Сети ЭВМ и телекоммуникации

Компьютерная безопасность

Компьютерный вирус – программный код, встроенный в другую программу, или документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.

Основные типы компьютерных вирусов:

- программные вирусы;
- загрузочные вирусы;
- макровирусы.

Программные вирусы – это блоки программного кода, целенаправленно внедренные внутрь других прикладных программ. Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и / или в содержании других программ.

Компьютерная безопасность

Загрузочные вирусы - отличаются от программных методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей (гибких и жестких дисков). На включенном компьютере они могут временно располагаться в оперативной памяти.

Макровирусы – особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманды.

Компьютерная безопасность

Методы защиты от компьютерных вирусов.

Существует три рубежа защиты от компьютерных вирусов:

- Предотвращение поступления вирусов;
- Предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;
- Предотвращение разрушительных последствий, если все-таки атака произошла.

Существует три метода реализации защиты:

- Программные методы защиты;
- Аппаратные методы защиты;
- Организационные методы защиты.

Компьютерная безопасность

Основное средство защиты информации – *резервное копирование* наиболее ценных данных!!!

Защита информации в Интернете

Принципы защиты информации в Интернете опираются на определение информации «Информация – это совокупность данных и адекватных им методов».

Системы защиты сосредоточены на «методах». Их принцип действия основан на том, чтобы исключить или затруднить возможность подбора «адекватного» метода для преобразования данных в информацию.

Шифрование информации

1. Симметричное шифрование

Обычный подход – к документу применяется некий метод шифрования (ключ), после чего документ становится недоступен для чтения обычными средствами. Его может прочитать только тот, кто знает ключ (т.е. может применить адекватный метод). Аналогично происходит шифрование и ответного сообщения. Если в процессе обмена информацией для шифрования и чтения пользуются одним и тем же ключом, то такой криптографический процесс является ***симметричным.***

Проблема – перед обменом надо выполнить передачу ключа.

Шифрование информации

2. Несимметричное шифрование

Используется не один, а два ключа. Компания для работы с клиентом создает два ключа: один – ***открытый*** (публичный) ключ, а другой – ***закрытый*** (личный) ключ. На самом деле это две «половинки» одного целого ключа, связанные друг с другом.

Ключи устроены так, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой (не той, которой оно было закодировано).

Публичный ключ распространяется для широкого пользователя, закрытый (личный ключ) надежно хранится.

Ключ – это некая кодовая последовательность.

Проблема – можно реконструировать закрытый ключ.

Шифрование информации

Принцип достаточности защиты:

Он предполагает, что защита не абсолютна, и приемы ее снятия известны, но она все же достаточна для того, чтобы сделать это мероприятие целесообразным. При появлении иных средств, позволяющих-таки получить зашифрованную информацию в разумные сроки, изменяют принцип работы алгоритма, и проблема повторяется на более высоком уровне.

Область науки, посвященная исследованиям методов реконструкции закрытого ключа называется **криптоанализом**

Средняя продолжительность времени, необходимого для реконструкции закрытого ключа по его опубликованному открытому ключу, называется **криптостойкостью** алгоритма шифрования.

Понятие об электронной подписи

ЭЦП – документа позволяет получателю только удостовериться в истинности отправителя документа, но не проверить подлинность документа.

Создаются (с помощью специальной программы полученной от банка) два ключа: закрытый и публичный.

Публичный ключ передается банку. Если надо отправить поручение банку на операцию с расчетным счетом, оно кодируется публичным ключом банка, а своя подпись под ним кодируется собственным закрытым ключом.

Банк поступает наоборот. Он читает поручение с помощью своего закрытого ключа, а подпись – с помощью публичного ключа поручителя. Если подпись читаема, банк может быть уверен, что поручение отправили именно мы, и никто другой.