Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Системное программирование

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

на тему:

**ПРОГРАММНОЕ СРЕДСТВО «ПРИЛОЖЕНИЕ ДЛЯ РАБОТЫ С ШИФРОВАННЫМИ ФАЙЛАМИ»**

БГУИР КП 1-40 01 01 015 ПЗ

Студент Маталыга Е.А.

Руководитель Алексеев И.Г.

Минск 2024

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** 5](#_Toc184367722)

[**1 АНАЛИЗ ПРОТОТИПОВ** 6](#_Toc184367723)

[**1.1 Cryptomator** 6](#_Toc184367724)

[**1.2 Encrypto** 7](#_Toc184367725)

[**2 ФОРМИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К РАЗРАБАТЫВАЕМОМУ ПРОГРАММНОМУ СРЕДСТВУ** 8](#_Toc184367726)

[**2.1 Описание и спецификация функциональных требований** 8](#_Toc184367727)

[**2.2 Используемые ресурсы** 8](#_Toc184367728)

[**3 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО СРЕДСТВА** 9](#_Toc184367729)

[**3.1 Структура программы** 9](#_Toc184367730)

[**3.2 Проектирование пользовательского интерфейса** 9](#_Toc184367731)

[**3.3 Проектирование функционала программного средства** 12](#_Toc184367732)

[**4 РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА** 16](#_Toc184367733)

[**4.1 Шифрование** 16](#_Toc184367734)

[**4.2 Добавление нового хранилища** 16](#_Toc184367735)

[**4.3 Добавление файла в хранилище** 18](#_Toc184367736)

[**4.4 Отображение файлов в хранилище** 19](#_Toc184367737)

[**4.5 Вспомогательные функции** 19](#_Toc184367738)

[**5. ТЕСТИРОВАНИЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ ПРОГРАММНОГО СРЕДСТВА** 21](#_Toc184367739)

[**6 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ** 24](#_Toc184367740)

[**6.1 Интерфейс программного средства** 24](#_Toc184367741)

[**6.2 Управление хранилищем** 26](#_Toc184367742)

[**ЗАКЛЮЧЕНИЕ** 29](#_Toc184367743)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 30](#_Toc184367744)

[**Приложение А** 31](#_Toc184367745)

# **ВВЕДЕНИЕ**

В современном цифровом мире безопасность информации становится одной из ключевых задач, стоящих перед пользователями и организациями. С ростом объема передаваемых и хранимых данных возрастает необходимость в надежных методах защиты конфиденциальной информации. Шифрование файлов представляет собой один из самых эффективных способов обеспечить безопасность данных, позволяя защитить их от несанкционированного доступа и утечек.

Цель данного курсового проекта заключается в разработке приложения для работы с шифрованными файлами, которое будет обеспечивать пользователям простоту и удобство в использовании, а также высокую степень безопасности. Приложение будет включать функциональность для шифрования и дешифрования файлов, а так же создания и управления хранилищами зашифрованных файлов.

Задачи курсовой работы включают:

1. Реализация алгоритма шифрования и дешифрования
2. Обеспечение безопасного хранения ключей
3. Создание пользовательского интерфейса для удобной работы с приложением.
4. Проведение тестирования и анализа безопасности разработанного приложения

Ожидается, что разработанное приложение станет полезным инструментом для пользователей, стремящихся защитить свои данные от потенциальных угроз, и повысит осведомленность о важности применения современных методов шифрования.

# **1 АНАЛИЗ ПРОТОТИПОВ**

## **1.1 Cryptomator**

Разработанное в ходе выполнения курсовой работы приложение основано на уже существующем приложении для работы с шифрованными файлами «Cryptomator».

Cryptmator является полностью бесплатным и свободным ПО, с открытым исходным кодом, для шифрования данных на стороне клиента.

К плюсам Cryptomator можно отнести:

1. Использование AES с 256 битным ключом
2. Пароль от хранилища защищен от брут-форс атак с помощью scrypt
3. Создание и управление несколькими хранилищами одновременно
4. Может работать с облачными хранилищами (при условии что на компьютере уже смонтирована папка облачного хранилища)
5. Прост в установке, прост в использовании

С помощью Cryptomator можно надежно защитить свои данные, поместив их в зашифрованные хранилища. Получить доступ к данным может только тот, кто знает пароль к хранилищу. При открытии хранилища с помощью Cryptomator, оно будет отображаться как виртуальный накопитель. С ним можно работать как с обычной USB-флешкой.

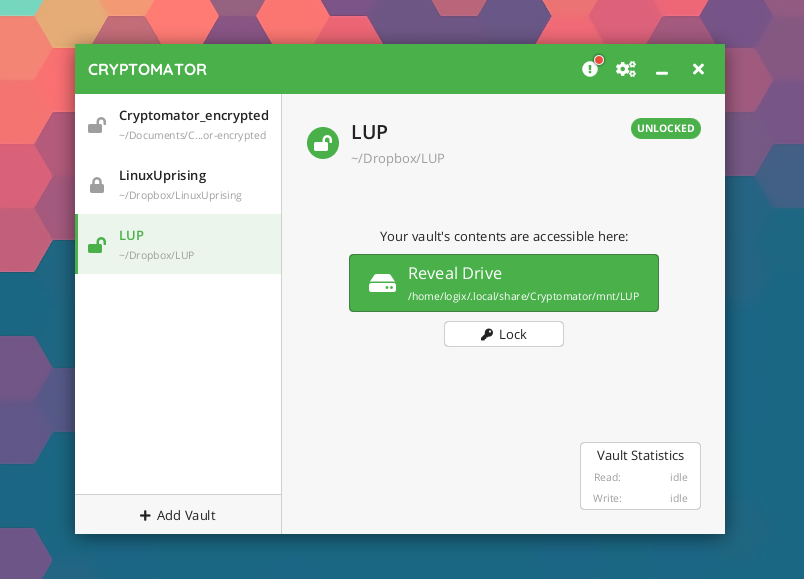


Рис. 1.1 – Интерфейс приложения Cryptomator

Зашифрованные данные хранятся в обычной папке. Если открыть хранилище без Cryptomator, то будет отображён только набор каталогов и файлов с непонятными именами. Распознать что это хранилище Cryptomator можно по файлу masterkey.cryptomator, который находится внутри папки.

## **1.2 Encrypto**

Encrypto – приложение для шифрования и дешифрования файлов с минимальным функционалом. После запуска приложения на экране компьютера появляется небольшое окно. Туда нужно переместить файл, который небходимо зашифровать. Переместив его, необходимо ввести пароль и кодовый вопрос (по желанию). Приложение начнёт процесс шифровки, по окончании которого представит вам файл с расширением .crypto. Для расшифровки файла достаточно ввода ключа в приложении.

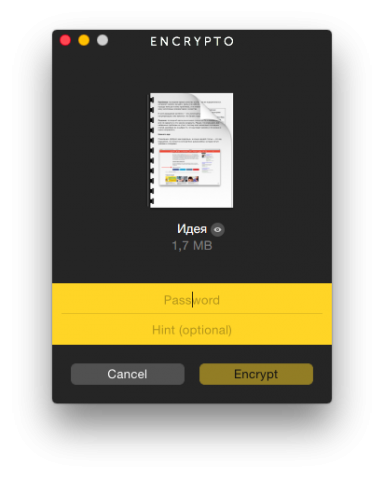


Рис. 1.2 – Интерфейс приложения Encrypto

К достоинствам Encrypto можно отнести:

1 Использование AES с 256 битным ключом;

2 Простота в установке и использовании;

3 Высокая скорость работы.

# **2 ФОРМИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К РАЗРАБАТЫВАЕМОМУ ПРОГРАММНОМУ СРЕДСТВУ**

# **2.1 Описание и спецификация функциональных требований**

Основные требования к функционалу программного средства:

1 Корректное шифрование и дешифрование файлов;

2 Работа с файлами любых форматов;

3. Создание хранилищ;

4 Работа с файлами хранилища:

− Добавление;

− Удаление;

− Экспорт;

5 Обработка удаления хранилища;

6 Безопасное хранение ключей к хранилищу;

7 Безопасное хранение файлов хранилища.

## **2.2 Используемые ресурсы**

В данном курсовом проекте для разработки приложения, создающего зашифрованные хранилища, будут использованы язык программирования C++ и WinAPI. C++ обеспечивает высокую производительность и гибкость, позволяя разрабатывать эффективный код, в то время как WinAPI предоставляет необходимые функции для работы с интерфейсом Windows и системными ресурсами. Стандартная библиотека C++ упростит работу с данными и вводом/выводом. Для компиляции и отладки приложения будет использована интегрированная среда разработки Microsoft Visual Studio, что обеспечит удобство работы и доступ к инструментам для тестирования.

# **3 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО СРЕДСТВА**

## **3.1 Структура программы**

Вся логика работы приложения содержится в файле «CryptoPanda.cpp». Помимо основного файла используется так же класс Encoder, в котором реализована логика генерации ключевой последовательности, шифрование и дешифрование файла.

## **3.2 Проектирование пользовательского интерфейса**

При разработке программного средства за основу будет взят дизайн приложения Crypromator.

Среди основных действий пользователя можно выделить следующие:

1 Создание хранилища;

2 Просмотр содержимого хранилища;

3 Добавление файла в хранилище;

4 Удаление файла из хранилища;

5 Экспорт файла из хранилища;

6 Блокировка и разблокировка хранилища.



Рис. 3.1 − Основные действия пользователя

**3.2.1** Главное окно

Главное окно приложение должно состоять из двух основных частей: списка уже созданных пользователем хранилищ с кнопкой создания нового хранилища и рабочей область, которая при открытии приложения является пустой, но, по мере работы в приложении, её содержимое должно меняться. Макет окна представлен на рисунке 3.2.

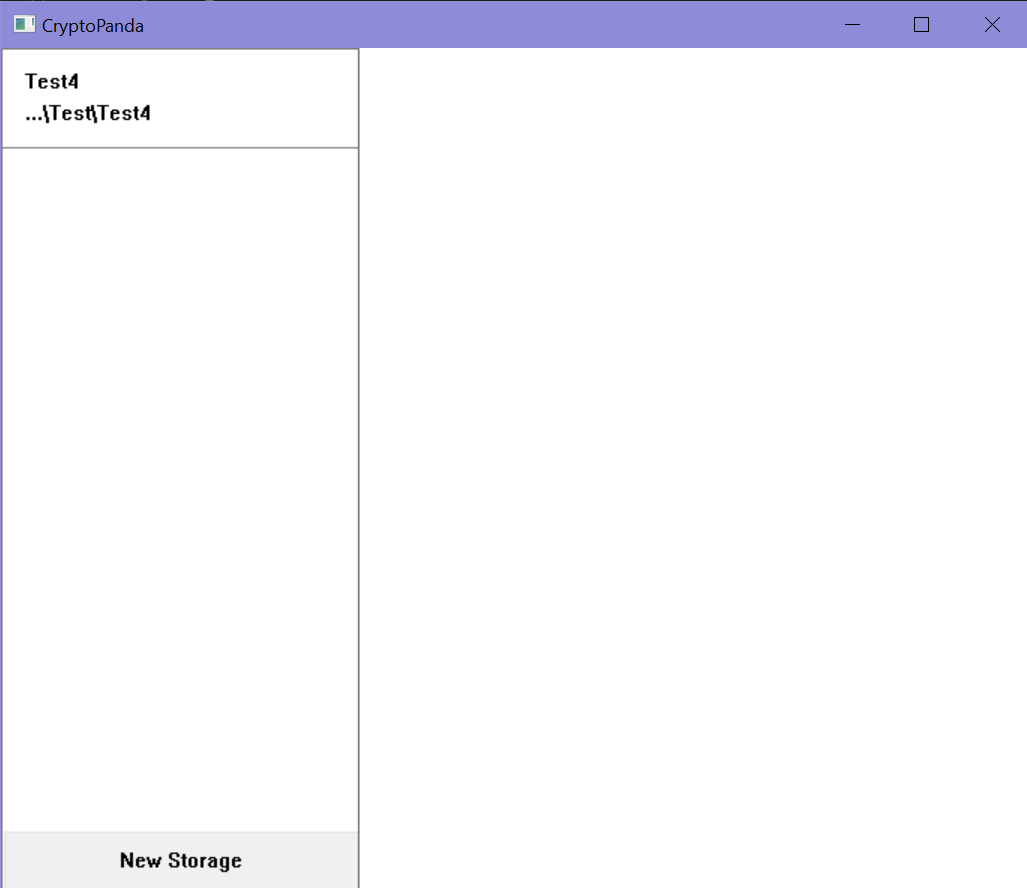


Рис 3.2 − Главное окно

**3.2.2** Окно создания хранилища

Окно создания хранилища должно открываться на месте рабочей области главного окна при нажатии на кнопку «New Storage». Для создания нового хранилища необходимо будет ввести путь к директории, в которой должно быть создано нового хранилище, имя хранилища и пароль, который будет необходим для разблокировки хранилища и которым будут шифроваться все файлы в хранилище. Макет окна представлен на рисунке 3.3.

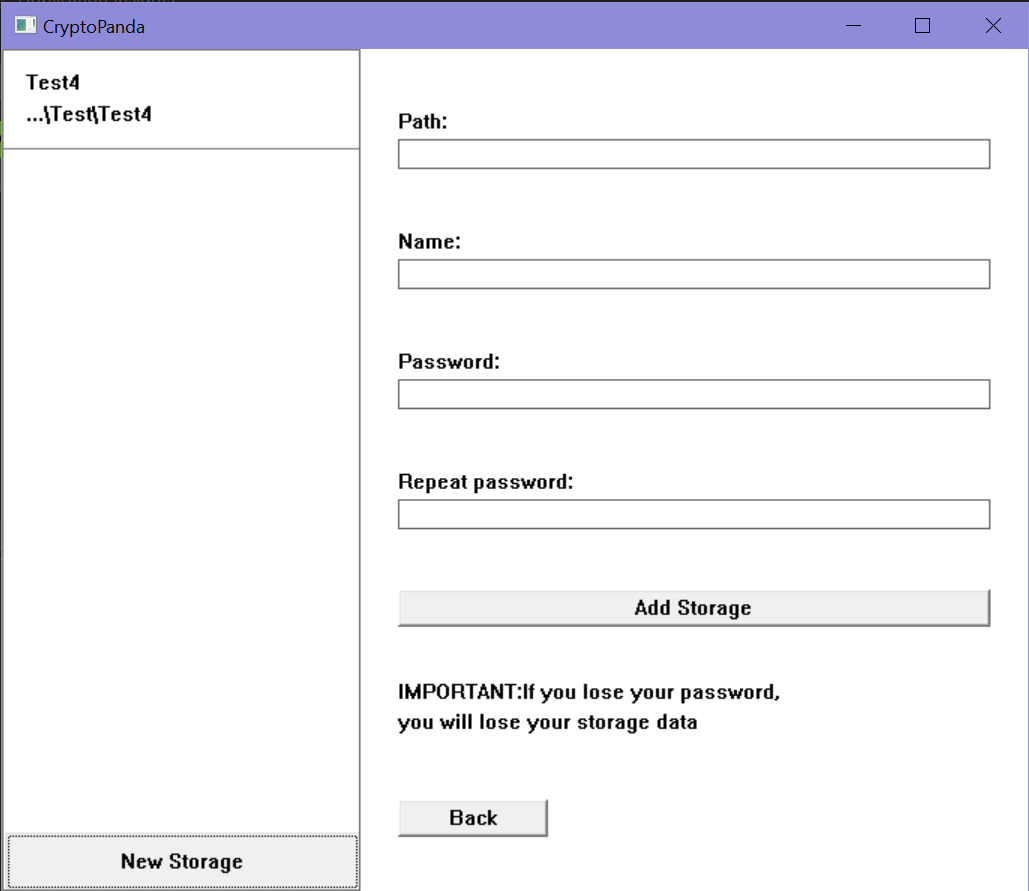


Рис. 3.3 − Окно создания нового хранилища

**3.2.3** Окно просмотра содержимого хранилища

Окно просмотра так же должно открываться на месте рабочей области основного окна. У пользователя должна быть возможность просмотреть список всех файлов, которые лежат в хранилище, с расшифрованными именами, добавить новый файл, заблокировать хранилище, чтобы для повторного входа требовался пароль, а так же удалить или экспортировать файл из хранилища в расшифрованном виде. Макет страницы представлен на рисунке 3.4.

