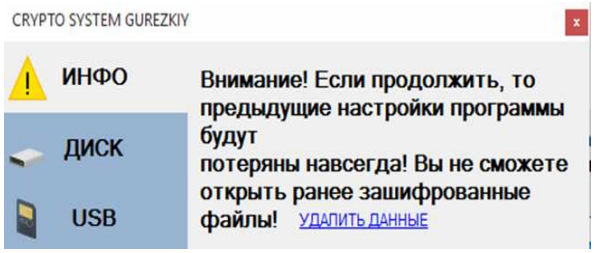

Рисунок 2. – Инфо

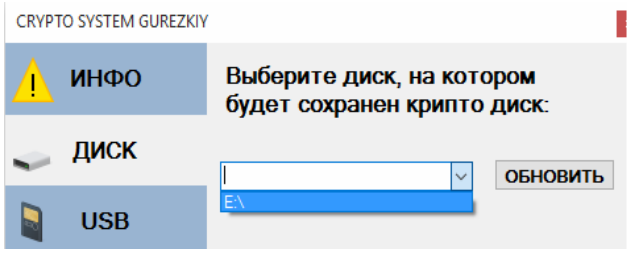

Рисунок 3. – Выбор диска для хранения папки с зашифрованными файлами

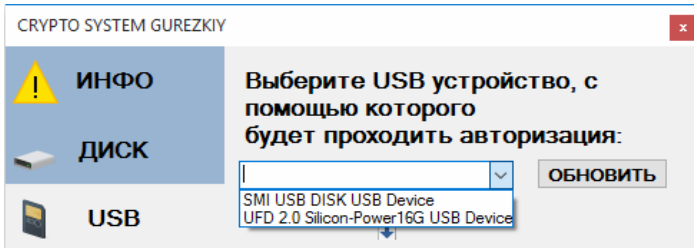

Рисунок 4. – Выбор флэш-карты

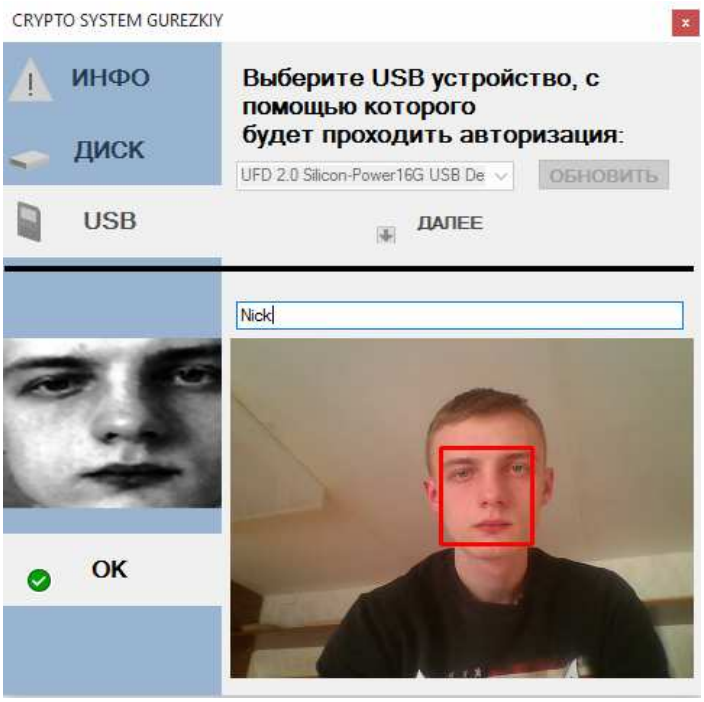

Рисунок 5. – Снимок лица пользователя

Заключение. Авторами разработан программный продукт для надёжного хранения конфиденциальной, приватной, секретной информации на персональном компьютере, позволяющий пользователю комфортно проходить процедуру аутентификации. Для этого 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 доступа: 08.12.2015.
2. Службы Windows [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Службы_Windows. – Дата доступа: 19.12.2015.
3. Межпроцессное взаимодействие [Электронный ресурс]. – Режим доступа http://dic.academic.ru/dic.nsf/ruwiki/658474. – Дата доступа: 10.01.2016.
4. OpenCV [Электронный ресурс]. – Режим доступа: http://opencv.org. – Дата доступа: 12.01.2016.
5. OpenCV [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/OpenCV. – Дата доступа: 3.01.2016.