**Техническое задание**

**на защищенное хранилище**

**Содержание**

[1 Общие сведения 4](#_Toc478210449)

[1.1 Полное наименование системы 4](#_Toc478210450)

[1.2 Основания разработки 4](#_Toc478210451)

[1.3 Сроки исполнения работ 4](#_Toc478210452)

[2 Характеристика объекта реализации 5](#_Toc478210453)

[2.1 Краткое описание объекта 5](#_Toc478210454)

[2.2 Краткое описание серверной части приложения 5](#_Toc478210455)

[2.3 Краткое описание клиентской части приложения 5](#_Toc478210456)

[2.4 Краткое описание базы данных клиентов 5](#_Toc478210457)

[3 Требования к серверной части 6](#_Toc478210458)

[3.1 Требования к размещению серверной части 6](#_Toc478210459)

[3.2 Требования к хранению файлов 6](#_Toc478210460)

[3.2 Требование к режиму регистрации клиентов 6](#_Toc478210461)

[3.3 Требования к режиму авторизации клиентов 6](#_Toc478210462)

[3.4 Требования к режиму загрузки 6](#_Toc478210463)

[3.5 Требования к режиму скачивания 7](#_Toc478210464)

[3.6 Требования к режиму восстановления файлов 7](#_Toc478210465)

[3.7 Требования разграничению доступа 7](#_Toc478210466)

[4 Требования к Клиентской части 9](#_Toc478210467)

[4.1 Требования к размещению клиентской части 9](#_Toc478210468)

[4.2 Требования к интерфейсу 9](#_Toc478210469)

**Перечень сокращений и условных обозначений**

БД – база данных;

СЗУХД – система защищенного удаленного хранения данных

# 1 Общие сведения

## 1.1 Полное наименование системы

Полное наименование системы: Система защищенного удаленного хранения данных.

## 1.2 Основания разработки

Основание для выполнения работ, являются документы:

* Техническое задание;
* Задание на курсовую работу;

## 1.3 Сроки исполнения работ

Начало разработки: 06.02.2017

Окончание разработки: 31.05.2017

# 2 Характеристика объекта реализации

## 2.1 Краткое описание объекта

Проект представляет собой клиент-серверное приложение, реализующее создание защищенного корпоративного файлового хранилища, с хранением клиентской информации в базе данных клиентов.

Основное назначение приложения – обеспечение надежного хранения критичной (в т.ч. конфиденциальной) информации.

## 2.2 Краткое описание серверной части приложения

Сервер должен реализовывать следующие режимы работы:

* Режим авторизации клиентов;
* Режим загрузки файлов;
* Режим скачивания файлов;
* Режим восстановления файла;

Сервер должен реализовывать следующий функционал:

* Регистрация клиентов и генерация ключевой информации, с занесением данных клиента в БД;
* Авторизация клиентов на сервере на основе защищенных алгоритмов;
* Создание защищенного соединения между клиентом и сервером при загрузке и скачивании файлов;
* Ограничение доступа к файлам, принадлежащим иным клиентам
* Сохранение удаленных файлов в корзине для последующего восстановления или окончательного уничтожения

## 2.3 Краткое описание клиентской части приложения

Клиентское приложение должно реализовывать следующие функции:

* Интерфейс взаимодействия;
* Поддержка алгоритмов аутентификации, используемых для авторизации на сервере;
* Поддержка алгоритмов генерации сессионных ключей;
* Поддержка алгоритмов симметричного шифрования, используемых на сервере, на основе сессионных ключей;

## 2.4 Краткое описание базы данных клиентов

База данных должна обеспечивать хранение аутентификационных данных клиентов;

# 3 Требования к серверной части

## 3.1 Требования к размещению серверной части

Серверная часть должна быть установлена внутри корпоративной сети организации, подключение из внешней сети должно быть исключено.

## 3.2 Требования к хранению файлов

СЗУХД должна быть централизованной. Хранилище состоит из каталогов клиентов, публичного каталога и «корзины». В каталогах также хранятся файлы БД, в которых записана информация о каждом файле в каталоге. Создание каталогов клиентами запрещено.

В БД каталога, в который загружается файл, добавляется запись вида:

* ID;
* ID владельца;
* Наименование файла;
* Расширение;
* Дата добавления;
* MD5-сумма
* Метка (для удобства в работе).

## 3.2 Требования к режиму авторизации клиентов

Регистрация новых клиентов происходит на стороне сервера.

Сервер в режиме авторизации клиентов должен реализовывать следующее:

* Генерация ключевой информации;
* Защищенная передача ключевой информации;
* Проверка номера жесткого диска;
* Запрос пароля клиента;

## 3.3 Требования к режиму загрузки

Доступ к режиму загрузки должен предоставляться только авторизованным клиентам. Для загрузки создаются новые ключи транзакций. Контрольная сумма MD5 загруженного файла сверяется с файлом в устройстве клиента для подтверждения целостности. Должна быть исключена возможность внедрения вредоносного кода в систему. Необходимо обеспечить это путем запрета наиболее опасных расширений файлов:

* .EXE
* .COM
* .MSC
* .MSI
* .JAR
* .CMD
* .BAT
* .VB, .VBS, .VBE
* .JS, .JSE
* .REG

## 3.4 Требования к режиму скачивания

Доступ к режиму скачивания должен предоставляться только авторизованным клиентам. Для загрузки создаются новые ключи транзакций. Контрольная сумма MD5 файла в Хранилище сверяется со скачанным файлом в устройстве клиента для подтверждения целостности.

## 3.5 Требования к режиму восстановления файлов

Удаленный файл помещаются в «корзину». Запись о нем переносится из БД исходного каталога в БД «корзины», где обновляется «дата добавления». В течение 3-х дней после удаления авторизованный клиент может восстановить файл в исходный каталог или уничтожить вручную. После этого срока файл и запись о нем уничтожаются.

## 3.6 Требования разграничению доступа

Неавторизованный пользователь имеет доступ к аутентификации в системе. После авторизации пользователь получает доступ к остальным режимам с некоторыми ограничениями.

Так, загрузка файлов возможна только в личный или публичный каталог. Перевод файлов между каталогами запрещен. Максимальный размер личных каталогов не должен превышать 500 Мб. Максимальный размер файлов одного клиента в публичном каталоге не должен превышать 100 Мб. Замена «чужих» файлов в публичном каталоге запрещена.

Скачивать можно личные файлы из личного каталога и файлы всех клиентов из публичного каталога.

Удалять разрешено только файлы, которые принадлежат клиенту. В корзине возможно видеть, восстанавливать или удалять только свои файлы.

Клиенты не должны видеть файлы БД, чужие папки, корневой каталог и чужие файлы в «корзине».

В прочих вопросах пользоваться принципом «запрещено всё то, что прямо не разрешено».

# 4 Требования к Клиентской части

## 4.1 Требования к размещению клиентской части

Клиентская часть должна быть установлена на конечных устройствах корпоративной сети организации, подключение из внешней сети должно быть исключено.

## 4.2 Требования к интерфейсу

Интерфейс клиента должен быть графическим. Содержимое окон должно быть интуитивно понятным, а работа с системой не должна вызывать вопросов. В случае возникновения сложностей клиенты должны получать помощь в виде справки.

* Требования к внешнему виду:
* Стиль приложения: оконный
* Цветовая схема: стандартная цветовая схема Windows
* Шрифт: Arial
* Размер шрифта: 10 пт