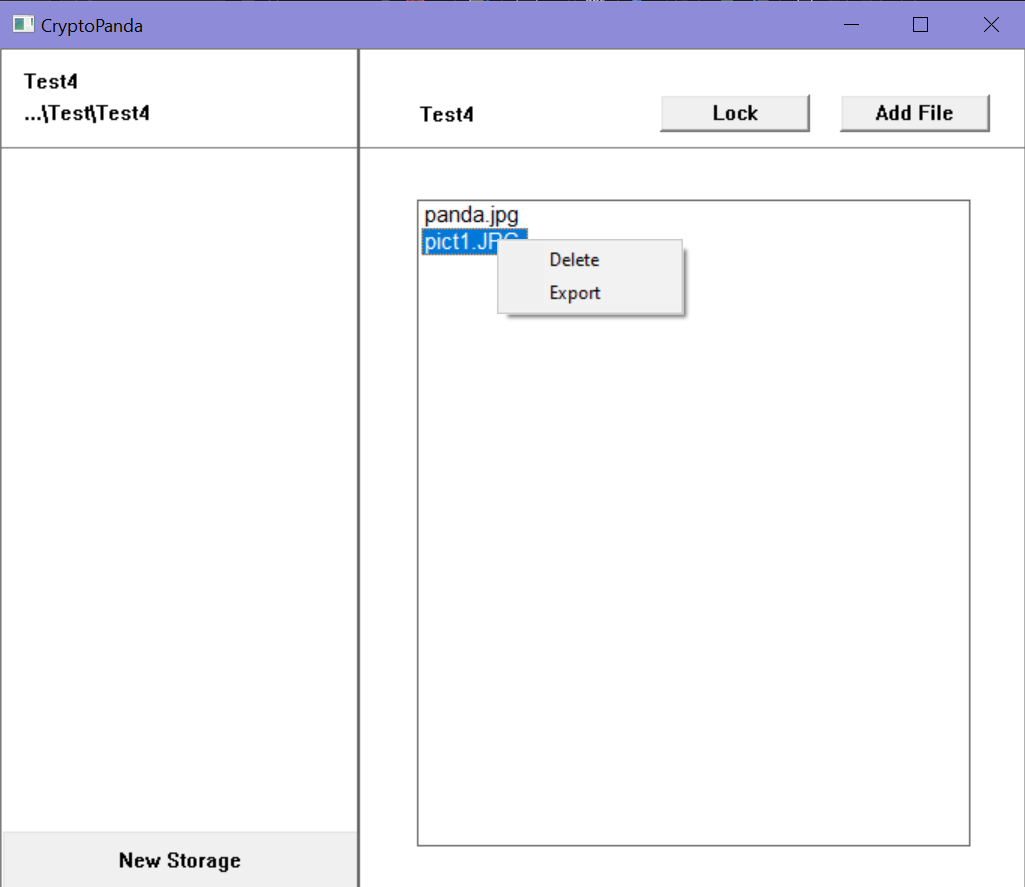


Рис. 3.4 − Окно просмотра содержимого хранилища

**3.2.4** Дополнительные окна

Помимо основных окон, в которых реализуется основная логика работы приложения, должны быть так же и дополнительные окна для ввода пароля при разблокировке приложения и добавления файла в хранилище.

Окно для ввода пароля должно указывать, доступ к какому хранилищу пользователь хочет получить доступ, и содержать всего одно поле и кнопки подтверждения и отмены операции. Макет окна представлен на рисунке 3.5.

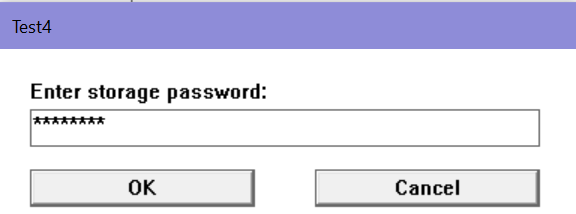


Рис. 3.5 – Макет окна для ввода пароля от хранилища

Окно добавления файла в хранилище должно иметь поля для ввода пути к файлу, который нужно зашифровать, и поле для ввода имени, под которым этот файл будет отображаться в хранилище при его открытии в приложении. В окне должны так же быть кнопки для подтверждения и отмены операции. Макет окна представлен на рисунке 3.6.

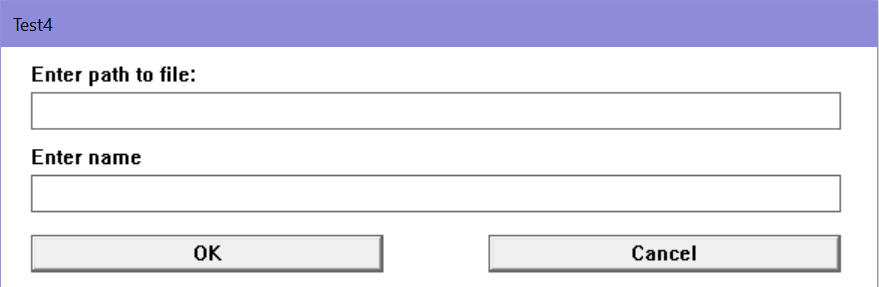


Рис. 3.6 − Окно добавления файла в хранилище

## **3.3 Проектирование функционала программного средства**

**3.3.1** Алгоритм шифрования

В данном курсовом проекте для реализации защиты данных используется потоковое шифрование с операцией XOR. Этот метод шифрования обеспечивает высокий уровень безопасности при относительно низких затратах на вычисления. Основной принцип заключается в том, что каждый бит исходных данных шифруется с помощью соответствующего бита псевдослучайной последовательности.

В качестве ключа для шифрования используется псевдослучайная последовательность, которая генерируется на основе ключа пользователя. Эта последовательность создается с помощью линейного генератора с обратной связью (LFSR), заданного определённым примитивным многочленом.

Для генерации ключевой последовательности был выбран LFSR, т.к. он достаточно просто реализуется в программном и аппаратном виде, обладает высокой скоростью генерации и большим периодом ключа. Регистр LFSR состоит из двух частей: сдвигового регистра, выполняющего сдвиг своих разрядов влево на один разряд, и функции обратной связи, вычисляющей вдвигаемое в первый разряд значение.

Преимущества такого подхода:

1 Скорость. Потоковое шифрование позволяет быстро обрабатывать данные;

2 Гибкость. Поддержка шифрования данных произвольных размеров;

3 Простота реализации. Алгоритм легко реализовать и адаптировать под различные требования;

4 Одинаковая процедура шифрования и дешифрования.

На рисунке 3.7 представлена схема шифрования и дешифрования файла и сохранения результата.

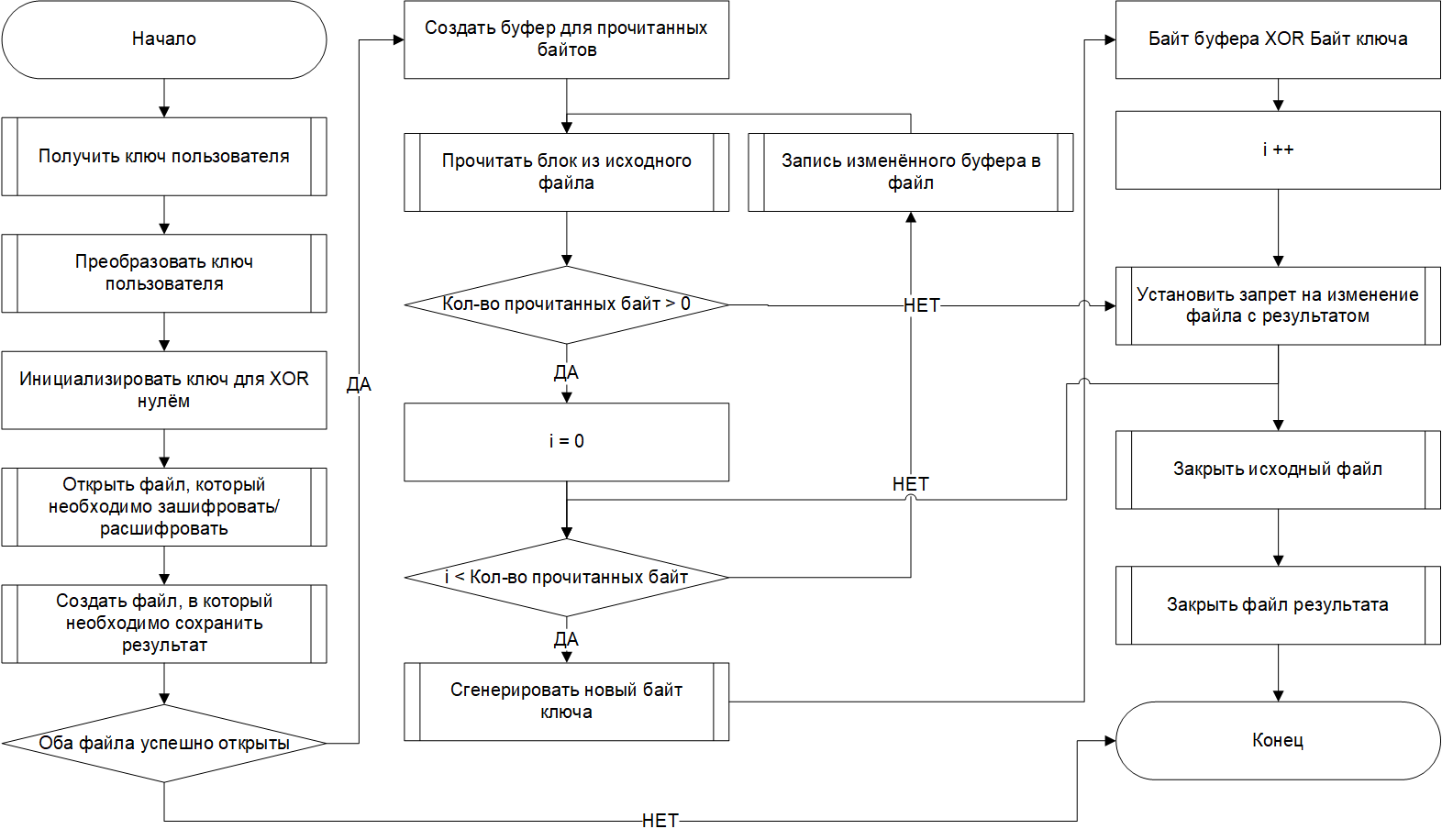


Рис. 3.7 − Алгоритм шифрования файла

**3.3.2** Хранение ключей

Все ключи, которые пользователь задаёт при создании хранилища, не хранятся в открытом виде, а шифруются при помощи DPAPI и сохраняются в зашифрованном виде в бинарном файле.

Data Protection API (DPAPI) — это встроенный механизм шифрования в операционной системе Windows, предназначенный для защиты конфиденциальной информации, такой как ключи шифрования, пароли и другие чувствительные данные. DPAPI обеспечивает простой и безопасный способ шифрования данных, используя системные ключи, которые могут быть связаны с конкретной учётной записью или машиной.

DPAPI предоставляет разработчикам API для шифрования и расшифровки данных с использованием двух основных функций:

1 CryptProtectData: Эта функция используется для шифрования данных. Она принимает открытые данные, которые нужно защитить, и возвращает зашифрованные данные.

2 CryptUnprotectData: Эта функция используется для расшифровки данных. Она принимает зашифрованные данные и возвращает исходные открытые данные.

Функции DPAPI используются на двух этапах: при создании нового хранилища и при разблокировке хранилища (рисунок 3.8).

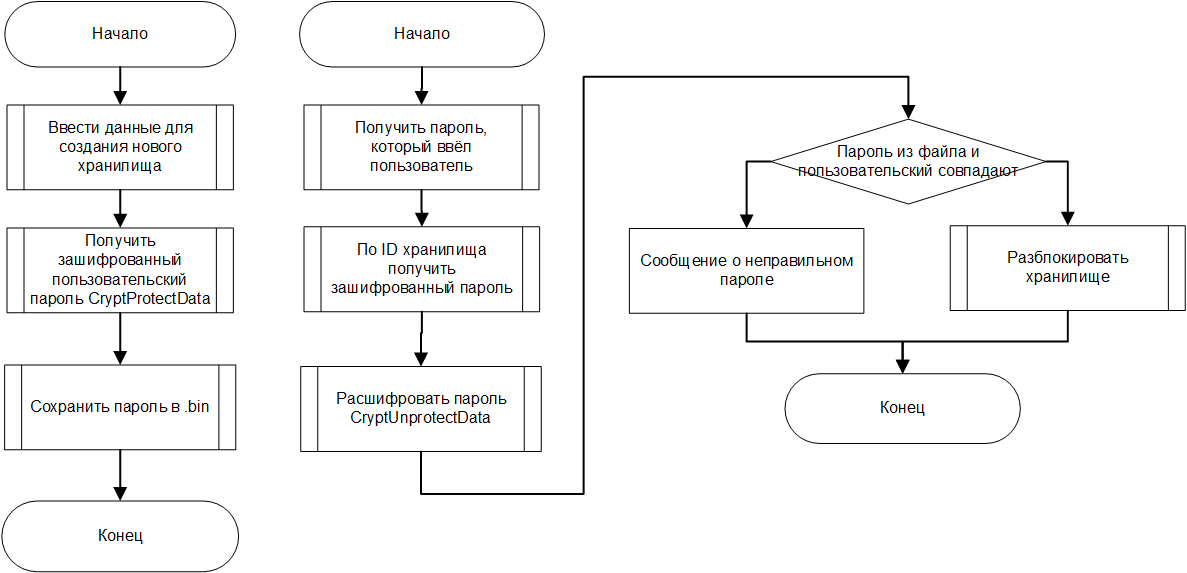


Рис. 3.8 − Использование функций DPAPI

**3.3.3** Управление хранилищем

В разблокированном хранилище пользователь может выполнять следующие действия:

1 Заблокировать хранилище, чтобы при следующем открытии требовался пароль

2 Добавить файл в хранилище

3 Удалить файл из хранилища

4 Экспортировать файл из хранилища

Схема управления хранилищем представлена на рисунке 3.9.

