**Защита информации**

**Введение**

С конца 80-ых начала 90-ых годов проблемы связанные с защитой информации беспокоят как специалистов в области компьютерной безопасности так и многочисленных рядовых пользователей персональных компьютеров. Это связано с глубокими изменениями вносимыми компьютерной технологией в нашу жизнь. Изменился сам подход к понятию “информация”. Этот термин сейчас больше используется для обозначения специального товара который можно купить, продать, обменять на что-то другое и т.д. При этом стоимость подобного товара зачастую превосходит в десятки, а то и в сотни раз стоимость самой вычислительной техники, в рамках которой он функционирует.

Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий. Однако, большая часть пользователей не осознает, что постоянно рискует своей безопасностью и личными тайнами. И лишь немногие хоть каким либо образом защищают свои данные. Пользователи компьютеров регулярно оставляют полностью незащищенными даже такие данные как налоговая и банковская информация, деловая переписка и электронные таблицы. Проблемы значительно усложняются, когда вы начинаете работать или играть в сети так как хакеру намного легче в это время заполучить или уничтожить информацию, находящуюся на вашем компьютере.

**Кому нужны ваши данные?..**

Это зависит от того, кто вы такой и какими данными располагаете. Но также существует отдельный тип рода деятельности называемый хакером (англ. cracker – взломщик). Некоторые работают группами, некоторые отдельно. Их методы различны, но основной постоянный рабочий инструмент – программа-взломщик, делящаяся на два основных компонента: программа для доступа к удаленным компьютерам по телефонным сетям и словарь вероятных кодов и паролей. Задача программы-взломщика получить доступ к удаленному компьютеру с помощью подбора кодов и паролей до тех пор, пока комбинация не будет найдена; это обеспечит доступ к системе.

Фрикеры – это взломщики, которые специализируются на нападениях на телефонные системы. Телефонная сеть привлекает внимание большинства взломщиков так как она является на данный момент самой большой (глобальной) сетью на планете.

**Выбор системы защиты**

Запирать двери не очень удобно, однако без этого вы не выходите из дома. То же относится и к защите вашей компьютерной системы. Все, что от вас требуется – это готовность выполнять текущий контроль и совсем немного технических знаний.

Любая компьютерная система не является идеальной, то есть полностью не может обеспечить безопасность данных на вашем ПК. Чтобы на 100% защитить данные от попадания в чужие руки надо их уничтожить. А чтобы сохранить содержимое вашего компьютера в целости надо найти компромисс между важностью защищаемых вами данных и неудобствами связанными с использованием мер защиты. Далее я расскажу о ценных методах защиты данных, а также о том как уменьшить связанные с защитой данных неудобства. Дело в том, что каждый раз, когда повышается уровень защиты требуется более изощренный способ ее обхода. Выбор средства защиты должен основываться на обеспечении достаточной защищенности и в то же время не доставлять неудобств. Каждый пользователь должен произвести собственный анализ риска и решить какие меры защиты наиболее подходят вам в данном случае. Анализ риска для персональных компьютеров можно разделить на три класса: анализ автономных систем, то есть одного компьютера, анализ локальных систем и анализ систем удаленного доступа имеющих связь с глобальной сетью (напр. Internet).

**Использование паролей**

Идея использования паролей заключается в следующем: если кто-либо попробует обратиться к вашим данным или аппаратным средствам, то пароли должны создать собой массу неудобств. Чем сложнее будет угадать или “взломать” используемый вами пароль, тем в большей безопасности будут ваши данные. Длина пароля существенно влияет на уровень защиты. Личные номера на сегодняшний день являются одним из наименее безопасных паролей широкого использования (напр. Кредитные карты для кассовых аппаратов АТМ или телефонные карты). В личных номерах могут использоваться цифры от 0 до 9, то есть номер может иметь десять тысяч вариаций. Этого достаточно если речь идет о человеке стоящем возле АТМ и набирающего код наугад, но совсем не много если речь идет о компьютере использующем лобовой метод решения.

