Оглавление

[Введение 2](#_Toc322260939)

[Постановка задачи 3](#_Toc322260940)

[1. Исследовательская часть 4](#_Toc322260941)

[1.1. Анализ аналогичных программных продуктов 4](#_Toc322260942)

[1.1.1. Плагин для WordPress - Simpleforum 4](#_Toc322260943)

[1.1.2. Simple Machine Forum (SMF) 5](#_Toc322260944)

[1.1.3. phpBB 6](#_Toc322260945)

[1.1.4 Выводы 7](#_Toc322260946)

[1.2. Анализ программных средств разработки 8](#_Toc322260947)

[1.2.1. Выбор инструментальных средств 8](#_Toc322260948)

[1.2.2. Выбор способа хранения данных 9](#_Toc322260949)

[1.2.3. Выбор основных технологий 10](#_Toc322260950)

[1.2.4. Сервер Apache 11](#_Toc322260951)

[1.2.5. Netbeans IDE 12](#_Toc322260952)

[1.2.6. Средство отладки Opera 13](#_Toc322260953)

[1.2.7. Система контроля версий GitHub 14](#_Toc322260954)

[1.2.8. Клиент GitHub - TortoiseGit 15](#_Toc322260955)

[1.2.9. Sql сервер MySQL 16](#_Toc322260956)

[1.2.10. Шифрование MD5 17](#_Toc322260957)

# Введение

На сегодняшний день

# Постановка задачи

# 1. Исследовательская часть

## 1.1. Анализ аналогичных программных продуктов

### 1.1.1. Плагин для WordPress - Simpleforum

### 1.1.2. Simple Machine Forum (SMF)

### 1.1.3. phpBB

### 1.1.4 Выводы

## 1.2. Анализ программных средств разработки

### 1.2.1. Выбор инструментальных средств

### 1.2.2. Выбор способа хранения данных

### 1.2.3. Выбор основных технологий

### 1.2.4. Сервер Apache

### 1.2.5. Netbeans IDE

### 1.2.6. Средство отладки Opera Dragonfly

### 1.2.7. Система контроля версий GitHub

### 1.2.8. Клиент GitHub - TortoiseGit

### 1.2.9. Sql сервер MySQL

### 1.2.10. Шифрование MD5

MD5 позволяет получать относительно надёжный идентификатор для блока данных. Такое свойство алгоритма широко применяется в разных областях. Оно позволяет искать дублирующиеся файлы на компьютере, сравнивая MD5 файлов, а не их содержимое. Как пример, dupliFinder — графическая программа под Windows и Linux. Такой же поиск может работать и в интернете.

С помощью MD5 проверяют целостность скачанных файлов — так, некоторые программы идут вместе со значением хеша. Например, диски для инсталляции.

MD5 используется для хеширования паролей. В системе UNIX каждый пользователь имеет свой пароль и его знает только пользователь. Для защиты паролей используется хеширование. Предполагалось, что получить настоящий пароль можно только полным перебором. При появлении UNIX единственным способом хеширования был DES (Data Encryption Standard), но им могли пользоваться только жители США, потому что исходные коды DES нельзя было вывозить из страны. Во FreeBSD решили эту проблему. Пользователи США могли использовать библиотеку DES, а остальные пользователи имеют метод, разрешённый для экспорта. Поэтому в FreeBSD стали использовать MD5 по умолчанию.[11]. Некоторые Linux-системы также используют MD5 для хранения паролей.

Многие системы используют базу данных для хранения паролей и существует несколько способов для хранения паролей.

* Пароли хранятся как есть. При взломе такой базы все пароли станут известны.
* Хранятся только хеши паролей (с помощью MD5, SHA). Найти пароли можно только полным перебором. Но при условии использования несложного, популярного или просто несчастливого пароля (который встречался ранее и занесён в таблицу) такая задача решается за доли секунды. Пароль из таблицы был найден всего за 0,036059 сек.
* Хранятся хеши паролей и несколько случайных символов. К каждому паролю добавляется несколько случайных символов (их ещё называют «salt» или «соль») и результат ещё раз хешируется. Например, md5(md5(pass)+word). Найти пароль с помощью таблиц таким методом не получится.