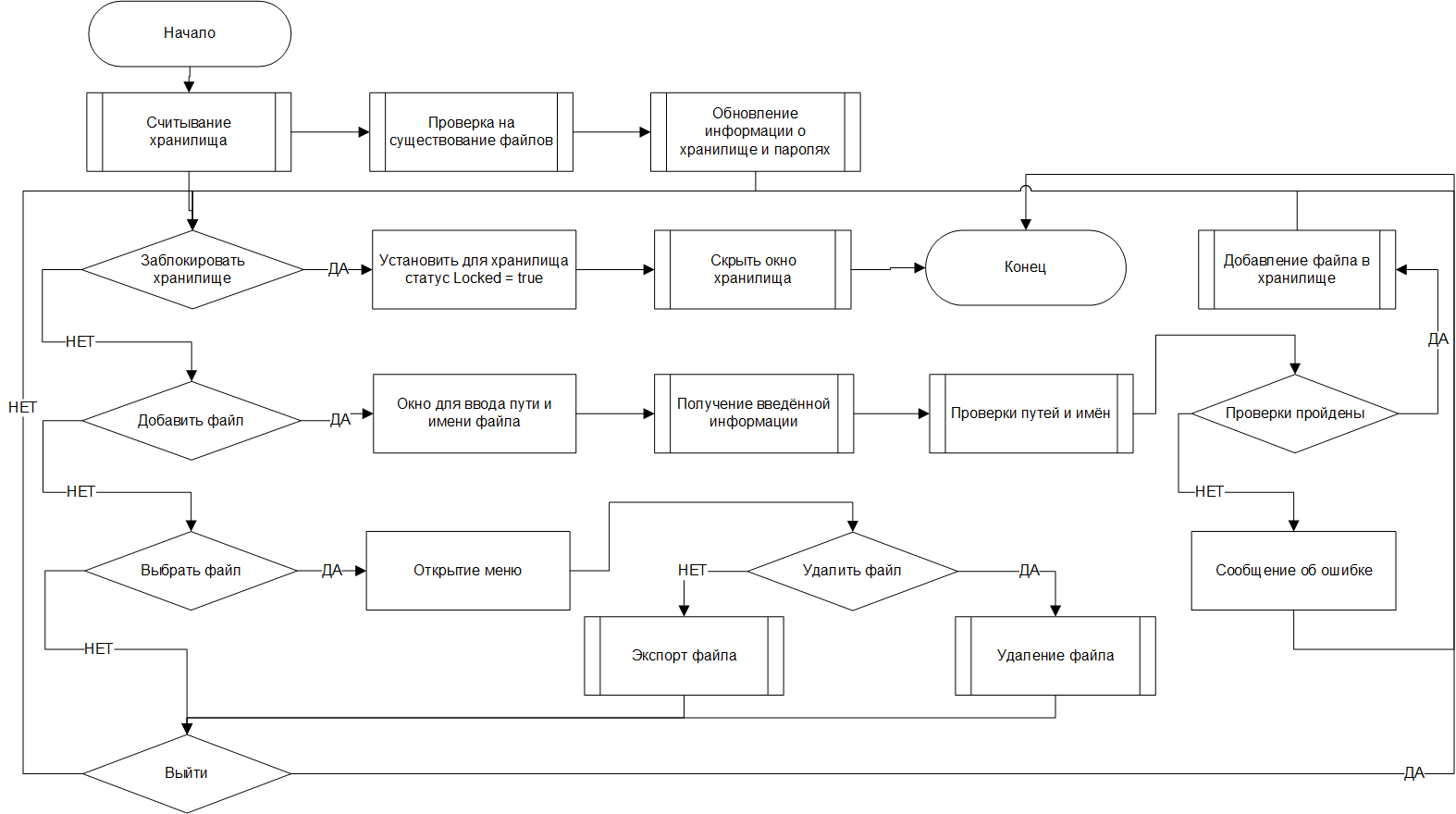


Рисунок 3.9 − Управление хранилищем

Все файлы хранилищ имеют особые настройки доступа, которые не позволяют изменять файлы, чтобы не нарушить их целостность и, как следствие, не потерять данные при расшифровке.

Однако у пользователя должна быть возможность удалить хранилище или файл. В таком случае, необходимо обеспечить корректную обработку этого удаления. Для этого каждый раз при загрузке приложения происходит анализ файла со списком хранилищ, проверка существования этих хранилищ и изменение информации о хранилищах и их паролях.

# **4 РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА**

## **4.1 Шифрование**

Основная часть работы с шифрованными файлами, включающая открытие, создание файлов, шифрование и установку атрибутов безопасности, реализована в классе Encoder. Для этого используются библиотеки для работы с файловым вводом и выводом <fstream>, <filesystem>, <vector> для хранения информации, <bitset> для работы с битам, <Windows.h> для настройки прав доступа и <locale> для настройки локали. Следующий код отражает процедуру шифрования и расшифровки:

bool Encoder::EncryptDecryptFile(const std::wstring& input, const std::wstring& output) {

std::ifstream file\_in(input, std::ios::binary);

std::ofstream file\_out(output, std::ios::binary);

if (!file\_in.is\_open()) {

return false;

}

if (!file\_out.is\_open()) {

return false;

}

std::vector<uint8\_t> buffer(BlockSize);

while (file\_in.read(reinterpret\_cast<char\*>(buffer.data()), buffer.size()) || file\_in.gcount() > 0) {

int bytesRead = file\_in.gcount();

int j = 0;

for (int i = 0; i < bytesRead; i++) {

shift();

buffer[i] ^= Key;

}

file\_out.write(reinterpret\_cast<char\*>(buffer.data()), bytesRead);

}

DWORD attributes = GetFileAttributes(output.c\_str());

if (attributes != INVALID\_FILE\_ATTRIBUTES) {

SetFileAttributes(output.c\_str(), attributes | FILE\_ATTRIBUTE\_READONLY);

}

file\_in.close();

file\_out.close();

return true;

}

## **4.2 Добавление нового хранилища**

Для добавления нового хранилища необходимо сначала получить всю информацию, введённую пользователем, проверить её на корректность, проверить существование пути и обновить информацию о хранилищах в файлах и в самом приложении. Для этого также используются библиотеки для работы с файловым вводом и выводом <fstream>, <filesystem>, <vector> для хранения информации, <dpapi.h> для работы с DPAPI. Следующий код реализует механизм добавления нового хранилища:

void AddNewStorage() {

//RECT clearRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

int x = GetWindowTextLength(newDirInput);

if (x == 0) {

MessageBox(mainWnd, L"Enter path", L"failed", MB\_OK);

return;

}

std::wstring directory(x, L'\0');

GetWindowText(newDirInput, &directory[0], x + 1);

x = GetWindowTextLength(newNameInput);

if (x == 0) {

MessageBox(mainWnd, L"Enter name", L"failed", MB\_OK);

return;

}

if (x > 256 - directory.size()) {

MessageBox(mainWnd, L"Name is too long", L"failed", MB\_OK);

return;

}

std::wstring name(x, L'\0');

GetWindowText(newNameInput, &name[0], x + 1);

if (СontainsInvalidChars(name)) {

MessageBox(mainWnd, L"Name contains invalid chars", L"failed", MB\_OK);

return;

}

for (int i = 0;i < storages.size();i++)

{

if (storages[i].name == name)

{

MessageBox(mainWnd, L"Storage with this name already exists", L"failed", MB\_OK);

return;

}

}

x = GetWindowTextLength(newPassInput);

if (x > 32) {

MessageBox(mainWnd, L"Password is too long", L"failed", MB\_OK);

return;

}

if (x < 8) {

MessageBox(mainWnd, L"Password is too short", L"failed", MB\_OK);

return;

}

if (x == 0) {

MessageBox(mainWnd, L"Enter Password", L"failed", MB\_OK);

return;

}

std::wstring password(x, L'\0');

GetWindowText(newPassInput, &password[0], x + 1);

x = GetWindowTextLength(newPassRepInput);

if (x <= 0 || x > 22) {

MessageBox(mainWnd, L"Mismatch", L"failed", MB\_OK);

return;

}

std::wstring passwordRep(x, L'\0');

GetWindowText(newPassRepInput, &passwordRep[0], x + 1);

if (password.compare(passwordRep) != 0) {

MessageBox(mainWnd, L"Mismatch", L"failed", MB\_OK);

return;

}

std::wstring fullPath = directory + L"\\" + name;

if (!CreateDirectory(fullPath.c\_str(), NULL) && GetLastError() != ERROR\_ALREADY\_EXISTS) {

MessageBox(mainWnd, L"Failed to create directory", L"failed", MB\_OK);

return;

}

SaveToFile(L"CPKeys.bin", ProtectData(reinterpret\_cast<const BYTE\*>(password.c\_str()), password.size() \* sizeof(wchar\_t)));

std::wofstream outFile("CPStorages.txt", std::ios::app);

if (!outFile.is\_open()) {

MessageBox(mainWnd, L"Failed to open CPStorages.txt for writing", L"failed", MB\_OK);

return;

}

outFile.imbue(std::locale(".utf-8"));

outFile << fullPath << std::endl;

outFile.close();

storages.clear();

ReadEntriesFromFile(L"D:\\БГУИР\\Курсовые\\CryptoPanda\\CryptoPanda\\CPStorages.txt");

}

## **4.3 Добавление файла в хранилище**

Добавление файла в хранилище так же подразумевает проверки пользовательского ввода, действительность путей, непосредственно добавление файла в хранилище и обновление информации о списке файлов в хранилище. Следующая функция реализует добавление нового файла в хранилище:

void AddNewFileInStorage()

{

int x = GetWindowTextLength(newFilePathEdit);

if (x == 0)

{

MessageBox(mainWnd, L"Enter path", L"failed", MB\_OK);

return;

}

std::wstring direcory(x, L'\0');

GetWindowText(newFilePathEdit, &direcory[0], x + 1);

x = GetWindowTextLength(newFileNameEdit);

if (x == 0)

{

MessageBox(mainWnd, L"Enter name", L"failed", MB\_OK);

return;

}

std::wstring name(x, L'\0');

GetWindowText(newFileNameEdit, &name[0], x + 1);

for (int i = 0;i < filesInStorage.size();i++) {

if (filesInStorage[i].name == name) {

MessageBox(viewStorageWnd, L"This file name is already in storage.Choose another one", L"Failed", MB\_OK);

return;

}

}

std::wstring key = GetPassword();

encoder->SetKey(key);

std::wstring encodedName = L" ";

encodedName = encoder->EncryptLine(name);

encoder->SetKey(key);

std::wstring newFilePath = storages[storageID].path + L"\\" + encodedName + L".txt";

if (std::filesystem::exists(direcory) && encoder->EncryptDecryptFile(direcory, newFilePath))

{

AddItemInFileTable(name);

filesInStorage.push\_back({name, encodedName});

}

else MessageBox(viewStorageWnd, L"FilePath doesn't exist", L"Faild", MB\_OK);

}

## **4.4 Отображение файлов в хранилище**

При открытии хранилища не в приложении, пользователь увидит зашифрованные файлы с зашифрованными именами. Для обнаружения какого-либо зашифрованного файла, его настоящее имя нужно найти в хранилище, открытом в приложении. Для отображения списка файла в понятном для пользователя виде, необходимо получить ключ пользователя и расшифровать им имена всех файлов хранилища. Следующая функция реализует описанный алгоритм:

void GetFilesInStorage() {

std::wstring key = GetPassword();

std::wstring dirPath = storages[storageID].path;

try {

for (const std::filesystem::directory\_entry& entry : std::filesystem::recursive\_directory\_iterator(dirPath)) {

if (std::filesystem::is\_regular\_file(entry.status())) {

FileNames filename;

std::filesystem::path filePath = entry.path(); // Получаем путь к файлу

std::wstring filenameWithoutExtension = filePath.stem().wstring();

encoder->SetKey(key);

filename.encodedName = filenameWithoutExtension;

std::wstring name = encoder->EncryptLine(filenameWithoutExtension);

filename.name = name;

filesInStorage.push\_back(filename);

}

}

}

catch (const std::filesystem::filesystem\_error& e) {

MessageBox(viewStorageWnd, L"Can not reade storage", L"Failed", NULL);

}

}

## **4.5 Вспомогательные функции**

Таблица 4.1 − Вспомогательные функции

|  |  |  |
| --- | --- | --- |
| Модуль | Прототип функции | Назначение |
| Encoder.cpp | void Encoder::shift() | Формирует байт ключевой последовательности |
| Encoder.cpp | std::wstring Encoder::EncryptLine(const std::wstring& input) | Используется для шифрования и расшифровки имён файлов |
| CryproPanda.cpp | DeleteFileFromStorage(int fileId) | Удаляет выбранный файл из хранилища |
| CryproPanda.cpp | bool ExportFileFromStorage(int fileId) | Экспортирует выбранный файл из хранилища в расшифрованном виде в папку Export |
| CryproPanda.cpp | std::wstring GetPassword() | Получение ключа хранилища при помощи DPAPI |
| CryproPanda.cpp | bool ComparePassword(const std::wstring& inputPassword, const std::wstring& filename, size\_t index) | Сравнивает пароль, введённый пользователем, и пароль хранилища |
| CryproPanda.cpp | bool ComparePassword(const std::wstring& inputPassword, const std::wstring& filename, size\_t index) | Обновляет информацию о паролях, если хранилище было удалено |

# **5. ТЕСТИРОВАНИЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ ПРОГРАММНОГО СРЕДСТВА**

Для обеспечения надежности и безопасности разработанного приложения были проведены различные тесты, направленные на проверку корректности его работы и устойчивости к ошибкам. В следующей таблице представлены результаты тестирования ключевых функций приложения.

Таблица включает в себя следующие параметры: название теста, описание, ожидаемый результат и фактический результат.

