Криптиращо приложение

Инструкция за работа с криптиращото приложение *CryptorPhi1*

1. **Въведение**

Криптиращото приложение *CryptorPhi1* е разработено като част от *Процедурата ОКИ-101*[[1]](#footnote-1). По-конкретно, то е предназначено за изпълнението на криптиране ФАЗА1 (*Процедура ОКИ-101*, т. 4) от страна на TM/60K на определени колони от контактния файл с КЛЮЧ1, известен единствено на TM/60K.

За разлика от разпространените криптиращи приложения, криптиращото приложение *CryptorPhi1* е съобразена със спецификата на телемаркетинг кампаниите. Криптира съдържанието на файла не като цяло, а по редове, с оглед запазване на структурираността на информацията в необходимата степен, като всеки ред отговаря на записа за конкретно контактно лице.

Заложеният подход, представен във файла *ПРЕЗЕНТАЦИЯ.СНС2019.183706.pptx*, се основава на *схема за защита на личните данни* чрез разделянето на канала за лични данни от канала с управляващата информация (номер и име на кампанията, име на Възложителя, име на контактния файл, дата/час на импортиране, диспозиции и т.н.).

Криптиращото приложение *CryptorPhi1* съдържа три основни модула:

* Модул за избирателно криптиране/декриптиране (ENC/DEC), изпълнен чрез библиотечния клас *Cryptor*, разработен в рамките на провежданите работи;
* Модул за достъп до файловата система;
* Операторски интерфейс.

В този документ се описва накратко операторският интерфейс и редът за работа.

Текущата версия[[2]](#footnote-2) на криптиращото приложение *CryptorPhi1* предполага неговата автономна работа. Впоследствие са възможни допълнения за осигуряване на по-висока степен на автоматизация при работата на персонала на TM/60K с криптираната в системната БД информация.

1. **Функционалност**

Процедурата ОКИ-101 предполага единствено криптиране на контактни файлове от типа .XLSX.

С оглед тестването на модула за избирателно криптиране/декриптиране (ENC/DEC), изпълнен чрез разработения библиотечен клас *Cryptor*, обаче се поддържат няколко формати на входните файлове, подлежащи на криптиране - TXT, BIN, WAV, WMA, XLSX.

Поддръжката на WAV и WMA форматите е свързана с тестване на възможността за последващото автоматично криптиране/декриптиране на аудиофайловете, генерирани от клиентското CTI приложение при приключването на всеки един разговор.

Файловете с разширение BIN са произволни двоични файлове.

На фиг. 1 е показано съответствието на разширенията на входния (отворения) файл и изходния (криптирания) файл.

|  |  |
| --- | --- |
| Разширения на файловете | |
| Входен (отворен) файл | Изходен (криптиран) файл |
| TXT | TXT |
| BIN | BI\_ |
| XLSX | CSV |
| WAV | WA\_ |
| WMA | WM\_ |
| BIN | BI\_ |

Фиг. 1. Съответствия на файловите разширения

1. **Файлова структура**

Основната работна папка *Cryptor* на приложението може да се разположи на произволно устройство – *C*, *D* или друго, по избор на оператора.

Папката *Cryptor* съдържа изпълнимия модул *CryptorPhi1.exe* и две поддиректории – *DOC* и *SAMPLES*.

Изпълнимият модул *CryptorPhi1.exe* е самостоятелен, не използва външни библиотеки и не изисква инсталация/деинсталация.

Папката *DOC* съдържа документацията за самото приложение, а папката *SAMPLES* – обработваните файлове.

Папката *SAMPLES* е включена единствено за илюстрация. В случая тази папка има две примерни поддиректории – *BIN* и *TEXT*. Папката BIN е пример за разполагане на двоични файлове, а папката *TEXT* – за текстови файлови. Тези имена не са задължителни и се определят от начина на работа на оператора. Добре е обаче да се съблюдава стремеж към структурираност[[3]](#footnote-3).

Един възможен вариант е например операторът да създаде отделна поддиректория на папката *Cryptor* за контактните файлове на всеки един проект.

