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:

Бубер Любовь Леонидовна

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

 Москва

 2016/2017 уч.г.

**Оглавление**

|  |  |  |
| --- | --- | --- |
|  | ОГЛАВЛЕНИЕ |  |
| 1 | Введение | 3 |
| 2 | Основная часть 1 Общее понятие хэширования | 5 |
|  | * 1. Параграф

Назначение пароля | 5 |
|  | 1.2 Параграф Понятие хеш-функция | 6 |
|  | 1.3Параграф Понятие хеш-таблица и коллизия | 7 |
| 2 | Основная часть 2 Угрозы для хэша | 9 |
|  | 2.1 Параграф Варианты атак на хэш пароля | 9 |
|  | 2.2 Параграф Способы защиты от атак на хэш пароля | 10 |
|  | 2.3 Параграф Свойства, влияющие на надёжность пароля | 11 |
| 3 | Заключение | 12 |
| 4 | Список литературных источников | 14 |

**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, серьёзные усилия будут прилагать люди, чтобы заполучить её себе. Поэтому программисты хешированием стараются наиболее надёжно скрыть её местонахождение и путь к ней. Таким образом, 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 пользователи 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 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 взломов.

**Задачи**

1. Изучить информацию по данной теме реферата.
2. Объяснить необходимость надёжной защиты информации.
3. Изучить виды различных атак и способов взлома.
4. Рассмотреть виды различных способов сокрытия и защиты информации.
5. Рассказать о необходимых правилах создания надёжного пароля.

**ПЕРВАЯ ГЛАВА**

1. **Назначение пароля**

Порой информация это настоящее «сокровище» для взломщиков. Поэтому люди стараются максимально обезопасить свою собственность. В различных сферах техно индустрии защита стала одной из главных проблем, которую нельзя пропустить.

Пароли использовались с древнейших времён. Например, в Древнем Риме он использовался для защиты войск. Таким образом, чтобы попасть в расположение своей части солдатам необходимо было сказать пароль караульному.[[1]](#footnote-1)

В современном мире защита паролем - первый этап по обеспечению безопасности информации на вашем компьютере. Использование пароля позволяет вам защитить информацию на компьютере от многих угроз:

•несанкционированного доступа (как от прямого вторжения, так и по сети);

•от вирусов и шпионских программ.

1. **Понятие хеш-функция**

Одного пароля для защиты любой информации мало. Необходимо защитить сам пароль, а точнее его местоположение и содержание. Для того придумывается множество алгоритмов для сокрытия. Они называются хэш-функции.

В январе 1953 года сотрудник фирмы IBM Ханс Петер Лун впервые предложил использовать «хэш-кодирование». Принятую во всём мире идею хэширования описал в 1956 году Арнольд Думи в своей работе «Computers and automation». Думи рассматривал «хэширование», как решение проблемы перечня, предложил использовать в качестве «хэш-адреса» остаток от деления на простое число. После Думи термин хэширование употреблялся в таких изданиях, как:

1. Статья Уэсли Питерсона (1957 год).
2. Работа Вернера Бухгольца (1963 год).
3. Книга Херберта Хеллермана «Принципы цифровых вычислительных систем» (1967 год).

Но наибольшее распространение хэширование получило после публикации в 1968 году статьи Робертом Моррисом. Эта работа считается ключевой публикацией, вводящей понятие о «хешировании» в научный оборот, и закрепившей термин хеширование, ранее применявшийся только специалистами. До начала 1990-х годов в России вместо термина хеширование, использовалось слово «расстановка» или «окрошка». Однако сейчас используется преимущественно термин «хеширование».

Таким образом, хэш-функция это функция особым образом переделывающая пароль. Само переделанное значение называется хэш-кодом.

Также, важной особенностью хэширования является необратимость. С помощью хэш-функции мы можем получить для каждого пароля хэш-код, но, зная хэш-код, мы не сможем узнать саму функцию. Но при простой хэш-функции довольно легко понять алгоритм, поэтому чтобы улучшить безопасность придумывают более сложные функции.

