**Лабораторная работа № 1**

**Тема: «Защита информации с помощью пароля»**

**Цель работы**

1. Изучить виды атак на пароль и защиту программного обеспечения с применением пароля.
2. Приобрести умения и навыки противодействия атакам на пароль.

**1 Теоретическая часть**

**1.1 Атаки на пароль**

На сегодняшний день пароль является наиболее приемлемым и потому наиболее часто используемым средством установления подлинности, основанным на знаниях субъектов доступа.

В любой критической системе ошибки человека-оператора являются чуть ли не самыми дорогостоящими и распространенными. В случае криптосистем, непрофессиональные действия пользователя сводят на нет самый стойкий криптоалгоритм и самую корректную его реализацию и применение.

В первую очередь это связано с выбором паролей. Очевидно, что короткие или осмысленные пароли легко запоминаются человеком, но они гораздо проще для вскрытия. Использование длинных и бессмысленных паролей безусловно лучше с точки зрения криптостойкости, но человек обычно не может их запомнить и записывает на бумажке, которая потом либо теряется, либо попадает в руки злоумышленнику. Именно из того, что неискушенные пользователи обычно выбирают либо короткие, либо осмысленные пароли, существуют два метода их вскрытия: атака полным перебором и атака по словарю.

Защищенность пароля при его подборе зависит, в общем случае, от скорости проверки паролей и от размера полного множества возможных паролей, которое, в свою очередь, зависит от длины пароля и размера применяемого алфавита символов. Кроме того, на защищенность сильно влияет реализация парольной защиты.

В связи с резким ростом вычислительных мощностей атаки полным перебором имеют гораздо больше шансов на успех, чем раньше. Кроме того, активно используются распределенные вычисления, т.е. равномерное распределение задачи на большое количество машин, работающих параллельно. Это позволяет многократно сократить время взлома.

**2 Порядок выполнения работ**

**2.1.Проведение атаки перебором (bruteforce attack)**

1. Используя программу для вскрытия паролей произвести атаку на зашифрованный файл try\_me.rar (try\_me.arj, try\_me.zip – в зависимости от варианта). Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов. Время выполнения на компьютере класса Pentium примерно 3-4 минуты. На компьютере класса Pentium II – 50 секунд. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.
2. Выполнив пункт 1, сократить область перебора до фактически используемого (например если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

**2.2. Проведение атаки по словарю (dictionary attack)**

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

1. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.



 

