Борьба с компьютерными вирусами при работе на ПК

Компью́терный ви́рус - разновидность компьютерных программ, отличительной особенностью которой является способность к размножению.

Создание и распространение компьютерных вирусов и вредоносных программ преследуется в России согласно Уголовному Кодексу РФ (глава 28, статья 273).

Чем опасны вирусы:

- могут повредить или полностью уничтожить все файлы и данные;
- повредить или уничтожить операционную систему со всеми файлами в целом;
- блокировать работу отдельных устройств компьютера(мыши, флешки и др.).

Способы распространения вирусов:

- **флеш-накопители** (флешки) – цифровые фотоаппараты, карты памяти, цифровые видеокамеры, MP3-плееры, сотовые телефоны. Среди *содержимого* этих устройств сидит специальный вредный и опасный файл **autorun.inf, к**оторый запускается при открытии такого накопителя. *Флешки— основной источник заражения для компьютеров, не подключённых единой локальной сети или Интернету!*
- **Электронная почта** – основной канал распространения вирусов. Обычно вирусы маскируются под безобидные вложения: *картинки, документы, музыку, ссылки на сайты*. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если *открыть* такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из почтового ящика клиента для рассылки самого себя дальше.
- **Системы обмена мгновенными сообщениями**(ICQ).
- **Веб-страницы** сети Интернет – используются уязвимости программного обеспечения (ПО), установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.
- **Черви -** вид вирусов, которые проникают на компьютер-жертву без участия пользователя, используя так называемые «дыры» (уязвимости) в ПО операционных систем. Уязвимости — это ошибки и недоработки в ПО, а вирус-червь попадает в операционную системы и начинает действия по заражению других компьютеров через локальную сеть или Интернет (рассылки спама или различные атаки).

Симптомы вирусного заражения:

- замедление работы некоторых программ;
- увеличение размеров файлов (особенно выполняемых);
- появление не существовавших ранее «странных» файлов;
- уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы);
- внезапно возникающие разнообразные видео и звуковые эффекты;
- неустойчивая работа ПК;
- частые «самостоятельные» перезагрузки ПК.

От вирусов нужно использовать **комплексную** защиту:

1. **Общие средства защиты информации –** страховка от физической порчи дисков, неправильно работающих программ, ошибочных действий пользователей и прочее. К ним относятся:
   - *копирование информации* - создание резервных копий файлов, дисков, «эталонных» дисков с программными продуктами;
   - *разграничение доступа*.
2. **Профилактические меры,** позволяющие уменьшить вероятность заражения компьютерным вирусом.
3. **Специализированные программы** для защиты от вирусов.

Распространенные антивирусные программы:

- **«Лаборатория Касперского»** - российский лидер в области разработки систем антивирусной безопасности, предназначена для защиты от всех современных интернет-угроз: вирусов, хакерских атак, спама и др.
- **Avas**t – разработка чешской компании, предназначена для защиты от макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама.
- **Dr.Web**—российская разработка, предназначена для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, спама, фишинг-сообщений.
- **NOD32** — антивирусный пакет, выпускаемый словацкой фирмой. Комплексное антивирусное решение для защиты в реальном времени. NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, фишинг-атаки.
- **Rising Antivirus** 2009 – китайская разработка, защищает ваш компьютер против всех типов угроз — вирусов, троянов, червей, руткитов и других вредоносных программ.

Меры, позволяющие уменьшить вероятность заражения компьютера вирусом, а также свести к минимуму ущерб от заражения вирусом:

- ✔ Неплохо бы иметь и при необходимости обновлять архивные и эталонные копии используемых пакетов программ и данных. Перед архивацией данных целесообразно проверить их на наличие вируса.
- ✔ Целесообразно так же скопировать на CD служебную информацию вашего диска (FAT, загрузочные сектора).
- ✔ Не следует заниматься нелицензионным и нелегальным копированием программного обеспечения с других компьютеров!
- ✔ Все данные, поступающие извне, НАДО проверять на вирусы, особенно файлы из Интернета.
- ✔ На время обычной работы, не связанной с восстановлением компьютера, стоит отключить загрузку с дискет, дисков. Это предотвратит заражение загрузочным вирусом.
- ✔ Используйте программы – фильтры для раннего обнаружения вирусов.

Меры, позволяющие уменьшить вероятность заражения компьютера вирусом, а также свести к минимуму ущерб от заражения вирусом (продолжение):

- ✔ Периодически проверяйте диск антивирусными программами.
- ✔ Обновляйте базу антивирусных программ.
- ✔ Допускайте к компьютеру только доверенных пользователей.
- ✔ При работе с электронной почтой не открывайте письма от подозрительных адресатов.
- ✔ Используйте только лицензионный антивирус.
- ✔ Перед использованием внешних носителей (флешки, CD и др.) **проверяйте** их на наличие вирусов.

Заключение

Соблюдение профилактических мер предосторожностей при работе на компьютере - это единственный цивилизованный способ защиты от вирусов.

Если вирус все-таки проник на компьютер - это не повод для паники. Не стоит бояться компьютерных вирусов, все они лечатся. Но, нередко главной бедой при работе с ПК и Интернетом являются не вирусы и хакеры, а такое распространенное явление, как компьютерная безграмотность.

Благодарю за внимание

Презентацию подготовила преподаватель ГБОУ СПО «Баймакский сельскохозяйственный техникум»
Мусина Ж.М.