Лекция 9. Безопасная навигация в Интернете

- *9.1. Защита информации в Интернете*
- *9.2. Понятие об электронных сертификатах*
- *9.3. Компьютерные вирусы*
- *9.4. Методы защиты от компьютерных вирусов*
- *9.5. Средства антивирусной защиты*

Защита информации в Интернете

- Работая во Всемирной сети, следует помнить о том, что абсолютно все действия фиксируются и протоколируются специальными программными средствами и информация как о законных, так и о незаконных действиях обязательно где-то накапливается.
- Соответственно, системы защиты сосредоточены на втором компоненте информации - на методах. Их принцип действия основан на том, чтобы исключить или, по крайней мере, затруднить возможность подбора *адекватного* метода для преобразования данных в информацию.
- Одним из приемов такой защиты является *шифрование* данных.

Сертификация даты

- Сертификация даты выполняется при участии третьей, независимой стороны.
- Например, это может быть сервер организации, авторитет которой в данном вопросе признают оба партнера. В этом случае документ, зашифрованный открытым ключом партнера и снабженный своей электронной подписью, отправляется сначала на сервер сертифицирующей организации. Там он получает «приписку» с указанием точной даты и времени, зашифрованную закрытым ключом этой организации.
- Партнер декодирует содержание документа, электронную подпись отправителя и отметку о дате с помощью своих «половинок» ключей. Вся работа автоматизирована.

Сертификация Web-узлов

- Прежде чем выполнять платежи через Интернет или отправлять данные о своей кредитной карте кому-либо, следует проверить наличие действующего сертификата у получателя путем обращения в сертификационный центр.
- Это называется *сертификацией Web-узлов.*

Сертификация издателей

- Подтверждение того, что сервер, распространяющий программные продукты от имени известной фирмы, действительно уполномочен ею для этой деятельности, осуществляется путем *сертификации издателей.*
- Она организована аналогично сертификации Web-узлов.

Понятие компьютерного вируса

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

Типы компьютерных вирусов

- • программные вирусы;
- • загрузочные вирусы;
- • макровирусы.
- К компьютерным вирусам примыкают и так называемые *троянские кони (троянские программы, троянцы).*

Программные вирусы

- Программные вирусы - это блоки программного кода, целенаправленно внедренные внутрь других прикладных программ.
- При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода.
- Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ.

Как происходит заражение

- При обычном копировании зараженных файлов заражение компьютера произойти не может.
- В связи с этим все данные, принятые из Интернета, должны проходить обязательную проверку на безопасность, а если получены незатребованные данные из незнакомого источника, их следует уничтожать, не рассматривая.

Загрузочные вирусы

- Обычно заражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус. Так, например, при попытке загрузить компьютер с гибкого диска происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

Макровирусы

- Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых *макрокоманд.*
- В частности, к таким документам относятся документы текстового процессора Microsoft Word (они имеют расширение .DOC).
- Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

Три рубежа защиты от компьютерных вирусов

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

Три метода реализации защиты

- программные методы защиты;
- аппаратные методы защиты;
- организационные методы защиты.

Средства антивирусной защиты

- Основным средством защиты информации является резервное копирование наиболее ценных данных.
- Вспомогательными средствами защиты информации являются антивирусные программы и средства аппаратной защиты.

Создание образа жесткого диска на внешних носителях

- В случае выхода из строя данных в системных областях жесткого диска сохраненный «образ диска» может позволить восстановить если не все данные, то по крайней мере их большую часть.
- Это же средство может защитить от утраты данных при аппаратных сбоях и при неаккуратном форматировании жесткого диска.

Регулярное сканирование жестких дисков в поисках компьютерных вирусов

- Сканирование обычно выполняется автоматически при каждом включении компьютера и при размещении внешнего диска в считывающем устройстве.
- При сканировании следует иметь в виду, что антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящимися в базе данных.
- Если база данных устарела, а вирус является новым, сканирующая программа его не обнаружит.

Контроль за изменением размеров и других атрибутов файлов

- Поскольку некоторые компьютерные вирусы на этапе размножения изменяют параметры зараженных файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.

Контроль за обращениями к жесткому диску

- Поскольку наиболее опасные операции, связанные с работой компьютерных вирусов, так или иначе обращены на модификацию данных, записанных на жестком диске, антивирусные программы могут контролировать обращения к нему и предупреждать пользователя о подозрительной активности.