Таблица 5.1 − Результаты тестирования

|  |  |  |  |
| --- | --- | --- | --- |
| Название функции | Действия пользователя | Ожидаемое поведение системы | Результат |
| Ввод верного пароля хранилища | Ввод пользователем верной последовательности в поле для ввода и нажатие на кнопку OK | Разблокировка хранилища. Отображение содержимого хранилища на экране | Пройден |
| Ввод неверного пароля хранилища | Ввод пользователем неверной последовательности в поле для ввода и нажатие на кнопку OK | Сообщение о неверном пароле | Пройден |
| Открытие окна добаввления нового хранилища | Нажатие пользователем кнопки «New Storage» | Обновление рабочей области. Отображение полей для ввода информации о новом хранилище | Пройден |
| Добавление нового хранилища. Корректные данные | Ввод пользователем корректной информации о создаваемом хранилище. Нажатие на кнопку «Add Storage» | Создание нового хранилища. Обновление списка хранилищ. Сохранение информации о новом хранилище | Пройден |

Таблица 5.1 − Продолжение

|  |  |  |  |
| --- | --- | --- | --- |
| Добавление нового хранилища. Несуществующий путь | Ввод пользователем пути к несуществующей папке | Сообщение об ошибке создания нового хранилища | Пройден |
| Добавление нового хранилища. Повторное создание | Ввод пользователем такой же информации, как для уже сущетсвующего хранилища | Сообщение об ошибке создания нового хранилища | Пройден |
| Добавление нового хранилища. Не совпадают пароли | Ввод пользователем отличающихся паролей в поле создание пароля и его подтверждения | Сообщение о несовпадении паролей | Пройден |
| Добавление нового хранилища. Закрытие окна | Выход из окна создания хранилища без создания при помощи кнопки «Back» | Открытие рабочей области главного окна | Пройден |
| Блокировка хранилища | Нажатие пользователем кнопки Lock | Блокировка хранилища. Открытие рабочей области главного окна | Пройден |
| Добавление файла в хранилище. Корректные данные | Ввод пользователем существующего пути и неповторяющегося имени | Добавление нового файла. Обновление списка файлов | Пройден |
| Добавление файла в хранилище. Несуществующий путь | Ввод пользователем несуществующего пути к файлу | Сообщение об ошибке добавления нового файла | Пройден |
| Добавление файла в хранилище. Повтор имени | Ввод пользователем имени для файла, которое уже есть в хранилище | Сообщение об ошибке добавления нового файла | Пройден |

Таблица 5.1 − Продолжение

|  |  |  |  |
| --- | --- | --- | --- |
| Удаление файла из хранилища | Выбор файла. Выбор в контекстном меню опции «Delete» | Удаление файла из хранилища. Обновление списка файлов хранилища | Пройден |
| Экспорт файла из хранилища | Выбор файла. Выбор в контекстном меню опции «Export» | Экспорт файла из хранилища в папку Export | Пройден |
| Изменение файла | Попытка пользователем изменить содержимое файла из проводника | Создание копии файла, сохранение прежней версии | Пройден |
| Удаление хранилища | Удаление пользователем хранилища из проводника | Обновление списка хранилищ и паролей | Пройден |

# **6 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

## **6.1 Интерфейс программного средства**

**6.1.1** Главное окно

Главное окно программы отображает только список уже созданных хранилищ, каждый элемент которого состоит из имени хранилища и пути к хранилищу, и кнопку для создания нового хранилища. При добавлении большого числа хранилищ у окна появится скроллбар. Вид главного окна представлен на рисунке 6.1.

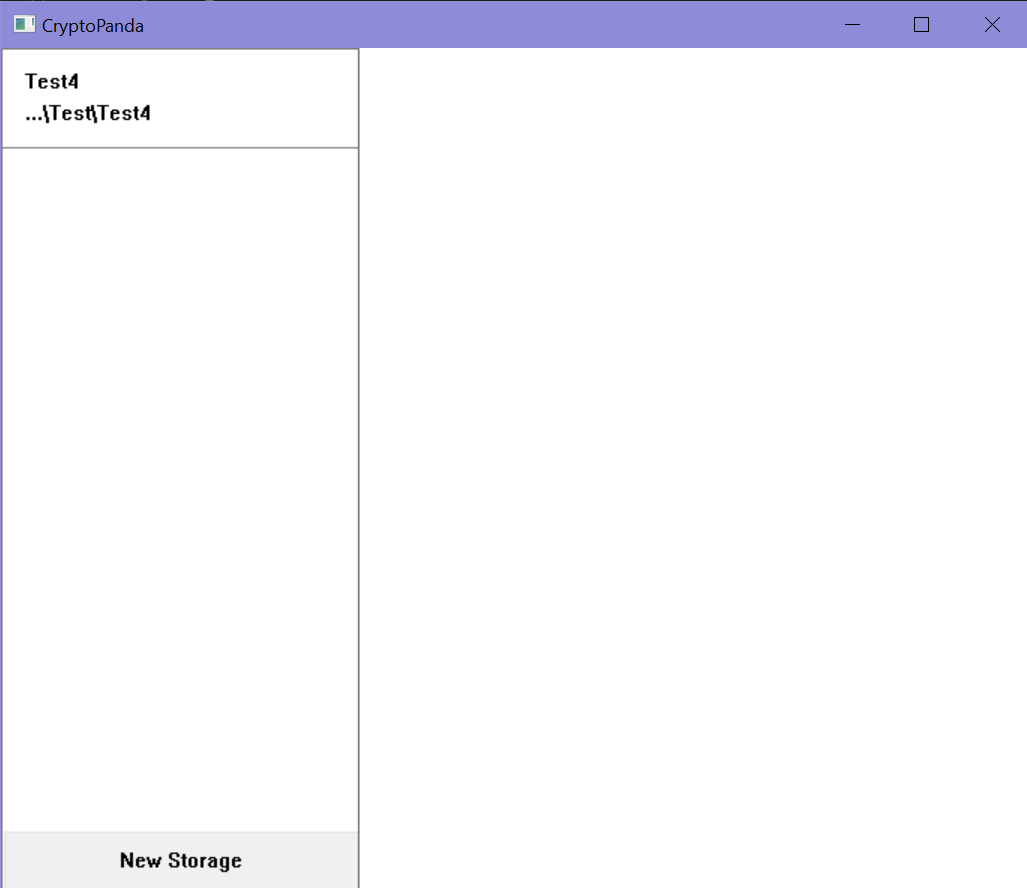


Рисунок 6.1 − Главное окно

Для добавления нового хранилища необходимо нажать на кнопку «New Storage», после чего откроется окно с полями для ввода.

**6.1.2** Окно создания нового хранилища

Для создания нового хранилища необходимо ввести следующие данные:

1 Путь к папке, в которой необходимо создать хранилище;

2 Имя хранилища;

3 Пароль, который будет использоваться для шифрования файлов. Пароль должен быть от 8 до 32 символов и не содержать запрещённых символов;

4 Повторить пароль, введённый в поле выше.

Пример заполнения данных представлен на рисунке 6.2.

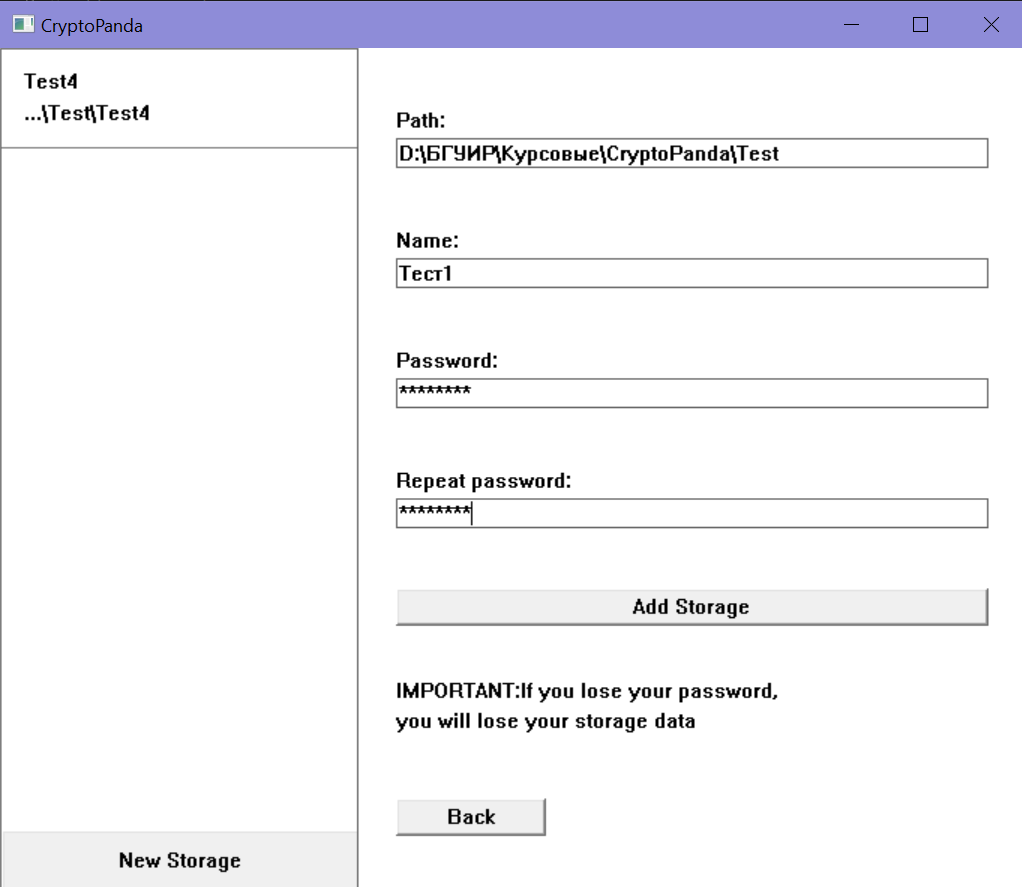


Рисунок 6.2 − Пример заполнения данных

Если данные введены верно, то после нажатия на кнопку «New Storage» в списке доступных хранилищ появится только что созданное (рис. 6.3). При нажатии на кнопку «Back» хранилище создано не будет.

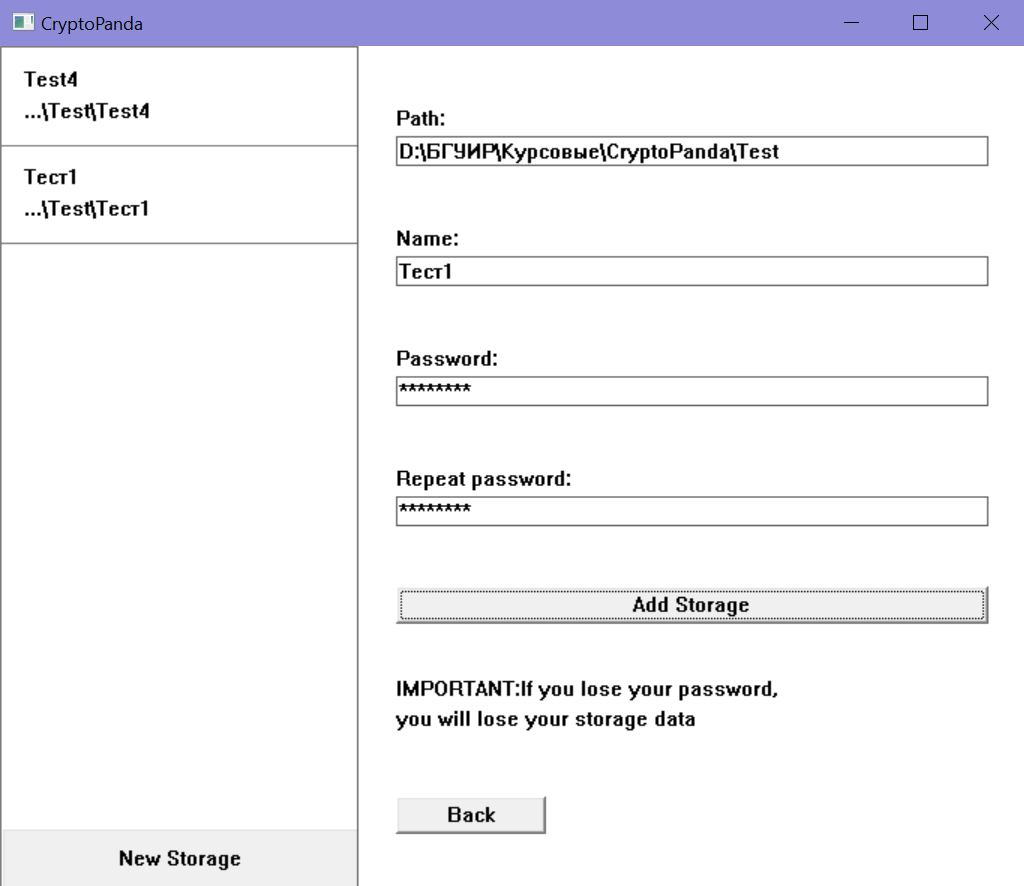


Рисунок 6.3 − Успешное создание хранилища

**6.1.3** Открытие хранилища

Для открытия хранилища необходимо выбрать одно из доступных и нажать на него. Появится окно для ввода пароля. Если пароль введён верно, то откроется окно управления хранилищем. Если пароль неверный, появится сообщение об ошибке. Пример ввода отображён на рисунке 6.4.

