УДК 004.021

ПРОЕКТИРОВАНИЕ 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 надёжной криптосистемы с нестандартным способом хранения пароля и аутентификации. Целью работы явилось написание программы для защиты пользовательских файлов с использованием флэш карты в качестве пароля и аутентификации пользователя по лицу. Задача решалась путём разбиения основной программы на библиотеки и вспомогательные подпрограммы. Программа написана на языке программирования C# с использованием Win32 API и библиотеки распознавания OpenCV.

В данной работе в качестве объекта исследования выступают пользовательские файлы 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. Разработанный программный продукт предназначен для быстрого и надёжного шифрования файлов, дешифрования, открытия без возможности внесения изменений, сокрытия этих файлов стандартными средствами Windows; использование надёжного ключа шифрования, который не знает даже сам пользователь.

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, необходимое 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 сопоставить лицо и видеокамеру, после чего пароль будет храниться в стэке приложения.

Для удобства использования этой криптосистемы процесс аутентификации пользователя и хранение пароля вынесен в отдельную службу Windows. Службы операционной системы Windows (англ. Windows Service, службы) – приложения, автоматически (если настроено) запускаемые системой при запуске Windows и выполняющиеся вне зависимости от статуса пользователя. Имеет общие черты с концепцией демонов в Unix [2].

Для общения службы с приложением дешифрования и открытия файлов необходимо использовать межпроцессорное взаимодействие. Межпроцессорное взаимодействие (англ. Inter-Process Communication, IPC) – набор способов обмена данными между множеством потоков в одном или более процессах.

Процессы могут быть запущены на одном или более компьютерах, связанных между собой сетью. IPC-способы делятся на методы обмена сообщениями, синхронизации, разделяемой памяти и удаленных вызовов (RPC). Методы IPC зависят от пропускной способности и задержки взаимодействия между потоками и типа передаваемых данных.

IPC также может упоминаться как межпотоковое взаимодействие (англ. inter-thread communication), межпоточное взаимодействие и межпрограммное взаимодействие (англ. inter-application communication). IPC наряду с концепцией адресного пространства является основой для разграничения адресного пространства [3].

Аутентификация по лицу будет производиться с помощью технологии OpenCV [4]. OpenCV (англ. Open Source Computer Vision Library, библиотека компьютерного зрения с открытым исходным кодом) – библиотека алгоритмов компьютерного зрения, обработки изображений и численных алгоритмов общего назначения с открытым кодом. Реализована на C/C++/C#, также разрабатывается для Python, Java, Ruby, Matlab, Lua. Может свободно использоваться в академических и коммерческих целях – распространяется на условиях лицензии BSD [5].

Логика работы приложения представлена на рисунке 1.

Рисунок 1. – Логика работы приложения

Для экономии ресурсов и удобства работы вся программа разбита на несколько отдельных подпрограмм:

- служба Windows CryptoServiceGurezkiy.exe для мониторинга подключенных флэшек, аутентификации пользователя, мониторинга появления новых файлов на виртуальном диске и шифрования этих файлов, а также для выдачи пароля другим программам по IPC;
- программа cryper.exe для расшифровывания файлов и их копирования;
- CryptoSystem.exe для настройки приложения.

Так как эти программы используют схожий функционал, то целесообразно вынести все классы и методы в общую библиотеку классов, причём в несколько разных.

Библиотеки:

- библиотека Crypto3DES.dll для шифрования и расшифровки файлов;
- библиотека InterComunication.dll для общения службы CryptoServiceGurezkiy.exe и cryper.exe;
- библиотека LogicApp.dll для хранения общей логики программы и классов для хеширования данных, распознавания флэшек в системе, работы с реестром, сохранения изображения лица пользовате-

ля, распознавания лица пользователя, монтирования папки в качестве виртуального диска, отслеживания изменений в файловой системе виртуального диска.

Общая схема зависимостей показана на рисунке 2.

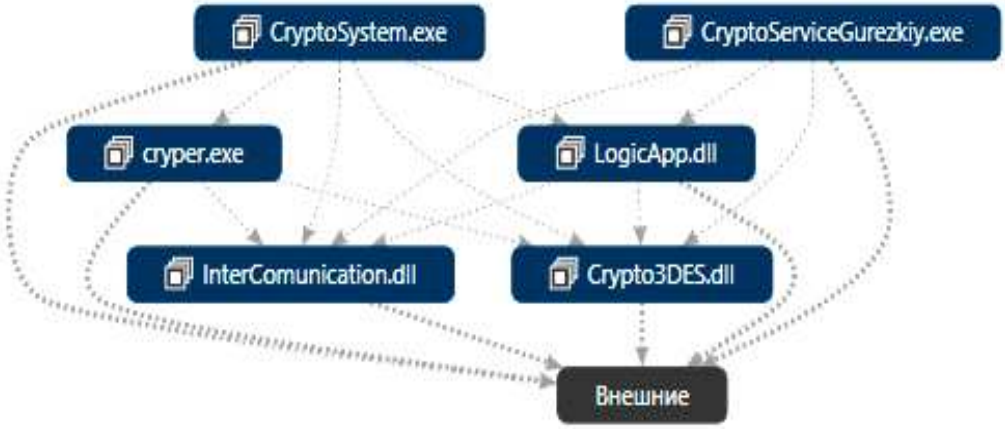

Рисунок 2. – Схема зависимостей проекта

Заключение. Авторами спроектирован 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: 13.01.2016.