Титульный лист

Secure disk

Содержание

[1. Введение 3](#_Toc416038431)

[2. Обзор литературы 4](#_Toc416038432)

[2.1. Устройство логического диска 4](#_Toc416038433)

[2.2. Язык программирования 4](#_Toc416038434)

[2.3. Чтение и запись 4](#_Toc416038435)

[2.4. Шифрование/дешифрование 4](#_Toc416038436)

# 1. Введение

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречен на бесконечность в своей последовательности. Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества.

Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированных доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте. Однако по данным, опубликованным в сети, общие потери от несанкционированного доступа к информации в компьютерных системах в 1997 году оценивались в 20 миллионов долларов, а уже в 1998 года в 53,6 миллионов долларов.

В связи с этим, было принято решение, разработать приложение, позволяющее защитить информацию на диске.

# 2. Обзор литературы

## 2.1. Устройство логического диска

## 2.2. Язык программирования

В качестве языка программирования был выбран С(си). [2]

## 2.3. Чтение и запись

Ч

## 2.4. Шифрование/дешифрование

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующим свойством:

Если известно x, то f(x) вычислить относительно просто

Если известно y=f(x), то для вычисления x нет простого (эффективного) пути.

Под односторонностью понимается не теоретическая однонаправленность, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени.[1]

RSA Class

# 3. Список литературы

<http://ru.wikipedia.org/wiki/Главная_загрузочная_запись>

<http://ru.wikipedia.org/wiki/Раздел_диска>

1.

2. <http://www.codenet.ru/progr/cpp/c-vs-cpp/>

3. https://ru.wikipedia.org/wiki/RSA