Борьба с компьютерными вирусами при работе на ПК

Компью́терный ви́рус – определенная группа компьютерных программ, ориентированная на выполнение на вычислительных устройствах действий, нежелательных для их пользователей. Негативные последствия их функционирования выражаются в порче данных на информационных носителях, нарушении нормальной работы устройств и установленных на них приложений, а также нейтрализации средств защиты конфиденциальных сведений.

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.
- **Microsoft Security Essentials**–разработка компании Microsoft, защищает ваш компьютер против основных 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 копии используемых данных на сетевые диски, а особо важные данные храните на съёмных носителях (флешки, CD и др.).
- ✔ Все данные, поступающие извне, НАДО проверять на вирусы, особенно файлы из Интернета.
- ✔ 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.
- ✔ Перед использованием внешних носителей (флешки, CD и др.) **проверяйте** их на наличие вирусов.

Правила работы с электронной почтой:

- ✔ При работе с электронной почтой не открывайте письма и не сохраняйте прикрепленные файлы от подозрительных адресатов.
- ✔ Даже если Вы ожидаете письмо с похожей информацией, желательно связаться с автором письма и уточнить, действительно ли он отправлял Вам именно это письмо и именно с таким вложенным файлом.
- ✔ Если у Вас есть хоть бы малейшие сомнения относительно письма и прикрепленных файлов - УДАЛЯЙТЕ ПИСЬМО!
- ✔ Если Вы не знаете, что предпринять - ПОЗВОНИТЕ В IT-ОТДЕЛ!

Пример заражения

- ✔ Вам приходит письмо от неизвестного (но может и от вполне известного реально существующего!) с вполне разумными темой письма (например, "Резюме", "Акт сверки", "Информация о задолженности" и т.д.), текстом письма и вложенным файлом (.zip, .rar, .cab, .**scr**, .doc, .exe)
- ✔ **Открыв прикрепленный файл ВЫ запускаете вирус**, который шифрует все ваши самые нужные и важные файлы.
- ✔ В папках могут появляться файлы с подобным названием *"КАК_РАСШИФРОВАТЬ_ФАЙЛЫ.txt."*.
- ✔ Следует помнить что на сегодняшний день не существует возможности расшифровать зашифрованные вирусом файлы, так что вся важная информация не расположенная на сетевых дисках (или архивированная на съёмный накопитель) будет потеряна.

Вместо заключения

Если есть подозрение на заражение вашего компьютера необходимо выполнить:

- ✔ Оповестить системного администратора
- ✔ Не работать с сетевыми ресурсами и не открывать никаких документов.
- ✔ Желательно отключить компьютер от сети или даже выключить его.