***Государственное бюджетное образовательное учреждение   
высшего образования Московской области  
Университет «Дубна»***

**Лабораторная работа №1**

**На тему: система защиты компьютера с использованием паролей и средств не парольной защиты.**

**Студент:** Артюшов Андрей

**Группа**: 2281

**Позиция в группе:** 6

**Преподаватель:** П. А. Осипов

***г. Дубна, 2018***

**Задание 1. Ознакомление с теоретическим материалом и подготовка ответов на вопросы.**

**Как определить вероятность подбора пароля злоумышленником в течение срока его действия?**

Пусть *A* – мощность алфавита паролей - количество символов, которые могут быть использованы при составлении пароля (например, если пароль состоит только из малых английских букв, то A=26);

*L* – длина пароля;

 - число всевозможных паролей длины L, которые можно составить из символов алфавита A;

*V* – скорость перебора паролей злоумышленником;

*T* – максимальный срок действия пароля.

Тогда, вероятность *P* подбора пароля злоумышленником в течении срока его действия *V* определяется по следующей формуле:

.

**Как можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора злоумышленником и заданном сроке действия пароля?**

Для уменьшения скорости подбора пароля можно:

1. Использовать более длинные пароли;
2. Использовать все алфавитно-цифровые символы данного языка.

**Как изменится стойкость к взлому подсистемы парольной аутентификации при увеличении характеристик P, V, T? При их уменьшении?**

Исходя из формулы



можно заметить, что при увеличении V и T увеличится P, а это значит, что стойкость к взлому подсистемы парольной аутентификации будет ниже. При уменьшении данных параметров произойдет обратный процесс: стойкость к взлому увеличится.

**Задание 2. Определение необходимой длины пароля при заданных исходных данных.**

Для вычисления необходимой длины пароля нужно воспользоваться формулами, подставив в которые исходные значения можно получить ответ. Вот необходимые формулы для нахождения результата.

Пусть *A* – мощность алфавита паролей - количество символов, которые могут быть использованы при составлении пароля.

*L* – длина пароля;

 - число всевозможных паролей длины L, которые можно составить из символов алфавита A;

*V* – скорость перебора паролей злоумышленником;

*T* – максимальный срок действия пароля.

Тогда, вероятность *P* подбора пароля злоумышленником в течении срока его действия *V* определяется по следующей формуле:

.

В том случае, если значение А известно или задано, длину пароля можно определить по формуле:

L=LnS/LnA.

Получив исходные данные посчитаем:

**Задание 3. Изменение пароля при входе в операционную систему Windows**

Для изменения пароля пользователя, необходимо проделать следующие шаги:

1. Приготовьте компакт-диск, либо-же флешку, на которые должен быть записан специальный набор реанимационных программ, предназначающихся для восстановления Windows. Его вам нужно будет вставить в дисковод или в соответствующий порт во время последующей перезагрузки компьютера. Этот пакет реанимационных программ можно подготовить самостоятельно, загрузив туда программы, предназначающиеся для разделения, сохранения и восстановления данных, либо-же скачать какой-то, уже готовы, RBCD 10.0, к примеру;
2. Во время запуска ПК, для того, чтобы зайти в BIOS, нажимаем кнопку «DELETE». Там нам нужно будет поменять приоритет установки и назначить загрузку компьютера с CD-ROM. После этого мы посещаем наш загрузочный диск в дисковод и перезагружаем ПК;
3. Зайдя в меня диска-реаниматора, которое должно у нас появится после того, как произошла загрузка пакета реанимационных программ, мы должны выбрать редактируемую копию Windows и перейти в режим «Восстановление системы» — раздел, который будет находиться у вас в самом низу страницы;
4. Ищем командную строку и вводим туда «regedit» (ищем ее в диалоговых настройках этого же окна). Находим, а после и выделяем раздел HKEY\_LOCAL\_MACHINE, в котором нам потребуется выбрать File, а далее Load hive;
5. Открываем файл «SAM» и выбираем раздел — HKEY\_LOCAL\_MACHINE\имя\_куста\SAM\Domains\Account\Users\000001F4. Дважды щелкаем по размещенному там ключу F и переходим к самому первому значению, находящемуся в строке, которое нам нужно будет заменить цифрой 10;
6. В том же разделе выбираем «File», а после этого «Load Hive». Нажимаем «Да» для того, чтобы подтвердить выгрузку куста. Закрываем редактор реестра, заканчиваем таким образом процесс установки, достаем флешку или диск и перезагружаем компьютер.

**Задание 4. Исследование программного обеспечения для хранения паролей**

Для ознакомления с принципами работы хранения паролей была взята программа *LastPass.* Это достаточно простая и понятная в обращении программа. *LastPass* поможет создать для каждой учетной записи свой пароль, сложный и достаточно устойчивый к взлому, а самое важное то, что не придется хранить это у себя в памяти. Все пароли будут храниться в закодированном виде, закрытой одним главным ключом или специальным файлом.

Основные функции и особенности *LastPass:*

* Использование алгоритмов для шифрования баз данных паролей;
* Шифрование всей структуры данных, включая логин, имя и многое другое;
* Программа работает на защищенных потоках памяти;
* Программа защищена от клавиатурных шпионов;
* Программа в автоматическом режиме очищает буфер обмена после работы;
* Также программа имеет свой собственный алгоритм генерации паролей;
* Программа доступна в виде виджета в браузере;
* Так же программа подсказывает, похож ли новый пароль на мастер-пароли;
* Подсказывает, есть ли одинаковые пароли от разных ресурсов;
* Имеет публичный *API.*

Из недостатков программы *LastPass:*

* Как и любого другого менеджера хранения паролей есть вероятность взлома;
* Программа имеет открытый код, что дает злоумышленникам доступ к изучению работы системы.

**Задание 5. Разработка генератора паролей**

Программа для генерации паролей была разработана в среде программирования Python. Программа обладает возможностью выбора необходимых для создания пароля критериев таких как: заглавные буквы, прописные буквы и цифры. Программа не имеет GUI, а весь интерфейс реализован в терминале на рисунке (см. Рис. 1).

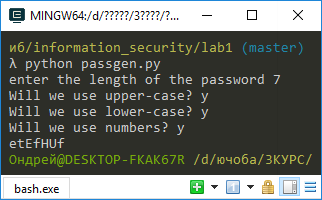


Рис. 1 «Интерфейс программы»

**Задание 6. Использование методов не парольной защиты**

Исследования методов не парольный защиты были проведены на примере программы *Rohos Logon Key*, разработанной компанией *Tesline-Service S.R.L*., предназначенной для хранения паролей в хорошо защищенном месте. Программа позволяет защитить *Windows* использую двухфакторную аутентификацию с помощью паролей, которые используются один раз. В целях повышения безопасности возможность настроить свой сервер для создания и доставки одноразового пароля конечному пользователю. С помощью данной функции нет необходимости отправлять секретный ключ ОТР и настраивать Аутентификацию на мобильном устройстве конечного пользователя.

Положительные стороны данной программы:

* Уникальная для своего класса структура аутентификации, которая дает возможность использовать в качестве входа не просто пароль, а внешний носитель;
* Удобство автоблокировки компьютера при отключении USB-Ключа;
* Использование одного ключа для доступа к нескольким устройствам.

За время изучения работы программы недостатков не было обнаружено.

На данный момент существует множество различных способов не парольной защиты, например: аутентификация по скану отпечатка пальца, скан сетчатки глаза и недавно изменившая мир аутентификация по анализу лица и глаз вместе взято.