Защита собственной информации от несанкционированного доступа

Подготовила: Ученица МКОУ Перелешинская СОШ
Хатунцева А.П

"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

Несанкционированный доступ

- **Несанкционированный доступ –**чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.
- Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.

- Для успешной защиты своей информации пользователь должен иметь абсолютно ясное представление о возможных *путях несанкционированного доступа*. Перечислим основные типовые пути несанкционированного получения информации:

- · хищение носителей информации и производственных отходов;
- · копирование носителей информации с преодолением мер защиты;
- · маскировка под зарегистрированного пользователя;
- · мистификация (маскировка под запросы системы);
- · использование недостатков операционных систем и языков программирования;
- · использование программных закладок и программных блоков типа "троянский конь";
- · перехват электронных излучений;
- · перехват акустических излучений;
- · дистанционное фотографирование;
- · применение подслушивающих устройств;
- · злоумышленный вывод из строя механизмов защиты и т.д..

- Для защиты информации от несанкционированного доступа применяются:

1) организационные мероприятия;

2) технические средства;

3) программные средства;

4) шифрование.

Организационные мероприятия

- *Организационные мероприятия* включают в себя:
- · пропускной режим;
- · хранение носителей и устройств в сейфе (дискеты, монитор, клавиатура и т.д.);
- · ограничение доступа лиц в компьютерные помещения и т.д..

Технические средства

- *Технические средства* включают в себя:
- · фильтры, экраны на аппаратуру;
- · ключ для блокировки клавиатуры;
- · устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т. д.;
- · электронные ключи на микросхемах и т.д.

Программные средства

- *Программные средства* включают в себя:
- · парольный доступ – задание полномочий пользователя;
- · блокировка экрана и клавиатуры с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilites;
- · использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом и т.д.

Резервное копирование

- Плюсы резервного копирования:
- с помощью резервных копий можно восстановить данные, если они были повреждены или вообще удалены.
- резервные копии можно хранить компактно в сжатом виде в одном файле.

Минусы резервного копирования
- Оно не защищает данные от несанкционированного доступа.

Если же для нужных Вам данных не было сделано резервных копий и они были удалены, то есть вероятность, что их можно восстановить. для этого существуют спец. программы

носителях (дискеты, CD, DVD)

Плюсы:

- Доступ к этой информации будете иметь только Вы (если, конечно, не допускать, чтобы эти сменные носители попали в чужие руки)

Минусы:

- Сменные носители могут быть повреждены и можно потерять информацию, хотя возможность восстановить ее все-таки есть, если использовать приведенные здесь программы

Шифрование важных данных.

- *Шифрование*–это преобразование (кодирование) открытой информации в зашифрованную, не доступную для понимания посторонних. Шифрование применяется в первую очередь для передачи секретной информации по незащищенным каналам связи. Шифровать можно любую информацию — тексты, рисунки, звук, базы данных и т.д. Человечество применяет шифрование с того момента, как появилась секретная информация, которую нужно было скрыть от врагов. Первое известное науке шифрованное сообщение — египетский текст, в котором вместо принятых тогда иероглифов были использованы другие знаки. Методы шифрования и расшифровывания сообщения изучает наука ***криптология***, история которой насчитывает около четырех тысяч лет. Она состоит двух ветвей: криптографии и криптоанализа.

Криптография - кодирование информации с помощью какого-либо шифра. т.е превращение информации в нечто нераспознаваемое. В этом случае для получения доступа к информации нужен пароль, даже если сам способ шифрования известен и есть доступ к зашифрованной информации.

Стеганография - скрытие самого факта наличия информации. Существуют алгоритмы, к-рые прячут информацию в файлы-контейнеры формата bmp, wav и некоторых других.

Картинки и аудио файлы хорошо подходят для этих целей, т.к. они достаточно велики и в них можно спрятать определенное кол-во информации.

Файл-контейнер (картинка или звук со встроенными данными) практически не отличается от оригинала ни по размеру ни по внешнему виду/звучанию.

Ключ

Ключ — это параметр алгоритма шифрования (шифра), позволяющий выбрать одно конкретное преобразование из всех вариантов, предусмотренных алгоритмом. Знание ключа позволяет свободно зашифровывать и расшифровывать сообщения.

Все шифры (системы шифрования) делятся на две группы — симметричные и несимметричные (с открытым ключом). *Симметричный шифр* означает, что и для шифрования, и для расшифровывания сообщений используется один и тот же ключ. В системах с *открытым ключом* используются два ключа — открытый и закрытый, которые связаны друг с другом с помощью некоторых математических зависимостей. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптостойкость шифра

Криптостойкость шифра — это устойчивость шифра к расшифровке без знания ключа. Стойким считается алгоритм, который для успешного раскрытия требует от противника недостижимых вычислительных ресурсов, недостижимого объема перехваченных сообщений или такого времени, что по его истечении защищенная информация будет уже неактуальна.

Шифр Цезаря

Один из самых известных и самых древних шифров – шифр Цезаря. В этом шифре каждая буква заменяется на другую, расположенную в алфавите на заданное число позиций k вправо от нее. Алфавит замыкается в кольцо, так что последние символы заменяются на первые. Шифр Цезаря относится к *шифрам простой подстановки*, так как каждый символ исходного сообщения заменяется на другой символ из того же алфавита. Такие шифры легко раскрываются с помощью частотного анализа, потому что в каждом языке частоты встречаемости букв примерно постоянны для любого достаточно большого текста.

Шифр Виженера

Значительно сложнее сломать шифр Виженера, который стал естественным развитием шифра Цезаря. Для использования шифра Виженера используется ключевое слово, которое задает переменную величину сдвига. Шифр Виженера обладает значительно более высокой криптостойкостью, чем шифр Цезаря. Это значит, что его труднее раскрыть — подобрать нужное ключевое слово. Теоретически, если длина ключа равна длине сообщения, и каждый ключ используется только один раз, шифр Виженера взломать невозможно.

Нам огромные возможности дает интернет:
В образовании, развлечении и в работе,
Но надо помнить, что безопасности нет
И ваш компьютер и данные под угрозой!
Чтобы эти проблемы избежать,
Надо знать правила простые.
И чтоб себя и компьютер защищать
Вот правила самые основные:
Выбирай безопасные веб - страницы
Не переходи по ссылкам незнакомым.
Не разглашай информацию личную,
Защищай страницу надежным паролем.
Не отвечай на сообщения в сетях,
Которые приходят от незнакомых лиц.
Нельзя их и по e-mail отравлять
Быть может, что это мошенник или аферист!
Не скачивай странные программы
Не при каких обстоятельствах.
Чтоб не нанести себе и компьютеру рану,
Избегай всех неприятностей!