Друг възможен, а може би и най-добър, вариант е да се работи с поддиректория, извън папката *Cryptor*, в която операторът поначало разполага подготвените за импортиране контактни файлове.

Папката *ENC* е поддиректория на папката, в която е избраният за криптиране файл. Създава се автоматично от самото криптиращо приложение и съдържа криптираните версии на файловете.

Поддиректория *DEC* е поддиректория на папката, в която е избраният за декриптиране файл. Създава се автоматично от самото криптиращо приложение и съдържа декриптираните версии на файловете.

За да може да се декриптира XLSX файл, в родителската ENC папка, съдържаща криптираната CSV версия на файла, предварително трябва да се копира шаблона *temp.xltx*. Общият вариант на този шаблон не съдържа форматиране, вследствие на което, след декриптирането ще се загуби форматирането на оригиналния файл[[4]](#footnote-4). Това обаче не пречи на нормалната работа в рамките на CTI системата, където това форматиране не се използва. Ако се налага, по някаква причина, да се запази форматирането, шаблона *temp.xltx* трябва предварително да се получи от оригиналния контактен файл.

1. **Подготвителни работи**

От Интернет ресурса <https://1drv.ms/f/s!AkU4-3af4I0PlO1FZdp1QUX57ehwlQ> се маркира и изтегля папката *Cryptor*. Полученият архив *Cryptor.zip* се разархивира на избраното дисково устройство (т. 4).

Изпълнимият модул *CryptorPhi1.exe* може да се стартира от самата основна работна папка *Cryptor*, но може за удобство към него да се направи препратка (*shortcut*) на работния екран.

1. **Ред на работа**

След стартирането на изпълнимия модул, криптиращото приложение *CryptorPhi1* се отваря в долния десен ъгъл на работния екран, като се разполага в системния панел (*system tray*).

Щом приложението се скрие в системния панел (*system tray*), то се управлява чрез контекстното меню. Достъпни са командите:

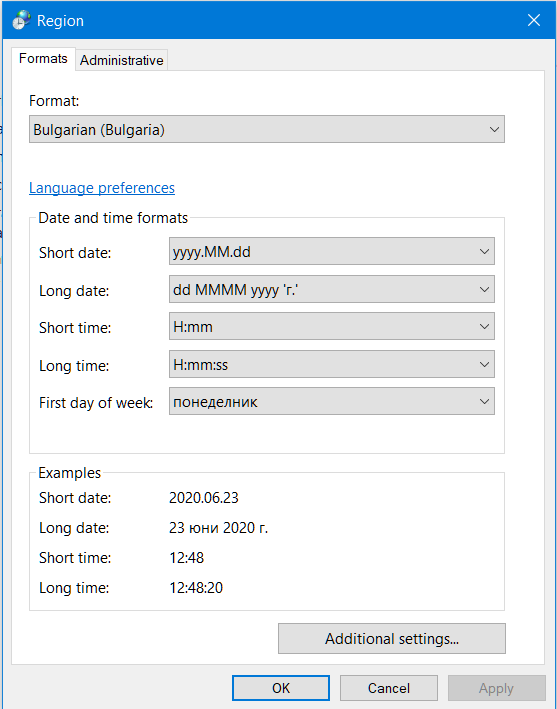
* Open, за визуализация на приложението;
* Close, за затваряне на приложението;
* Src, за визуализацията на приложението в режим *SRC*.

Работата на приложението се управлява от единствен бутон, в който се изписва кода на избрания режим на работа. Поддържаните режими на работа са приведени на фиг. 2.

|  |  |
| --- | --- |
| Режими на работа | |
| Код | Режим |
| SRC | Избор на входен файл |
| ENC TXT | Криптиране на TXT файл |
| DEC TXT | Декриптиране на TXT файл |
| ENC XLS | Криптиране на XLSX файл |
| DEC CSV | Декриптиране на XLSX файл |
| ENC WAV | Криптиране на WAV файл |
| DEC WA\_ | Декриптиране на WAV файл |
| ENC WMA | Криптиране на WMA файл |
| DEC WM\_ | Декриптиране на WMA файл |
| ENC BIN | Криптиране на BIN файл |
| DEC BI\_ | Декриптиране на BIN файл |

Фиг. 2. Режими на работа

Преди криптирането на XLSX файлове, в регионалните настройки като Short date format трябва да се зададе yyyy.MM.dd, както е показано на фиг. 3.