При “лобовом” нападении проверяются все возможные комбинации паролей до тех пор пока одна из них не сработает. При увеличении длины пароля сложность лобового нападения возрастает так как это займет больше времени. Конечно, многие банки используют не только четырехразрядный код (PIN), но и другие методы для повышения безопасности, например, видеокамеры и АТМ, которые блокируют карточки. При этом меры защиты в каждом банке сильно отличаются. Большинство банков также оказывают следующую услугу: вы можете позвонить в банк, набрать номер карточки и личный номер и узнать состояние текущего счета. Этот сценарий делает уязвимым ваш личный номер (PIN) – некто может засесть за телефон и пробовать разные варианты.

С телефонной карточкой возникает та же проблема. Сети дальней телефонной связи вроде AT & T, MCI, Sprint также используют личные четырехразрядные номера для опознания звонков. Предположим, вы потеряли бумажник… обычно первая реакция – сожаления о наличных ценностях, а лишь потом звонят в кредитные компании и сообщают о потере карточки. Это позволяет заблокировать платежи с ваших карточек. Однако большинство людей забывают, что телефонная карта тоже является кредитной и небольшую программу для взламывания ее PINа способен написать даже подросток. Например:

For i:=0 to 9999 do

DialAccess(i);

Функция DialAccess() – это небольшой отрывок кода. Он набирает телефон компании и последовательно (в данном случае от 0 до 9999) вводит номер карточки, используя i как PIN. Это классический пример лобового метода решения.

Таким образом, четырехразрядный пароль – ваш PIN – имеет всего 9999 возможных комбинаций. Однако большинство компьютерных паролей длиннее и кроме чисел 1-9 могу содержать символы. Четырехразрядный пароль, в котором используются числа и символы, расшифровать сложнее – он может содержать 1679616 уникальных комбинаций.

Вот формула для вычисления возможного количества комбинаций символов: c=xy, где с – число возможных комбинаций , x – количество различных символов используемых в каждой позиции пароля, y – число символов пароля. Например, при использовании PINа c=104. Также некоторые пароли чувствительны к регистру и включают в себя знаки препинания, так что число возможных комбинаций ещё возрастает.

Кроме паролей используемых для обращения к местной сети, Internet и т.д., у пользователей компьютеров есть ряд защитных мер включающих пароли. К ним относятся основанная на BIOS защита, требующая ввести пароль при загрузке компьютера, специальные защитные программы, блокирующие доступ к отдельным файлам, и защищенные паролем архивные ZIP-файлы.

**Простые меры защиты**

Есть кое какие несложные приемы для защиты ценной информации, которые используются уже много лет. Проблема в том, что все эти схемы легко обойдет хорошо осведомленный пользователь.

DOS и предшествующие операционные системы некоторое время сохраняют удаленные файлы, не уничтожая их полностью. При удалении просто редактируется FAT (File Allocation Table): запись имени файла объявляется недействительной, а сектора, где записан файл, - свободными. Это означает, что удаленные файлы можно восстановить с помощью некоторых широко распространенных утилит (нап. undelete).

Программы уничтожения полностью стирают файл, перезаписывая всю информацию о файле в FAT и сектора, где он находился.

Также можно надежно шифровать отдельные файлы и сообщения электронной почты используя правительственный стандарт шифрования DES. DES расшифровывается как Data Encryption Standart (стандарт шифрования данных). DES был разработан IBM по заказу FBI и CIA как программное обеспечение для шифрования. После разработки DES в 1977 году он был принят правительством USA. Программа DES for Windows, написанная Джеффом Зальцманом, является утилитой шифрования общего пользования.

**Защита электронной почты**

Подавляющее большинство электронной почты посылается через Internet или другие глобальные сети в виде простого текста, который можно прочесть. Закон о конфиденциальности электронных коммуникаций приравнивает вашу электронную почту к обычному телефонному звонку.

Вы должны понимать, что системные администраторы имеют все необходимые средства для чтения электронной почты на своей системе. Иногда им даже необходимо просматривать электронную почту, чтобы удостовериться, что система работает нормально.

Хакеры и любопытные отличаются тем, что владеют различными способами получения доступа к вашей почте, но обе эти категории не могут читать вашу почту, если она зашифрована. Если вам необходимо защитить секретную информацию используйте PGP (Pretty Good Privacy) для шифрования почты перед отправлением.

**Список литературы**

“Защита информации в персональных ЭВМ”, А.В. Спесивцев.

“Вычислительная техника и её применение”, В.В. Голубев.

“Безопасность компьютера”, Эд Тайли.