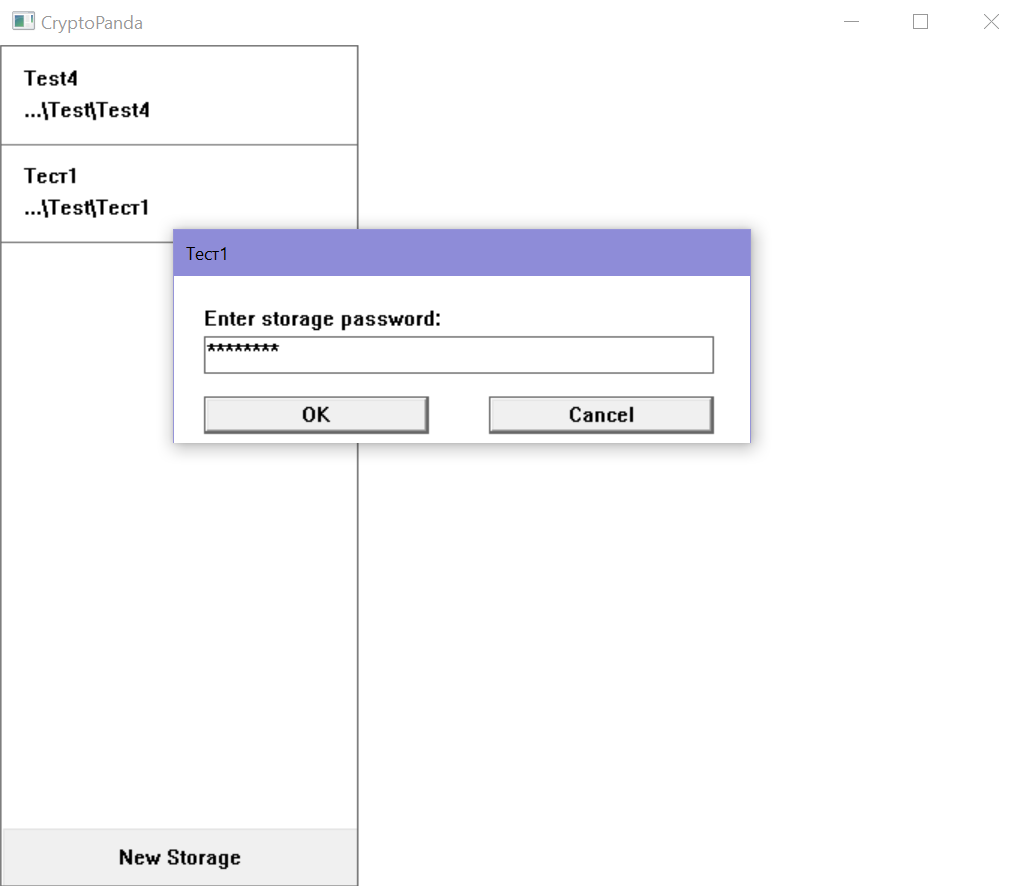


Рисунок 6.4 − Пример ввода пароля

## **6.2 Управление хранилищем**

При открытии хранилища появится окно, в котором пользователь сможет совершить следующие действия:

1 Заблокировать хранилище, нажав на кнопку «Lock»;

2 Добавить файл в хранилище, нажав на кнопку «Add File»;

3 Экспортировать файл в исходном виде;

4 Удалить файл.

**6.2.2** Добавление файла

Для добавления файла в хранилище необходимо ввести путь к исходному файлу и имя, под которым файл нужно сохранить, в окно, которое появится после нажатия на кнопку «Add File». Пример заполнения представлен на рисунке 6.5.

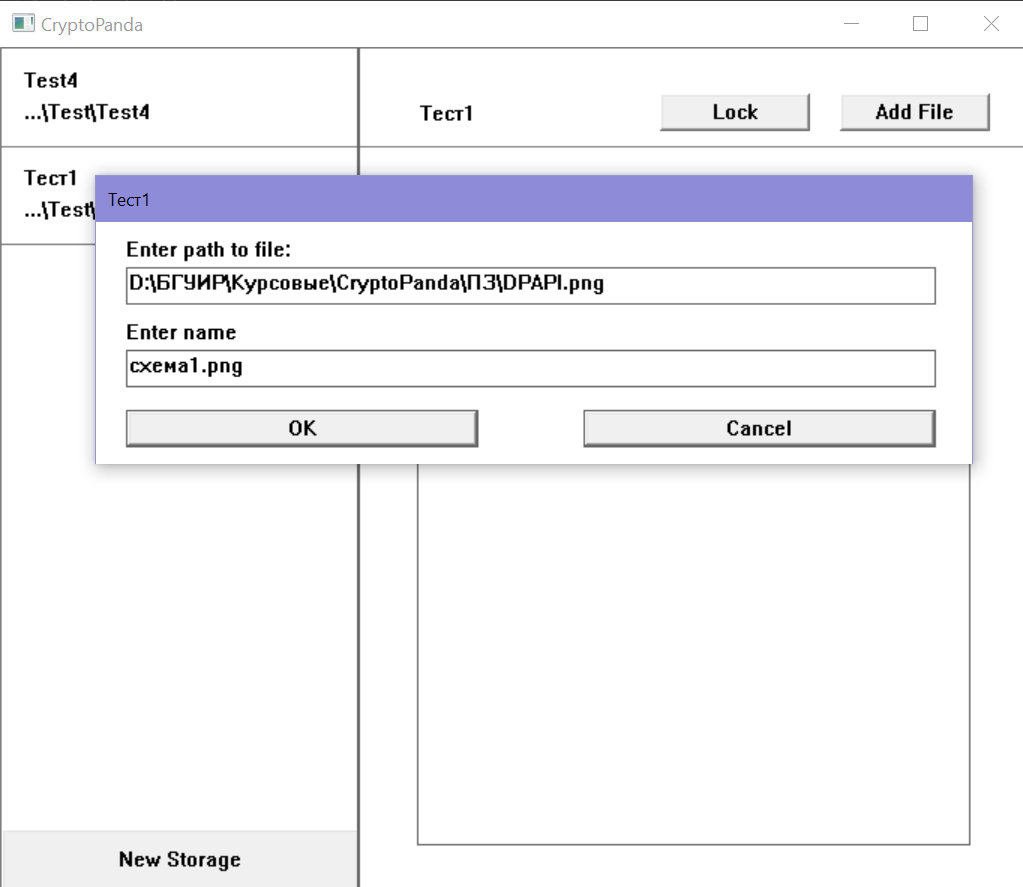


Рисунок 6.5 − Пример заполнения полей для добавления файла

При удачном добавлении имя файла появится в списке, а в хранилище появится файл с зашифрованной информацией. Результат добавления файла представлен на рисунке 6.6.

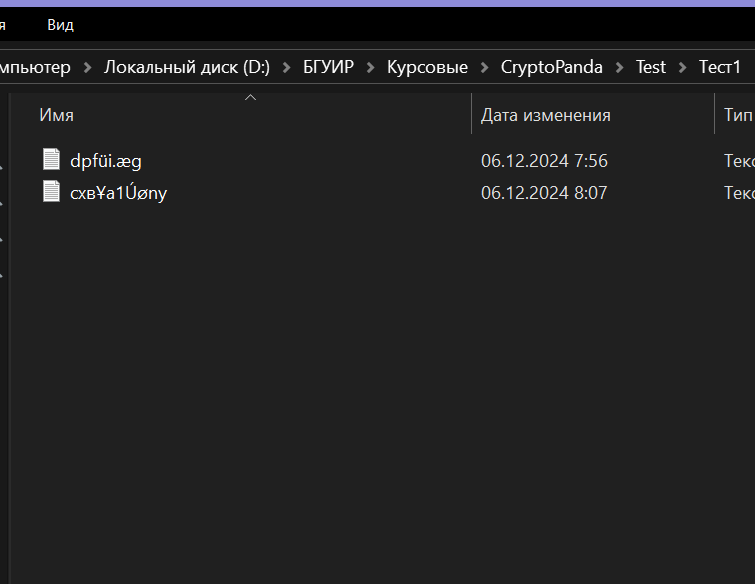
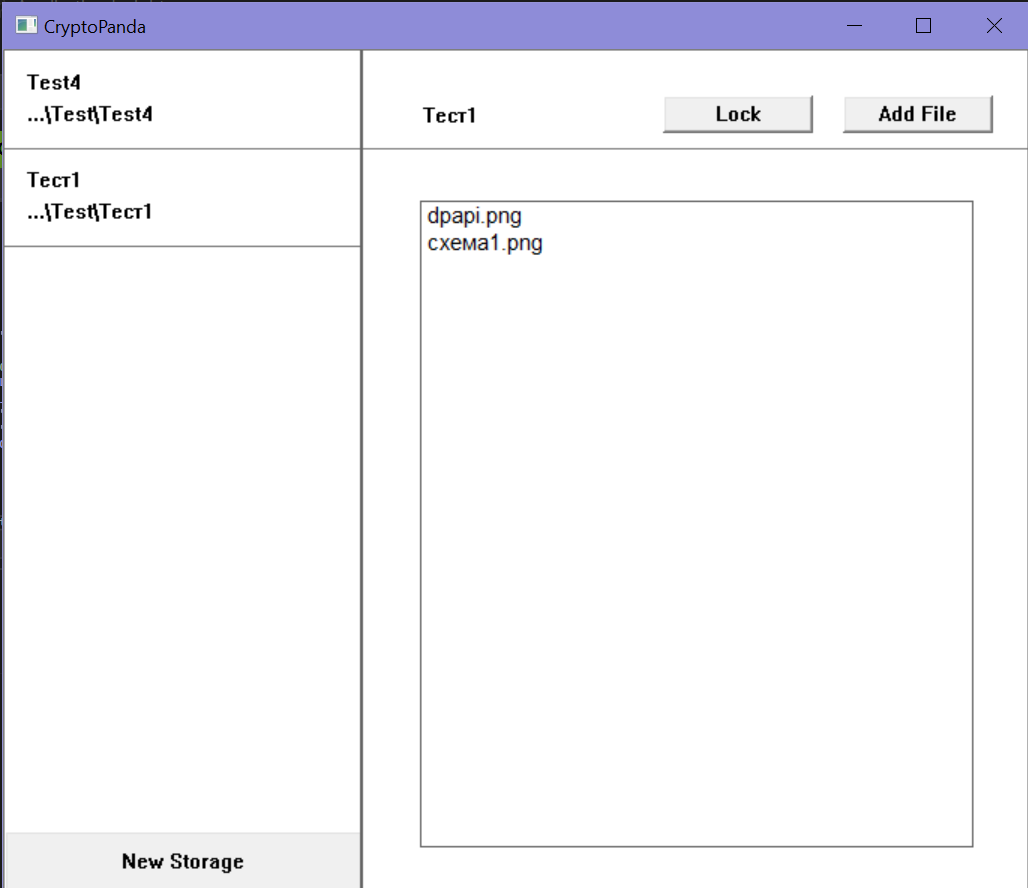


Рисунок 6.6 − Результат добавления файла в хранилище

**6.2.3** Управление файлами

Приложение предоставляет ещё 2 функции для работы с файлами: экспорт и удаление. Обе эти функции активируются при выборе их в контекстном меню выбранного файла. При выборе экспорта файл появится в расшифрованном виде в папке Export. Пример выполнения на рисунке 6.7. При удалении изменится содержимое хранилища, а так же списка файлов хранилища в приложении. Пример выполнения удаления на рисунке 6.8

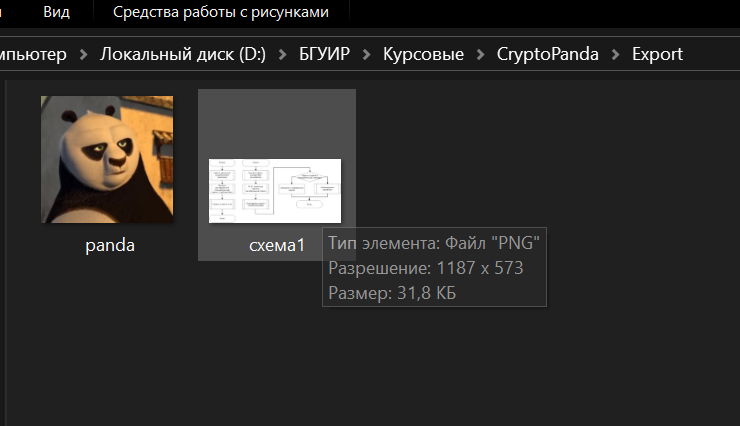
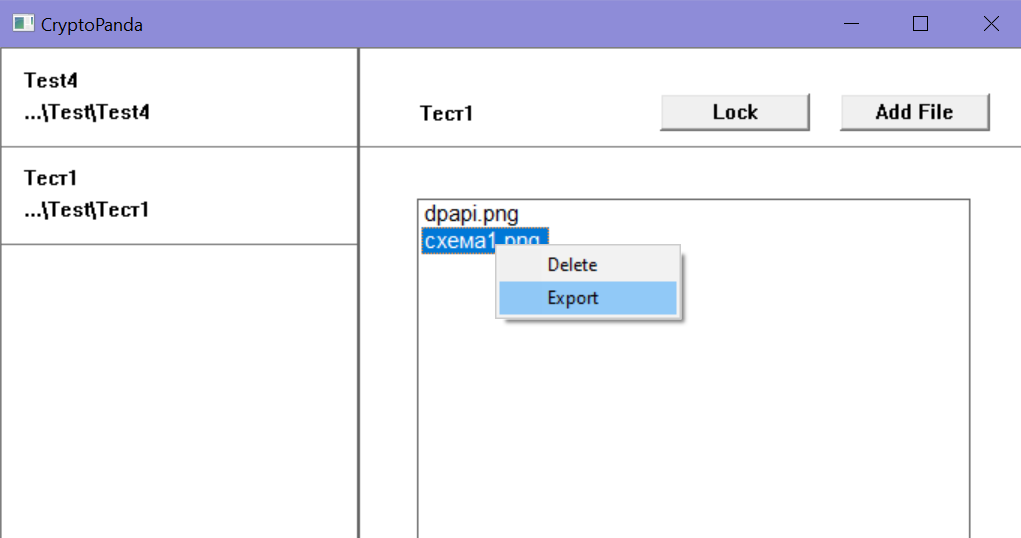


Рисунок 6.7 − Пример выполнения экспорта файла

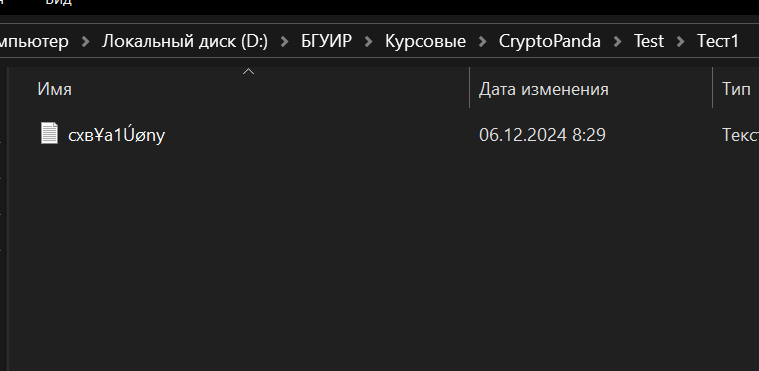
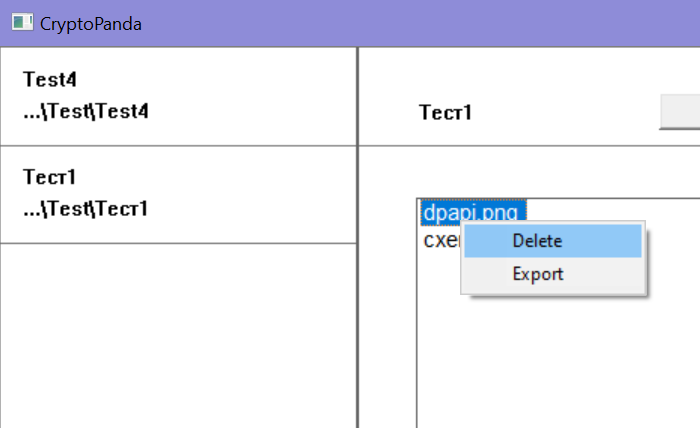


Рисунок 6.8 − Пример выполнения удаления файла

# **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсового проекта была разработана система для создания зашифрованных хранилищ, использующая методы потокового шифрования на основе алгоритма LFSR и операцию XOR. Разработка приложения включала в себя анализ требований, проектирование архитектуры, реализацию функционала и тестирование.

