Департамент образования города Москвы

Государственное бюджетное общеобразовательное учреждение города Москвы «Гимназия №1505

«Московская городская педагогическая гимназия-лаборатория»»

**РЕФЕРАТ**

**на тему**

**Хэширование и пароли**

Выполнил:

Шигаров Дмитрий Алексеевич

Руководитель:

Пяткина Галина Александровна

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись руководителя)

Рецензент:

ФИО рецензента

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись рецензента)

Москва

2016/2017 уч.г.

**Оглавление**

Введение

1. часть. Общее понятие хэширования
2. Назначение пароля
3. Понятие хеш-функция
4. Понятие хеш-таблица и коллизия в ней
5. часть. Угрозы для хэша
6. Варианты атак на хэш пароля
7. Способы защиты от атак на хэш пароля
8. Свойства влияющие на пароль

Заключение

Список литературы

**Введение**

В современном мире всё больше и больше используется интернет. Мы производим покупки и оплаты с различных сайтов, где остро становиться вопрос о защите личных данных. У каждой информации есть своя ценность, значит такие же усилия будут прилагать люди чтобы заполучить её себе. Поэтому программисты хешированием стараются наиболее надёжно скрыть её местонахождение и путь к ней. Таким образом в современном мире, выбранная мной тема наиболее актуальна в современном мире.

Хэширование— преобразование массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины, выполняемое определённым алгоритмом.

К сожалению не все люди просвещены в этой сфере и парой ведутся на уловки мошенников. Иногда люди просто не знают о необходимых средствах защиты личной информации, что приводит к её утечке.

Цель моего исследования – это изучить способы взлома и защиты данных, а также научиться правильно и наиболее надёжно подбирать пароль.

В своём исследовании я расскажу о современных разно уровневых способах защиты паролей на различных хранителях, информации и с какими угрозами вы можете столкнуться. Также я расскажу как правильно выбрать наиболее надёжный пароль для защиты денег и личной информации от различных вирусов и способов взломов.

**Задачи**

Изучить информацию по данной теме реферата.

Объяснить необходимость надёжной защиты информации.

Изучить виды различных атак и способов взлома.

Рассмотреть виды различных способов сокрытия и защиты информации.

Рассказать о необходимых правилах создания надёжного пароля.

**Список литературы**

1. Корбит А.Г., Кривоносова Т.М. Методическое пособие. Алгоритмы вычислительной математики. [ Электронный ресурс]

Режим доступа: <http://www.studfiles.ru/preview/5514229/page:7/>

1. Разработчики PHP. Технология хэширования паролей [Электронный ресурс]

Режим доступа: <http://phpfaq.ru/tech/hashing>

1. Издательский дом "К-Пресс". Бинарные деревья. [Электронный ресурс]

Режим доступа: <http://www.k-press.ru/CS/2000/4/bintree_htm/hash.asp>

1. Сергей Соболь. Хэш-таблицы. [Электронный ресурс]

Режим доступа: <https://acm.bsu.by/w/images/c/c0/HashTables.pdf>

1. Эрик Грубер. Подбор LM-хеша – радужные таблицы против прямого перебора при помощи GPU. [Электронный ресурс]

Режим доступа: <http://www.securitylab.ru/analytics/462201.php>

1. Сергей Суягин.Как создать и запомнить надежный пароль. [Электронный ресурс]

Режим доступа: <https://lifehacker.ru/2014/06/07/nadyozhnyj-parol/>

1. Атака на хэши. (практическое руководство). [Электронный ресурс]

Режим доступа: <https://forum.antichat.ru/threads/68675/>

1. Список словарей: Электронный ресурс.

Режим доступа: <http://wordbook.xyz/download>