Примером использования полностью рабочего алгоритма хэширования является использование алгоритма MD5(Message Digest 5) в операционной системе FreeBSD. MD5 это 128-битный алгоритм хэширования, разработанный профессором Рональдом Ривестом в начале 90-х годов. На выходе обычно представляется последовательностью из 32 шестнадцатеричных цифр. [[2]](#footnote-2) Подробнее об устройстве MD5 можно узнать здесь: Описание алгоритма MD5

//URL:<http://re.mipt.ru/infsec/2004/essay/2004_MD5_Message-Digest_Algorithm__Strelnikov.pdf>

1. **Понятие хеш-таблица и коллизия**

Хэш-таблица — это массивы, хранящие пары информации: ключ, значение, и выполняющие три операции: операцию добавления новой пары, операцию поиска и операцию удаления пары по ключу. Выполнение операции в хэш-таблице начинается с вычисления хэш-функции от ключа. Получающийся хэш играет роль индекса в массиве. Затем выполняемая операция перенаправляется объекту, который хранится в соответствующей ячейке массива.

Коллизия хэш-функции — ситуация, при которой два разных результата имеют одинаковый хэш-код. Это возможно, если длина последовательности символов будет достаточно большой. Чем больше длина, тем больше вероятность совпадения хэша. Коллизии осложняют использование хэш-таблиц, так как нарушают исключительность соответствия между хэш-кодами и данными. Тем не менее, существуют специальные методики для преодоления возникающих сложностей:

1. Метод цепочек
2. Открытая адресация
3. Хэширование с солью

Метод цепочек: технология сцепления элементов состоит в том, что элементы множества, которым соответствует одно и то же хэш-значение, связываются в цепочку-список. В позиции с определённым номером хранится указатель на список тех элементов, у которых хэш-значение ключа равно тому же номеру.

Открытая адресация: в отличие от хэширования с цепочками, при открытой адресации никаких списков нет, а все записи хранятся в самой хэш-таблице. Каждая ячейка таблицы содержит элемент такого множества.

Другим действенным средством является хэширование с солью, но я расскажу об этом позже.

**ВТОРАЯ ГЛАВА**

1. **Варианты атак хэша пароля**
2. Использование "радужных таблиц".
3. Фишинг
4. Перебор по словарям.
5. Вредоносное программное обеспечение

Радужная таблица - это комбинация уже готовых словарей хэш-функций, используемая для замены вычислений на поиск. Таблица включает в себя хэши всех возможных комбинаций паролей для многих видов алгоритма хэширования. Время, необходимое для взлома пароля с помощью радужной таблицы - это время поиска нужного захэшированного пароля в списке. Тем не менее, сама таблица огромна и для просмотра требует серьезных вычислительных мощностей. Такой вариант атак не подходит для поиска хэша с использованием соли, направленной против этого.

Применение радужных таблиц намного проще и быстрее использования метода грубой силы для подбора, но само первостепенное создание требует огромные вычислительные мощности, без которой это невозможно сделать приемлемое время. К примеру, для захешированных паролей длиной не более 8 символов, состоящих из букв, цифр и специальных символов, таблицы могут быть сгенерированы на компьютере за 3 года.

Фишинг – это ещё один часто используемый способ получения доступа к чужой информации. Это процедура получения паролей путём обмана пользователей всемирной сети. Она включает в себя создание ложных сайтов, где пользователи вводят свои персональные данные, которые передаются в руки злоумышленников. Обычно такие сайты рассчитывают на невнимательность людей, так как адрес подставного сайта от оригинала отличается только одним символом.[[3]](#footnote-3)

Перебор это метод поиска, включающий в себя прогон большого количества вариантов, в поисках подходящего. Чаще всего перебираются «простые пароли», реже более сложные, так как количество возможных вариантов сильно влияет на время перебора.

Простые пароли это комбинации символов, для поиска которых затрачивается малое время (не больше дня).

Простыми паролями чаще всего считаются:

1. Небольшие пароли, состоящие из набора цифр
2. Небольшие пароли, состоящие из набора строчных или заглавных букв
3. Односложные пароли любой доступной длины (77777777)
4. Пароль, состоящий из рядом расположенных символов на клавиатуре.
5. Часто используемые пароли, комбинации паролей
6. “слитые” пароли популярных сервисов.

Вредоносное программное обеспечение

Также, есть способ получения паролей и хэшей, внедряясь в устройство. Программа перехвата фиксирует всю вводимую информацию и переправляет копию этого файла на адреса взломщиков.