Использование Data Protection API (DPAPI) для шифрования ключей обеспечило высокий уровень безопасности и защиту конфиденциальных данных. В результате были достигнуты поставленные цели: приложение позволяет эффективно шифровать и расшифровывать данные, управлять ключами и обеспечивать безопасное хранение информации.

Проведенные тесты подтвердили работоспособность и надежность системы. В дальнейшем возможно расширение функционала приложения, включая поддержку различных алгоритмов шифрования и улучшение пользовательского интерфейса.

Таким образом, результаты работы демонстрируют успешное применение теоретических знаний на практике и возможность создания безопасных приложений для защиты данных.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

**1. Рихтер Д.** Программирование приложений для Windows. Разработка приложений для платформы Win32 API и .NET Framework. – М.: Диалектика, 2003. – 1248 с. – ISBN 5-8459-0685-1.

2. Поточные шифры [электр.рес]. Ссылка: [Поточные шифры](https://logic.pdmi.ras.ru/~sergey/teaching/aucryp11/03-streamciphers.pdf)

3. Шнайер Б. "Applied Cryptography". – 2nd ed. – Wiley, 1996.

4. **Шилдт Г.** C++: справочник. – М.: Вильямс, 2004. – 800 с. – ISBN 5-8459-0246-5.

5. **Евгеньев С.А.** Windows API: Теория и практика программирования. – СПб.: Питер, 2005. – 576 с. – ISBN 5-469-00142-9.

6. CNG DPAPI [электр.рес]. Ссылка: [CNG DPAPI - Win32 apps | Microsoft Learn](https://learn.microsoft.com/en-us/windows/win32/seccng/cng-dpapi)

# **Приложение А**

**Исходный код программы**

**CryproPanda.cpp**

#include <windows.h>

#include <iostream>

#include <fstream>

#include <sstream>

#include <vector>

#include <string>

#include <cctype>

#include <dpapi.h>

#include "Encoder.h"

#include <filesystem>

#include <sstream>

#include <commctrl.h>

#define NEW\_STORAGE 1

#define ADD\_STORAGE 2

#define BACK 3

#define ADD\_STORAGE\_PATH 4

#define ADD\_STORAGE\_NAME 5

#define ADD\_STORAGE\_PASS 6

#define ADD\_STORAGE\_REP 7

#define PASS\_CHECK 8

#define PASS\_CANCEL 9

#define LOCK\_STORAGE 10

#define ADD\_IN\_STORAGE 11

#define ADD\_FILE\_OK 12

#define ADD\_FILE\_CANCEL 13

#pragma comment (lib, "Crypt32")

int clientWidth = 0, clientHeight = 0, stListWndWidth, stListWndHeight, listScrollId = 0, listItmHeight = 65, scrollPos = 0, leftStorages = 0, stItmsToShow = 0,

controllHeight = 20, storageID = 0, fileID = 0;

RECT clientRect;

HWND mainWnd, stListWnd, addStorageWnd, newDirInput, newNameInput, newPassInput, newPassRepInput, dialogWnd, passCheckEdit, viewStorageWnd, addFileInStorageWnd,

newFilePathEdit, newFileNameEdit, fileInStorageListWnd;

HMENU fileInStorageFunc;

HINSTANCE hInst;

Encoder \*encoder = nullptr;

struct StorageInfo {

std::wstring path;

std::wstring name;

std::wstring folders;

bool locked;

};

struct FileNames {

std::wstring name;

std::wstring encodedName;

};

std::vector<StorageInfo> storages;

std::vector<FileNames> filesInStorage;

void DeleteFilesFromFileTable();

std::wstring GetPassword();

void GetFilesInStorage();

void UpdateScroll();

void UpdateClientSize();

void ReadEntriesFromFile(const std::wstring& filename);

void DrawList(HWND hwnd, HDC hdc);

void CreateChildWnd();

void NewStorageText(HDC hdc);

void AddNewStorage();

bool СontainsInvalidChars(const std::wstring& input);

bool CreateFolder(const std::wstring& path, const std::wstring& folderName);

std::vector<BYTE> LoadPasswordByIndex(const std::wstring& filename, size\_t index);

std::vector<BYTE> UnprotectData(const BYTE\* data, DWORD dataSize);

void SaveToFile(const std::wstring& filename, const std::vector<BYTE>& data);

std::vector<BYTE> ProtectData(const BYTE\* data, DWORD dataSize);

void SetDialogWnd();

bool CheckPassword();

bool ComparePassword(const std::wstring& inputPassword, const std::wstring& filename, size\_t index);

void ViewStorage(HDC hdc);

void SetAddFileWnd();

void AddNewFileInStorage();

void AddFilesInFileList();

void AddItemInFileTable(std::wstring newFile);

int GetFileItemClickPos(int x, int y);

bool DeleteFileFromStorage(int fileId);

bool ExportFileFromStorage(int fileId);

void StorageDntExist(int id);

LRESULT CALLBACK WindowProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

RECT clearRect = { 0,0,clientWidth, clientHeight};

HDC hdc;

PAINTSTRUCT ps;

switch (uMsg) {

case WM\_CREATE:

break;

case WM\_DESTROY:

PostQuitMessage(0);

break;

case WM\_SIZE:

UpdateClientSize();

InvalidateRect(hwnd, NULL, TRUE);

UpdateWindow(hwnd);

break;

case WM\_GETMINMAXINFO: {

MINMAXINFO\* mmi = (MINMAXINFO\*)lParam;

mmi->ptMinTrackSize.x = 700;

mmi->ptMinTrackSize.y = 600;

mmi->ptMaxTrackSize.x = 700;

mmi->ptMaxTrackSize.y = 600;

return 0;

}

case WM\_PAINT:

hdc = BeginPaint(hwnd, &ps);

FillRect(hdc, &clearRect, (HBRUSH)(COLOR\_WINDOW + 1));

EndPaint(hwnd, &ps);

break;

default:

return DefWindowProc(hwnd, uMsg, wParam, lParam);

}

return 0;

}

LRESULT CALLBACK stListWndProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

RECT clearRect = {0,0, stListWndWidth, stListWndHeight};

RECT mainRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

HDC hdc;

PAINTSTRUCT ps;

switch (uMsg) {

case WM\_CREATE:

break;

case WM\_DESTROY:

PostQuitMessage(0);

break;

case WM\_SIZE:

break;

case WM\_COMMAND:

if (LOWORD(wParam) == NEW\_STORAGE)

{

ShowWindow(viewStorageWnd, SW\_HIDE);

ShowWindow(addStorageWnd, SW\_SHOW);

InvalidateRect(mainWnd, &mainRect, TRUE);

UpdateWindow(mainWnd);

UpdateWindow(addStorageWnd);

}

break;

case WM\_PAINT:

hdc = BeginPaint(hwnd, &ps);

FillRect(hdc, &clearRect, (HBRUSH)(COLOR\_WINDOW + 1));

DrawList(hwnd, hdc);

EndPaint(hwnd, &ps);

break;

case WM\_LBUTTONDOWN: {

int x = LOWORD(lParam);

int y = HIWORD(lParam);

int clickedIndex = y / listItmHeight;

if (clickedIndex >= 0 && clickedIndex < storages.size()) {

storageID = clickedIndex;

if (storages[clickedIndex].locked) {

SetDialogWnd();

}

else

{

ShowWindow(viewStorageWnd, SW\_SHOW);

ShowWindow(addStorageWnd, SW\_HIDE);

InvalidateRect(mainWnd, &mainRect, TRUE);

UpdateWindow(mainWnd);

}

}

break;

}

case WM\_VSCROLL: {

int oldPos = scrollPos;

switch (LOWORD(wParam)) {

case SB\_LINEUP:

if (--scrollPos < 0) scrollPos = 0;

break;

case SB\_LINEDOWN:

if (++scrollPos > leftStorages) scrollPos = leftStorages;

else leftStorages--;

break;

}

if (oldPos != scrollPos)

{

SetScrollPos(stListWnd, SB\_VERT, scrollPos, true);

InvalidateRect(stListWnd, NULL, true);

}

break;

}

default:

return DefWindowProc(hwnd, uMsg, wParam, lParam);

}

return 0;

}

LRESULT CALLBACK dialogWndProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

RECT clearRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

HDC hdc;

PAINTSTRUCT ps;

switch (uMsg) {

case WM\_CREATE:

break;

case WM\_DESTROY:

PostQuitMessage(0);

break;

case WM\_SIZE:

break;

case WM\_PAINT:

hdc = BeginPaint(hwnd, &ps);

FillRect(hdc, &clearRect, (HBRUSH)(COLOR\_WINDOW + 1));

TextOut(hdc, 20, 20, L"Enter storage password:", 23);

EndPaint(hwnd, &ps);

break;

case WM\_COMMAND:

if (LOWORD(wParam) == PASS\_CANCEL) {

SetWindowText(passCheckEdit, L"");

CloseWindow(dialogWnd);

}

else if (LOWORD(wParam) == PASS\_CHECK) {

if (CheckPassword())

{

storages[storageID].locked = false;

filesInStorage.clear();

DeleteFilesFromFileTable();

ShowWindow(viewStorageWnd, SW\_SHOW);

ShowWindow(addStorageWnd, SW\_HIDE);

InvalidateRect(mainWnd, &clearRect, TRUE);

UpdateWindow(mainWnd);

SetWindowText(passCheckEdit, L"");

CloseWindow(dialogWnd);

GetFilesInStorage();

AddFilesInFileList();

}

}

break;

case WM\_CLOSE:

DestroyWindow(hwnd);

return 0;

break;

default:

return DefWindowProc(hwnd, uMsg, wParam, lParam);

}

return 0;

}

LRESULT CALLBACK addFileWndProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

RECT clearRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

HDC hdc;

PAINTSTRUCT ps;

switch (uMsg) {

case WM\_CREATE:

break;

case WM\_DESTROY:

PostQuitMessage(0);

break;

case WM\_SIZE:

break;

case WM\_PAINT:

hdc = BeginPaint(hwnd, &ps);

FillRect(hdc, &clearRect, (HBRUSH)(COLOR\_WINDOW + 1));

TextOut(hdc, 20, 10, L"Enter path to file:", 19);

TextOut(hdc, 20, 65, L"Enter name:", 10);

EndPaint(hwnd, &ps);

break;

case WM\_COMMAND:

if (LOWORD(wParam) == ADD\_FILE\_CANCEL) {

CloseWindow(hwnd);

}

if (LOWORD(wParam) == ADD\_FILE\_OK) {

CloseWindow(hwnd);

AddNewFileInStorage();

InvalidateRect(fileInStorageListWnd, NULL, true);

}

break;

case WM\_CLOSE:

DestroyWindow(hwnd);

return 0;

break;

default:

return DefWindowProc(hwnd, uMsg, wParam, lParam);

}

return 0;

}

LRESULT CALLBACK addStorageWndProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

RECT clearRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

RECT listRect = {0, 0, stListWndWidth, stListWndHeight};

HDC hdc;

PAINTSTRUCT ps;

switch (uMsg) {

case WM\_CREATE:

break;

case WM\_DESTROY:

PostQuitMessage(0);

break;

case WM\_SIZE:

break;

case WM\_PAINT:

hdc = BeginPaint(hwnd, &ps);

FillRect(hdc, &clearRect, (HBRUSH)(COLOR\_WINDOW + 1));

NewStorageText(hdc);

EndPaint(hwnd, &ps);

break;

case WM\_COMMAND:

if (LOWORD(wParam) == BACK)

{

SetWindowText(newDirInput, L"");

SetWindowText(newNameInput, L"");

SetWindowText(newPassInput, L"");

SetWindowText(newPassRepInput, L"");

ShowWindow(hwnd, SW\_HIDE);

InvalidateRect(mainWnd, &clearRect, TRUE);

UpdateWindow(mainWnd);

}

else if (LOWORD(wParam) == ADD\_STORAGE)

{

AddNewStorage();

UpdateScroll();

InvalidateRect(stListWnd, &listRect, TRUE);

UpdateWindow(stListWnd);

}

break;

default:

return DefWindowProc(hwnd, uMsg, wParam, lParam);

}

return 0;

}

LRESULT CALLBACK viewStorageProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

int clickPosX, clickPosY, commandId, itemIndex;

RECT clearRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

HDC hdc;

PAINTSTRUCT ps;

switch (uMsg) {

case WM\_CREATE:

break;

case WM\_DESTROY:

PostQuitMessage(0);

break;

case WM\_SIZE:

break;

case WM\_PAINT:

hdc = BeginPaint(hwnd, &ps);

FillRect(hdc, &clearRect, (HBRUSH)(COLOR\_WINDOW + 1));

ViewStorage(hdc);

EndPaint(hwnd, &ps);

break;

case WM\_COMMAND:

if (LOWORD(wParam) == LOCK\_STORAGE)

{

storages[storageID].locked = true;

ShowWindow(hwnd, SW\_HIDE);

InvalidateRect(mainWnd, &clearRect, TRUE);

UpdateWindow(mainWnd);

}

else if (LOWORD(wParam) == ADD\_IN\_STORAGE) {

SetAddFileWnd();

}

else if (LOWORD(wParam) == 20) {

bool res = DeleteFileFromStorage(fileID);

}

else if (LOWORD(wParam) == 21) {

bool res = ExportFileFromStorage(fileID);

}

break;

case WM\_NOTIFY: {

LPNMHDR nmhdr = (LPNMHDR)lParam;

if (nmhdr->hwndFrom == fileInStorageListWnd && nmhdr->code == NM\_CLICK) {

LVHITTESTINFO hit;

POINT pt;

DWORD pos = GetMessagePos();

pt.x = LOWORD(pos);

pt.y = HIWORD(pos);

ScreenToClient(fileInStorageListWnd, &pt);

fileID = GetFileItemClickPos(pt.x, pt.y);

if (fileID != -1) {

POINT screenPt = { pt.x, pt.y };

ClientToScreen(fileInStorageListWnd, &screenPt);

TrackPopupMenu(fileInStorageFunc, TPM\_RIGHTBUTTON, screenPt.x, screenPt.y, 0, hwnd, NULL);

}

}

break;

}

default:

return DefWindowProc(hwnd, uMsg, wParam, lParam);

}

return 0;

}

int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE, LPSTR, int nShowCmd) {

const wchar\_t CLASS\_NAME[] = L"CryptoPanda";

ReadEntriesFromFile(L"D:\\БГУИР\\Курсовые\\CryptoPanda\\CryptoPanda\\CPStorages.txt");