Фиг. 3. Регионални настройки

Началният режим e *SRC*. В зависимост от избрания тип файл, приложението превключва автоматично в съответния режим на работа. Ако операторът реши да се откаже от избрания режим, през контекстното меню се връща отново в началния режим *SRC*.

Вляво от управляващия бутон се намери плъзгача *Slider*. Той е управляващ панел, който нормално е скрит. Отваря се, чрез приплъзване хоризонтално вдясно при еднократно щракване по левия му ръб. Скрива се обратно чрез приплъзване вдясно чрез последващо еднократно щракване по левия му ръб или в неактивен участък на самия плъзгач.

Плъзгачът *Slider* служи за задаване на паролата чрез редакторското поле *Key*. Паролата се визуализира чрез щракване и задържане на мишката върху символа , разположен вляво от паролата.

Ако е полето *Password Strength* е маркирано, не се допуска паролата да бъде по-къса от 10 символа.

Полето *Process First Row* се използва при криптирането на XLSX файлове. При контактните файлове, с които се работи, първият ред не подлежи на криптиране. В този случай полето *Process First Row* не трябва да се маркира.

Полето *Process First Col* се използва при криптирането на XLSX файлове. При контактните файлове, с които се работи, първата колонка не подлежи на криптиране. В този случай полето *Process First Col* не трябва да се маркира.

Полето *Check Only Mode* се маркира, ако се изисква да се провери целостта на избрания криптиран файл, без при това да се декриптира. Може да се използва за проверка целостта на криптираните в CSV формат XLSX файлове.

Ако текущата обработка е по-продължителна, нейното развитие се визуализира чрез прогрес-лентата, разположена успоредно на долния хоризонтален ръб на управляващия плъзгач.

Преди изключване на компютъра не е необходима приложението да се затваря. Достатъчно е да е завършила текущата обработка.

1. **Заключение**

Предстои интегрирането на модула за избирателно криптиране/декриптиране (ENC/DEC) в операторската система eMOSys.6K, което предполага значителни промени в клиентското CTI приложение WSeMOSys.6K и в таблиците на системната БД[[5]](#footnote-5).

Сложността на тези работи се определя от два възлови момента:

* Необходимостта от прекомпилиране на клиентското CTI приложение с последната версия на инструменталната среда за разработка *C++ Builder*;
* Възможни допълнения в криптиращото приложение *CryptorPhi1* с оглед по-висока степен на автоматизация при работата на персонала на TM/60K с криптираната в системната БД информация;
* Необходимостта от поетапни промени, проект по проект, с оглед изискването за постепенен преход към пълно покритие на схемата за защита без нарушаване на текущата работа по телемаркетинг кампаниите.

Наличието на модула за избирателно криптиране/декриптиране (ENC/DEC) и неговото практическо тестване гарантират в значителна степен постигането на поставената цел – осигуряването на допълнително ниво на защита на личните данни.

ТТ/МЛ

2020.06.23

2019.06.04

2019.05.28

1. Актуалният вариант на тази процедура към текущия момент се съдържа във файла *ПРОЦЕДУРА.ОКИ-101.20190102.docx*. [↑](#footnote-ref-1)
2. Към текущия момент това е версия 3.1.4.8. [↑](#footnote-ref-2)
3. Пътят до файла, включително названието на файла, трябва да се състоят само от символи на латиница. Това ограничение не ми допада (бел. ТТ/МЛ). Впоследствие ще се постарая да го отстраня. [↑](#footnote-ref-3)
4. Всъщност, за съдържанието на шаблона *temp.xltx* е зададен текстови формат, за да не се получава изкривяване на декриптираното съдържание, вследствие на автоматичното преобразуване, извършвано от Excel. [↑](#footnote-ref-4)
5. Схемата на покритие е показана на слайд 18 (ИЗВОДИ 2) от файла *ПРЕЗЕНТАЦИЯ.СНС2019.183706.pptx*. [↑](#footnote-ref-5)