1. **Способы защиты от атак на хэш пароля**

После появления способов взлома паролей возникла острая необходимость в более высоком уровне защиты. Для защиты от поиска по радужным таблицам была придумано хэширование с солью. Это комбинация из определённых символов, добавляемая к паролю перед вычислением хэша. Тем самым хэш удлиняется до размера, не обрабатываемого никакой радужной таблицей.

Для защиты от метода грубой силы и перебора по словарю нет особого алгоритма защиты. На различных сайтах присутствуют специализированные требования к паролям и всплывающие окна, задерживающие перебор. Но основной преградой является правильный алгоритм хэширования и трудность пароля.

При правильном использовании интернета, скачивание из надёжных источников, шансы быть атакованным вредоносными программами минимальны. Но специализированную защиту, обеспечивают антивирусы. Они предотвращают скачивание вирусов, а в случае проникновения обнаруживают и удаляют.

Чтобы избежать потери данных из-за фишинга, необходимо всегда внимательно проверять адрес сайта, прежде чем вводить персональные данные, и избегать переходов по подозрительным ссылкам.

1. **Свойства, влияющие на надёжность пароля**

Практически единственное, что может сделать среднестатистический пользователь, чтобы защитить свою информацию, это использовать грамотный пароль. Некоторые интернет ресурсы, требующие пароль, дают различные советы пользователю по этому вопросу. Таким образом, они вынуждают пользователя выбрать правильный по нескольким пунктам пароль.

* Пароль должен быть достаточно длинным, обычно от 8 до 12 символов.
* Пароль должен содержать заглавные и прописные буквы, символы, знаки препинания и пробелы.
* Пароль не должен ассоциироваться с пользователем, такие пароли как имена, фамилии, памятные даты, номера телефонов и т.д. не подходят.
* Пароль не должен состоять из известных фраз или популярных слов.
* Пароль не должен быть просто запоминающимся и широко используемым.
* Пароль не должен совпадать с логином, именем сайта или любой общедоступным связанным словом.

**ЗАКЛЮЧЕНИЕ**

 В современном мире повсеместно используется интернет. Появляются множество новых дистанционных услуг и возможностей. Кроме того, мы храним на отдалённых серверах всё больше личной информации: личные телефоны, пароли, номера банковских карточек, важные документы. Защита паролем - первый и наиболее простой этап по обеспечению безопасности информации на вашем компьютере. Но защитить каждое место хранения огромного количества паролей проблематично, для этого используется метод хеширования.

Хэширование — изменение входных данных определённым алгоритмом, что позволяет исключить хранение большого количество паролей. Вместо сравнивания входных данных, с хранящимися в базе, происходит сопоставление их хэшей. Это дает гарантию, что при случайной утечке списка хэшей никто не сможет воспользоваться важными данными для своих целей.

Но в современном мире, кроме получения паролей обманом, различными уловками, были придуманы способы взлома, такие как:

1. Использование "радужных таблиц".
2. Перебор.
3. Использование вредоносного программного обеспечения.
4. Фишинг.

С учётом известных угроз были разработаны различные средства защиты, против направленных атак. Для защиты от поиска по радужным таблицам было придумано хэширование с солью. В свою очередь, для защиты от метода грубой силы служит сама сложность пароля и различные особенности сайтов.

Важной частью защиты своей техники и информации является выбор пароля. Многие пользователи не придумывают устойчивый к подбору пароль, а руководствуются минимальными требованиями системы к паролю. Поэтому во избежание утечки информации необходимо выбирать пароль по нескольким требованиям:

1. Нераспространённость среди пользователей
2. Комбинация заглавных, прописных букв и цифр
3. Длина пароля, в зависимости от доступной

Таким образом, поставленные мной задачи были выполнены. И так как данная область сильно востребована и очень быстро развивается, необходимо продолжать работу по этой теме.

**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/](http://www.studfiles.ru/preview/5514229/page%3A7/)

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>

1. Описание алгоритма MD5[Электронный ресурс]

Режим доступа: <http://re.mipt.ru/infsec/2004/essay/2004_MD5_Message-Digest_Algorithm__Strelnikov.pdf>

1. Пароль // Научное вики сообщество URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C [↑](#footnote-ref-1)
2. MD5 // Компьютерные советы URL: http://comp-security.net/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-md5/ [↑](#footnote-ref-2)
3. Парольная защита // life-prog.ru URL: http://life-prog.ru/1\_2842\_sposobi-ataki-na-parol-obespechenie-bezopasnosti-parolya.html [↑](#footnote-ref-3)