RECT workArea;

SystemParametersInfo(SPI\_GETWORKAREA, 0, &workArea, 0);

clientWidth = workArea.right - workArea.left;

clientHeight = workArea.bottom - workArea.top;

//основное окно

WNDCLASS wc = {};

wc.lpfnWndProc = WindowProc;

wc.hInstance = hInstance;

wc.lpszClassName = CLASS\_NAME;

RegisterClass(&wc);

mainWnd = CreateWindowEx(

0, CLASS\_NAME, L"CryptoPanda",

WS\_OVERLAPPEDWINDOW | WS\_VISIBLE,

CW\_USEDEFAULT, CW\_USEDEFAULT, 700, 600,

NULL, NULL, hInstance, NULL

);

if (mainWnd == NULL) {

return 0;

}

UpdateClientSize();

encoder = new Encoder();

CreateChildWnd();

ShowWindow(stListWnd, SW\_SHOW);

ShowWindow(addStorageWnd, SW\_HIDE);

ShowWindow(viewStorageWnd, SW\_HIDE);

InvalidateRect(mainWnd, NULL, TRUE);

UpdateWindow(mainWnd);

MSG msg = {};

while (GetMessage(&msg, NULL, 0, 0)) {

TranslateMessage(&msg);

DispatchMessage(&msg);

}

return 0;

}

void CreateChildWnd() {

//список доступных хранилищ

int rows = storages.size() - 8;

if (rows < 0) rows = 0;

WNDCLASS wc = {};

wc.lpfnWndProc = stListWndProc;

wc.hInstance = hInst;

wc.lpszClassName = L"StorageList";

RegisterClass(&wc);

stListWnd = CreateWindowEx(0, L"StorageList", L"Storage List", WS\_CHILD | WS\_VISIBLE | WS\_BORDER | WS\_VSCROLL, 0, 0, stListWndWidth, stListWndHeight, mainWnd, NULL, hInst, NULL);

CreateWindow(L"Button", L"New Storage", WS\_CHILD | WS\_VISIBLE, 0, stListWndHeight - 41, stListWndWidth, 41, stListWnd, (HMENU)NEW\_STORAGE, hInst, nullptr);

UpdateScroll();

//создание хранилища

WNDCLASS wc1 = {};

wc1.lpfnWndProc = addStorageWndProc;

wc1.hInstance = hInst;

wc1.lpszClassName = L"AddStorage";

RegisterClass(&wc1);

addStorageWnd = CreateWindowEx(0, L"AddStorage", L"AddStorage", WS\_CHILD | WS\_VISIBLE /\*| WS\_BORDER\*/, stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight, mainWnd, NULL, hInst, NULL);

newDirInput = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER, 25, 60, clientWidth - stListWndWidth - 50, controllHeight, addStorageWnd, (HMENU)ADD\_STORAGE\_PATH, NULL, NULL);

newNameInput = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER, 25, 140, clientWidth - stListWndWidth - 50, controllHeight, addStorageWnd, (HMENU)ADD\_STORAGE\_NAME, NULL, NULL);

newPassInput = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER | ES\_PASSWORD, 25, 220, clientWidth - stListWndWidth - 50, controllHeight, addStorageWnd, (HMENU)ADD\_STORAGE\_PASS, NULL, NULL);

newPassRepInput = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER | ES\_PASSWORD, 25, 300, clientWidth - stListWndWidth - 50, controllHeight, addStorageWnd, (HMENU)ADD\_STORAGE\_REP, NULL, NULL);

CreateWindow(L"Button", L"Add Storage", WS\_CHILD | WS\_VISIBLE, 25, 360, clientWidth - stListWndWidth - 50, 25, addStorageWnd, (HMENU)ADD\_STORAGE, hInst, nullptr);

CreateWindow(L"Button", L"Back", WS\_CHILD | WS\_VISIBLE, 25, 500, 100, 25, addStorageWnd, (HMENU)BACK, hInst, nullptr);

//просмотр содержимого хранилища

wc = {};

wc.lpfnWndProc = viewStorageProc;

wc.hInstance = hInst;

wc.lpszClassName = L"ViewStorage";

RegisterClass(&wc);

viewStorageWnd = CreateWindowEx(0, L"ViewStorage", L"", WS\_CHILD | WS\_VISIBLE | WS\_BORDER, stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight, mainWnd, NULL, hInst, NULL);

CreateWindow(L"Button", L"Lock", WS\_CHILD | WS\_VISIBLE, 200, 30, 100, 25, viewStorageWnd, (HMENU)LOCK\_STORAGE, hInst, nullptr);

CreateWindow(L"Button", L"Add File", WS\_CHILD | WS\_VISIBLE, 320, 30, 100, 25, viewStorageWnd, (HMENU)ADD\_IN\_STORAGE, hInst, nullptr);

//список файлов хранилища

fileInStorageListWnd = CreateWindowEx(0, WC\_LISTVIEW, NULL, WS\_VISIBLE | WS\_CHILD | LVS\_REPORT | LVS\_NOCOLUMNHEADER | WS\_VSCROLL | WS\_BORDER,

38, 100, clientWidth - stListWndWidth - 38\*2, clientHeight - 100 - 30,

viewStorageWnd, NULL, hInst, NULL);

//создание таблицы для файлов

LVCOLUMN col;

col.mask = LVCF\_TEXT | LVCF\_WIDTH | LVCF\_SUBITEM;

wchar\_t columnName[] = L"Files";

col.pszText = columnName;

col.cx = clientWidth - stListWndWidth - 38\*2;

ListView\_InsertColumn(fileInStorageListWnd, 0, &col);

//меню для работы с файлами

fileInStorageFunc = CreatePopupMenu();

AppendMenu(fileInStorageFunc, MF\_STRING, 20, L"Delete");

AppendMenu(fileInStorageFunc, MF\_STRING, 21, L"Export");

HFONT hFont = CreateFont(17, 0,0,0, FW\_NORMAL,FALSE, FALSE,FALSE,DEFAULT\_CHARSET,OUT\_DEFAULT\_PRECIS,

CLIP\_DEFAULT\_PRECIS, DEFAULT\_QUALITY, DEFAULT\_QUALITY, L"Arial");

SendMessage(fileInStorageListWnd, WM\_SETFONT, (WPARAM)hFont, TRUE);

}

void UpdateClientSize() {

GetClientRect(mainWnd, &clientRect);

clientWidth = clientRect.right - clientRect.left;

clientHeight = clientRect.bottom - clientRect.top;

stListWndHeight = clientHeight;

stListWndWidth = (int)(0.35 \* clientWidth);

}

void ReadEntriesFromFile(const std::wstring& pathsFilename) {

std::wifstream pathsFile(pathsFilename);

bool folderExists;

pathsFile.imbue(std::locale("ru\_RU.UTF-8"));

if (!pathsFile.is\_open()) {

return;

}

if (pathsFile.peek() == std::wifstream::traits\_type::eof()) {

return;

}

std::wstring line;

while (std::getline(pathsFile, line)) {

if (line.empty()) {

continue;

}

std::vector<std::wstring> pathParts;

std::wistringstream pathStream(line);

std::wstring part;

while (std::getline(pathStream, part, L'\\')) {

pathParts.push\_back(part);

}

if (pathParts.size() >= 2) {

std::wstring name = pathParts.back();

std::wstring folders = L"...\\" + pathParts[pathParts.size() - 2] + L"\\" + name;

folderExists = std::filesystem::exists(line) && std::filesystem::is\_directory(line);

if (folderExists == false)

StorageDntExist(storages.size());

else

storages.push\_back({ line, name, folders, true });

}

}

pathsFile.close();

std::wofstream outFile(pathsFilename, std::ios::trunc);

if (!outFile.is\_open()) {

std::wcerr << L"Ошибка открытия файла для записи!" << std::endl;

return;

}

outFile.imbue(std::locale(".utf-8"));

for (const auto& storagePath : storages) {

outFile << storagePath.path << std::endl;

}

outFile.close();

}

void DrawList(HWND hwnd, HDC hdc) {

// отрисовка списка доступных хранилищ

SIZE textSize1, textSize2;

int spaceX = 15, spaceY = 13, fontHeight = 16;

SetTextColor(hdc, RGB(0, 0, 0));

HPEN hPen = CreatePen(PS\_SOLID, 1, RGB(128, 128, 128));

SelectObject(hdc, hPen);

HBRUSH hBrush = CreateSolidBrush(RGB(128, 128, 128));

RECT fillRect;

MoveToEx(hdc, stListWndWidth - 1, 0, nullptr);

LineTo(hdc, stListWndWidth - 1, stListWndHeight);

stItmsToShow = storages.size() - scrollPos;

if (stItmsToShow < 0) stItmsToShow = storages.size();

if (stItmsToShow > 8) stItmsToShow = 8;

for (int i = scrollPos; i < stItmsToShow + scrollPos; i++)

{

GetTextExtentPoint32(hdc, storages[i].name.c\_str(), storages[i].name.size(), &textSize1);

GetTextExtentPoint32(hdc, storages[i].folders.c\_str(), storages[i].folders.size(), &textSize2);

TextOut(hdc, spaceX, spaceY + (i- scrollPos) \*listItmHeight, storages[i].name.c\_str(), storages[i].name.size());

TextOut(hdc, spaceX, spaceY + 21 + (i - scrollPos) \* listItmHeight, storages[i].folders.c\_str(), storages[i].folders.size());

MoveToEx(hdc, 0, (i - scrollPos +1)\*listItmHeight, nullptr);

LineTo(hdc, stListWndWidth, (i - scrollPos + 1) \* listItmHeight);

}

}

void StorageDntExist(int id) {

std::vector<std::vector<BYTE>> passwords;

size\_t index = 0;

while (true) {

std::vector<BYTE> password = LoadPasswordByIndex(L"CPKeys.bin", index);

if (password.empty()) {

break;

}

passwords.push\_back(std::move(password));

index++;

}

passwords.erase(passwords.begin() + id);

std::ofstream ofs(L"CPKeys.bin", std::ios::binary | std::ios::trunc);

for (int i = 0;i < passwords.size();i++) {

SaveToFile(L"CPKeys.bin", passwords[i]);

}

ofs.close();

passwords.clear();

}

void NewStorageText(HDC hdc) {

TextOut(hdc, 25, 40, L"Path:", 5);

TextOut(hdc, 25, 120, L"Name:", 5);

TextOut(hdc, 25, 200, L"Password:", 9);

TextOut(hdc, 25, 280, L"Repeat password:", 16);

TextOut(hdc, 25, 420, L"IMPORTANT:If you lose your password,", 36);

TextOut(hdc, 25, 440, L"you will lose your storage data", 32);

}

void AddNewStorage() {

//RECT clearRect = { stListWndWidth, 0, clientWidth - stListWndWidth, stListWndHeight };

int x = GetWindowTextLength(newDirInput);

if (x == 0) {

MessageBox(mainWnd, L"Enter path", L"failed", MB\_OK);

return;

}

std::wstring directory(x, L'\0');

GetWindowText(newDirInput, &directory[0], x + 1);

x = GetWindowTextLength(newNameInput);

if (x == 0) {

MessageBox(mainWnd, L"Enter name", L"failed", MB\_OK);

return;

}

if (x > 256 - directory.size()) {

MessageBox(mainWnd, L"Name is too long", L"failed", MB\_OK);

return;

}

std::wstring name(x, L'\0');

GetWindowText(newNameInput, &name[0], x + 1);

if (СontainsInvalidChars(name)) {

MessageBox(mainWnd, L"Name contains invalid chars", L"failed", MB\_OK);

return;

}

for (int i = 0;i < storages.size();i++)

{

if (storages[i].name == name)

{

MessageBox(mainWnd, L"Storage with this name already exists", L"failed", MB\_OK);

return;

}

}

x = GetWindowTextLength(newPassInput);

if (x > 32) {

MessageBox(mainWnd, L"Password is too long", L"failed", MB\_OK);

return;

}

if (x < 8) {

MessageBox(mainWnd, L"Password is too short", L"failed", MB\_OK);

return;

}

if (x == 0) {

MessageBox(mainWnd, L"Enter Password", L"failed", MB\_OK);

return;

}

std::wstring password(x, L'\0');

GetWindowText(newPassInput, &password[0], x + 1);

x = GetWindowTextLength(newPassRepInput);

if (x <= 0 || x > 22) {

MessageBox(mainWnd, L"Mismatch", L"failed", MB\_OK);

return;

}

std::wstring passwordRep(x, L'\0');

GetWindowText(newPassRepInput, &passwordRep[0], x + 1);

if (password.compare(passwordRep) != 0) {

MessageBox(mainWnd, L"Mismatch", L"failed", MB\_OK);

return;

}

std::wstring fullPath = directory + L"\\" + name;

if (!CreateDirectory(fullPath.c\_str(), NULL) && GetLastError() != ERROR\_ALREADY\_EXISTS) {

MessageBox(mainWnd, L"Failed to create directory", L"failed", MB\_OK);

return;

}

SaveToFile(L"CPKeys.bin", ProtectData(reinterpret\_cast<const BYTE\*>(password.c\_str()), password.size() \* sizeof(wchar\_t)));

std::wofstream outFile("CPStorages.txt", std::ios::app);

if (!outFile.is\_open()) {

MessageBox(mainWnd, L"Failed to open CPStorages.txt for writing", L"failed", MB\_OK);

return;

}

outFile.imbue(std::locale(".utf-8"));

outFile << fullPath << std::endl;

outFile.close();

storages.clear();

ReadEntriesFromFile(L"D:\\БГУИР\\Курсовые\\CryptoPanda\\CryptoPanda\\CPStorages.txt");

}

bool СontainsInvalidChars(const std::wstring& input) {

static const std::wstring invalidChars = L".,;<>:\"/\\|?\*\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0A\x0B\x0C\x0D\x0E\x0F\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1A\x1B\x1C\x1D\x1E\x1F";

for (wchar\_t c : input) {

if (invalidChars.find(c) != std::wstring::npos) {

return true;

}

}

return false;

}

bool CreateFolder(const std::wstring& path, const std::wstring& folderName) {

std::wstring fullPath = path + L"\\" + folderName;

DWORD dwAttrib = GetFileAttributes(fullPath.c\_str());

if (dwAttrib != INVALID\_FILE\_ATTRIBUTES && (dwAttrib & FILE\_ATTRIBUTE\_DIRECTORY)) {

return true;

}

if (!CreateDirectory(fullPath.c\_str(), NULL)) {

return false;

}

return true;

}

void SaveToFile(const std::wstring& filename, const std::vector<BYTE>& data) {

std::ofstream ofs(filename, std::ios::binary | std::ios::app);

if (ofs.is\_open()) {

DWORD size = static\_cast<DWORD>(data.size());

ofs.write(reinterpret\_cast<const char\*>(&size), sizeof(size));

ofs.write(reinterpret\_cast<const char\*>(data.data()), data.size());

ofs.close();

}

}

std::vector<BYTE> ProtectData(const BYTE\* data, DWORD dataSize) {

DATA\_BLOB inputBlob = { dataSize, const\_cast<BYTE\*>(data) };

DATA\_BLOB outputBlob;

if (CryptProtectData(&inputBlob, NULL, NULL, NULL, NULL, 0, &outputBlob)) {

std::vector<BYTE> result(outputBlob.pbData, outputBlob.pbData + outputBlob.cbData);

LocalFree(outputBlob.pbData);

return result;

}

return {};

}

std::vector<BYTE> UnprotectData(const BYTE\* data, DWORD dataSize) {

DATA\_BLOB inputBlob = { dataSize, const\_cast<BYTE\*>(data) };

DATA\_BLOB outputBlob;

if (CryptUnprotectData(&inputBlob, NULL, NULL, NULL, NULL, 0, &outputBlob)) {

std::vector<BYTE> result(outputBlob.pbData, outputBlob.pbData + outputBlob.cbData);

LocalFree(outputBlob.pbData);

return result;

}

return {};

}

std::vector<BYTE> LoadPasswordByIndex(const std::wstring& filename, size\_t index) {

std::ifstream ifs(filename, std::ios::binary);

if (!ifs.is\_open()) {

std::wcerr << L"Не удалось открыть файл для чтения." << std::endl;

return {};

}

while (true) {

DWORD size;

ifs.read(reinterpret\_cast<char\*>(&size), sizeof(size));

if (ifs.eof()) break;

if (index == 0) {

std::vector<BYTE> data(size);

ifs.read(reinterpret\_cast<char\*>(data.data()), size);

return data;

}

ifs.ignore(size);

index--;

}

return {};

}

void SetDialogWnd() {

WNDCLASS wc = {};

wc.lpfnWndProc = dialogWndProc;

wc.hInstance = hInst;

wc.lpszClassName = L"PasswordCheck";

RegisterClass(&wc);

dialogWnd = CreateWindowEx(0, L"PasswordCheck", storages[storageID].name.c\_str(), WS\_BORDER | WS\_VISIBLE | WS\_OVERLAPPED, clientWidth / 2 - 200, clientHeight / 2 - 100, 400, 150, mainWnd, NULL, hInst, NULL);

CreateWindow(L"Button", L"OK", WS\_CHILD | WS\_VISIBLE | WS\_BORDER, 20, 80, 150, 25, dialogWnd, (HMENU)PASS\_CHECK, hInst, nullptr);

CreateWindow(L"Button", L"Cancel", WS\_CHILD | WS\_VISIBLE | WS\_BORDER, 210, 80, 150, 25, dialogWnd, (HMENU)PASS\_CANCEL, hInst, nullptr);

passCheckEdit = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER | ES\_PASSWORD, 20, 40, 340, 25, dialogWnd, NULL, NULL, NULL);

ShowWindow(dialogWnd, SW\_SHOW);

}

bool ComparePassword(const std::wstring& inputPassword, const std::wstring& filename, size\_t index) {

std::vector<BYTE> loadedPassword = LoadPasswordByIndex(filename, index);

if (!loadedPassword.empty()) {

std::vector<BYTE> decryptedPassword = UnprotectData(loadedPassword.data(), loadedPassword.size());

if (!decryptedPassword.empty()) {

std::wstring decryptedWPassword = std::wstring(reinterpret\_cast<wchar\_t\*>(decryptedPassword.data()), decryptedPassword.size() / sizeof(wchar\_t));

return (inputPassword == decryptedWPassword);

}

}

return false;

}

bool CheckPassword() {

int x = GetWindowTextLength(passCheckEdit);

if (x > 22) {

MessageBox(mainWnd, L"Password is to long", L"failed", MB\_OK);

return false;

}

if (x == 0) {

MessageBox(mainWnd, L"Enter Password", L"failed", MB\_OK);

return false;

}

std::wstring password(x, L'\0');

GetWindowText(passCheckEdit, &password[0], x + 1);

if (ComparePassword(password, L"CPKeys.bin", storageID)) return true;

else MessageBox(mainWnd, L"Wrong password", L"failed", MB\_OK);

return false;

}

void ViewStorage(HDC hdc) {

TextOut(hdc, 40, 35, storages[storageID].name.c\_str(), storages[storageID].name.size());

HPEN hPen = CreatePen(PS\_SOLID, 1, RGB(128, 128, 128));

SelectObject(hdc, hPen);

MoveToEx(hdc, 0, 65, nullptr);

LineTo(hdc, clientWidth,65);

int height = clientHeight;

}

//поулчение всех имён файлов из хранилища в расшифрованном виде

void GetFilesInStorage() {

std::wstring key = GetPassword();

std::wstring dirPath = storages[storageID].path;

try {

for (const std::filesystem::directory\_entry& entry : std::filesystem::recursive\_directory\_iterator(dirPath)) {

if (std::filesystem::is\_regular\_file(entry.status())) {

FileNames filename;

std::filesystem::path filePath = entry.path(); // Получаем путь к файлу

std::wstring filenameWithoutExtension = filePath.stem().wstring();

encoder->SetKey(key);

filename.encodedName = filenameWithoutExtension;

std::wstring name = encoder->EncryptLine(filenameWithoutExtension);

filename.name = name;

filesInStorage.push\_back(filename);

}

}

}

catch (const std::filesystem::filesystem\_error& e) {

MessageBox(viewStorageWnd, L"Can not reade storage", L"Failed", NULL);

}

}

void SetAddFileWnd()

{

WNDCLASS wc = {};

wc.lpfnWndProc = addFileWndProc;

wc.hInstance = hInst;

wc.lpszClassName = L"AddFileInStorage";

RegisterClass(&wc);

addFileInStorageWnd = CreateWindowEx(0, L"AddFileInStorage", storages[storageID].name.c\_str(), WS\_OVERLAPPED | WS\_BORDER | WS\_VISIBLE & ~WS\_SIZEBOX, clientWidth / 2 - 200, clientHeight / 2 - 100, 600, 200, mainWnd, NULL, hInst, NULL);

CreateWindow(L"Button", L"OK", WS\_CHILD | WS\_VISIBLE | WS\_BORDER, 20, 125, 235, 25, addFileInStorageWnd, (HMENU)ADD\_FILE\_OK, hInst, nullptr);

CreateWindow(L"Button", L"Cancel", WS\_CHILD | WS\_VISIBLE | WS\_BORDER, 325, 125, 235, 25, addFileInStorageWnd, (HMENU)ADD\_FILE\_CANCEL, hInst, nullptr);

newFilePathEdit = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER, 20, 30, 540, 25, addFileInStorageWnd, NULL, NULL, NULL);

newFileNameEdit = CreateWindow(L"Edit", L"", WS\_VISIBLE | WS\_CHILD | WS\_BORDER, 20, 85, 540, 25, addFileInStorageWnd, NULL, NULL, NULL);

ShowWindow(addFileInStorageWnd, SW\_SHOW);

}

void AddNewFileInStorage()

{

int x = GetWindowTextLength(newFilePathEdit);

if (x == 0)

{

MessageBox(mainWnd, L"Enter path", L"failed", MB\_OK);

return;

}

std::wstring direcory(x, L'\0');

GetWindowText(newFilePathEdit, &direcory[0], x + 1);

x = GetWindowTextLength(newFileNameEdit);

if (x == 0)

{

MessageBox(mainWnd, L"Enter name", L"failed", MB\_OK);

return;

}

std::wstring name(x, L'\0');

GetWindowText(newFileNameEdit, &name[0], x + 1);

for (int i = 0;i < filesInStorage.size();i++) {

if (filesInStorage[i].name == name) {

MessageBox(viewStorageWnd, L"This file name is already in storage.Choose another one", L"Failed", MB\_OK);

return;

}

}

std::wstring key = GetPassword();

encoder->SetKey(key);

std::wstring encodedName = L" ";

encodedName = encoder->EncryptLine(name);

encoder->SetKey(key);

std::wstring newFilePath = storages[storageID].path + L"\\" + encodedName + L".txt";

if (std::filesystem::exists(direcory) && encoder->EncryptDecryptFile(direcory, newFilePath))

{

AddItemInFileTable(name);

filesInStorage.push\_back({name, encodedName});

}

else MessageBox(viewStorageWnd, L"FilePath doesn't exist", L"Faild", MB\_OK);

}

//обновление параметров скролла

void UpdateScroll() {

int rowsLeft = storages.size() - 8;

if (rowsLeft < 0) rowsLeft = 0;

leftStorages = rowsLeft;

SetScrollRange(stListWnd, SB\_VERT, 0, rowsLeft, true);

}

// получение мастер-ключа из DPAPI

std::wstring GetPassword() {

std::vector<BYTE> loadedPassword = LoadPasswordByIndex(L"CPKeys.bin", storageID);

if (!loadedPassword.empty()) {

std::vector<BYTE> decryptedPassword = UnprotectData(loadedPassword.data(), loadedPassword.size());

if (!decryptedPassword.empty()) {

std::wstring decryptedWPassword = std::wstring(reinterpret\_cast<wchar\_t\*>(decryptedPassword.data()), decryptedPassword.size() / sizeof(wchar\_t));

return decryptedWPassword;

}

}

return L"";

}

void AddItemInFileTable(std::wstring newFile) {

int i = filesInStorage.size();

LVITEM item;

item.mask = LVIF\_TEXT;

item.iItem = i;

item.iSubItem = 0;

item.pszText = const\_cast<LPWSTR>(newFile.c\_str());

ListView\_InsertItem(fileInStorageListWnd, &item);

}

void AddFilesInFileList() {

for (int i = 0;i < filesInStorage.size();i++) {

LVITEM item;

item.mask = LVIF\_TEXT;

item.iItem = i;

item.iSubItem = 0;

item.pszText = const\_cast<LPWSTR>(filesInStorage[i].name.c\_str());

ListView\_InsertItem(fileInStorageListWnd, &item);

}

}

void DeleteFilesFromFileTable() {

ListView\_DeleteAllItems(fileInStorageListWnd);

}

//получение координат клика по файлу из хранилища

int GetFileItemClickPos(int x, int y) {

for (int i = 0;i < filesInStorage.size();i++) {

if (y > i \* 20 && y < (i + 1) \* 20)

return i;

}

return -1;

}

bool DeleteFileFromStorage(int fileId) {

std::wstring filePath = storages[storageID].path + L"\\" + filesInStorage[fileId].encodedName + L".txt";

DWORD attributes = GetFileAttributes(filePath.c\_str());

if (attributes != INVALID\_FILE\_ATTRIBUTES) {

SetFileAttributes(filePath.c\_str(), attributes & ~FILE\_ATTRIBUTE\_READONLY);

}

if (DeleteFile(filePath.c\_str())) {

MessageBox(viewStorageWnd, L"File deleted successfully.", L"Info", MB\_OK);

ListView\_DeleteItem(fileInStorageListWnd, fileId);

return true;

}

MessageBox(viewStorageWnd, L"Failed to delete the file.", L"Error", MB\_OK | MB\_ICONERROR);

SetFileAttributes(filePath.c\_str(), attributes);

return false;

}

bool ExportFileFromStorage(int fileId) {

std::wstring output = L"D:\\БГУИР\\Курсовые\\CryptoPanda\\Export\\" + filesInStorage[fileId].name;

std::wstring input = storages[storageID].path + L"\\" + filesInStorage[fileId].encodedName + L".txt";

std::wstring key = GetPassword();

encoder->SetKey(key);

if (encoder->EncryptDecryptFile(input, output)) {

MessageBox(viewStorageWnd, L"File exported in Export Folder", L"Done", MB\_OK);

return true;

}

else MessageBox(viewStorageWnd, L"File wasn't exported", L"Failed", MB\_OK);

return false;

}

**Encoder.h**

#pragma once

#include <fstream>

#include <bitset>

#include <sstream>

#include <vector>

#include <locale>

#include <codecvt>

#include <filesystem>

#include <Windows.h>

class Encoder {

private:

uint32\_t iniKey; //исходный ключ

uint8\_t Key; //ключ для шифрования

const int BlockSize = 256;

void shift();

uint32\_t SumBytes(const std::wstring& input);

public:

Encoder();

void SetKey(std::wstring key);

bool EncryptDecryptFile(const std::wstring& input, const std::wstring& output);

std::wstring EncryptLine(const std::wstring& input);

};

**Encoder.cpp**

#include "Encoder.h"

Encoder::Encoder() {

}

void Encoder::SetKey(std::wstring key) {

this->iniKey = SumBytes(key);

this->Key = 0;

}

uint32\_t Encoder::SumBytes(const std::wstring& input) {

uint32\_t sum = 0;

int i = 1;

for (const wchar\_t& ch : input) {

sum += static\_cast<uint32\_t>(static\_cast<uint8\_t>(ch)) \* i;

i++;

}

return sum;

}

void Encoder::shift() {

Key = 0;

for (int i = 0; i < 8; i++) {

// Получить новый бит (младший байт регистра сдвига)

uint8\_t xorBit = (iniKey & 1) ^ ((iniKey >> 26) & 1) ^ ((iniKey >> 27) & 1) ^ ((iniKey >> 31) & 1);

// Получить новый бит ключа

uint8\_t bit32 = (iniKey >> 31) & 1;

// Запись нового бита в ключ справа

Key = (Key << 1) | bit32;

// Записать в регистр новый бит

iniKey = (iniKey << 1) | xorBit;

}

}

bool Encoder::EncryptDecryptFile(const std::wstring& input, const std::wstring& output) {

std::ifstream file\_in(input, std::ios::binary);

std::ofstream file\_out(output, std::ios::binary);

if (!file\_in.is\_open()) {

return false;

}

if (!file\_out.is\_open()) {

return false;

}

std::vector<uint8\_t> buffer(BlockSize);

while (file\_in.read(reinterpret\_cast<char\*>(buffer.data()), buffer.size()) || file\_in.gcount() > 0) {

int bytesRead = file\_in.gcount();

int j = 0;

for (int i = 0; i < bytesRead; i++) {

shift();

buffer[i] ^= Key;

}

file\_out.write(reinterpret\_cast<char\*>(buffer.data()), bytesRead);

}

DWORD attributes = GetFileAttributes(output.c\_str());

if (attributes != INVALID\_FILE\_ATTRIBUTES) {

SetFileAttributes(output.c\_str(), attributes | FILE\_ATTRIBUTE\_READONLY);

}

file\_in.close();

file\_out.close();

return true;

}

std::wstring Encoder::EncryptLine(const std::wstring& input) {

std::wstring output;

output.resize(input.size());

for (size\_t i = 0; i < input.size(); ++i) {

shift();

output[i] = input[i] ^ Key;

return output;

}