**Лекция 9**

**Проблемы, возникающие из-за вирусов и шпионских программ**

Сегодня никто не может чувствовать себя в полной безопасности. Вирусы становятся все вредоноснее, эпидемии - масштабнее, а финансовые потери растут. Угрозы информационной безопасности становятся всё более комплексными. Вирусы могут привести к серьезным сбоям в работе компьютера, привести к потере программ, уничтожить данные или стереть необходимую для работы компьютера информацию, записанную в системных областях памяти. Авторы вирусов, хакеры и спамеры постоянно изобретают новые способы, чтобы незаконно проникать на наши компьютеры, подчинять их себе и затем рассылать с них спам - предварительно не согласованные с получателем сообщения рекламного, коммерческого или агитационного характера. Количество вредоносных программ, известных на сегодняшний день, уже приближается к ста тысячам, появились десятки новых их типов и разновидностей - всё чаще смешанных, объединяющих все последние достижения "черной" компьютерной индустрии.

    Типы вредоносных программ

http://www.itaec.ru/images/e_punct_b.gif  Вирус.  
"Живет" и размножается внутри зараженной системы, присоединяясь к другим программам или документам (в этом случае вредоносный код называют макровирусом). Когда происходит исполнение программы, то одновременно исполняется и вирусный код. Распространяются вирусы путем переноса зараженной программы или документа на другой компьютер.

http://www.itaec.ru/images/e_punct_b.gif  Червь.  
В отличие от вируса является автономной программой и поэтому "живет", не присоединяясь к другому коду. Вносит изменения в ОС, чтобы исполняться при загрузке компьютера. Для распространения черви либо используют "дыры" в защите компьютеров, либо осуществляют какие-то обманные действия, вынуждающие пользователей запустить вредоносный код.

http://www.itaec.ru/images/e_punct_b.gif  Троянский конь.  
Подобно вирусу присоединяется к другим программам и совершает те или иные деструктивные действия. Чтобы распространяться, трояны "подделываются" под какие-либо полезные программы.

http://www.itaec.ru/images/e_punct_b.gif  Потайной вход.  
Открывает доступ к системе в обход нормальной процедуры аутентификации. Существуют два типа потайных входов. Первый работает как троян, второй - как червь.

http://www.itaec.ru/images/e_punct_b.gif  Программа-шпион.  
Собирает и отправляет информацию о пользователе - от адресов любимых сайтов (в лучшем случае) до номеров кредитных карт (в самом плохом). Работает и распространяется как троян.

Заметить, что компьютер заражен вирусом или на нем появилась чья-то шпионская программа, намного проще, чем, считают многие. Конечно, ничто не заменит хорошую антивирусную программу. Но перед тем, как принять решение проверить систему, стоит обратить внимание на сигналы, которые укажут на то, что проблема существует.

Когда обращаются с жалобами на некорректную работу системы, обычно хватает нескольких правильно сформулированных вопросов, для того чтобы определить виновного.

Не остается никаких сомнений, когда начинают описывать из неоткуда всплывающие окна, или внезапные изменения в настройках поисковика, или новые программы, о существовании которых их владелец даже не догадывается до тех пор, пока эти программы не заявляют о себе радостным предложением помощи в решении всех существующих проблем.

Большинство вирусов и шпионских программ (честно говоря, провести границу между двумя этими явлениями не всегда представляется возможным) обычно пытаются прикинутся частью операционной системы. Они копируют стиль обновлений операционной системы, всплывающих в нижнем правом углу экрана, они даже любезно предупреждают вас об опасности вирусной атаки на ваш компьютер. Не дайте себя обмануть, когда услужливо приглашают пройти по ссылке на какой-то незнакомый сайт и приобрести чудесную и способную решить все ваши проблемы антивирусную программу. Все это является частью коварного плана. Ясным знаком «вирусного» происхождения такого предложения так же является наличие в тексте орфографических и грамматических ошибок, а так же смысловые неточности и повторение одних и тех же слов.

Не раз встречались программы-подделки, которые полностью копировали внешний вид известного антивирусного программного обеспечения. Они внезапно появляются в списке автозагрузки и начинают засыпать владельца предложениями срочно установить обновления или загрузить якобы необходимые ему базы данных. Некоторые даже пытаются заставить заплатить за эти столь жизненно важные усовершенствования. Каждый клик мышкой по предложенным ссылкам позволяет вредоносным программам размножаться на вашем компьютере и усиливает натиск всплывающих окон.

Еще одним несомненным признаком того, что компьютер заражен, являются непонятным образом появляющиеся незнакомые ссылки в списке избранного и в программах автозагрузки. Любимые обои на рабочем столе вдруг заменяются приглашением на незнакомый веб-сайт, привычная домашняя страничка поисковика сменяется другой и отказывается возвращаться. Все это говорит о том, что система подверглась вирусной атаке, и теперь настройками вашего компьютера управляете не вы, а вирус.

Так же не следует оставлять без внимания внезапные изменения в процессе запуска системы, при введении пароля доступа, несанкционированные вами повторяющиеся перезагрузки, попытки системы без вашего участия подключиться к Интернету либо возникающие проблемы при загрузке сайтов, которые не указаны в списке вашей новой «домашней» странички.

Если вы уже столкнулись с чем-то из этого списка (или даже пока не столкнулись) вам обязательно нужно воспользоваться программой проверки системы на вирусы и вредоносные программы. В настоящее время существуют неплохие бесплатные антивирусные сервисы, которые позволят чувствовать себя увереннее на просторах Интернета и не потребуют много ресурсов.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

 Обдумайте возможность отказа от MS Windows и перехода на ОС семейства GNU/Linux или xBSD.

В этих операционных системах вопросам безопасности изначально уделялось намного больше внимания. Вредоносных программ, работающих под Linux или FreeBSD в настоящее время намного меньше, чем работающих под MS Windows.

Возможность отказа от MS Windows зависит от используемых Вами прикладных программ. Если Вам нужен только поиск информации в Internet и работа с электронной почтой -- проблем нет. Для очень многих задач есть прикладные программы под Linux, в ряде случаев они даже удобнее, чем аналоги под Windows. Однако c обработкой документов MS Office, играми и узкоспециализированным профессиональными приложениями могут возникнуть проблемы.

    1. Применяйте новейшие антивирусные программы.

Антивирусное программное обеспечение помогает защищать компьютер от известных вирусов, "червей", "троянцев" и других зловредных программ, от которых может произойти сбой в работе компьютера. Это очень серьезная проблема. Вирусы, "черви" и подобные им вредоносные программы могут предпринять злонамеренные действия, например, уничтожить файлы, предоставить посторонним доступ к личным сведениям, использовать компьютер для атаки на другие компьютеры.

Использование антивирусного программного обеспечения позволит проверить компьютер на наличие вирусов, предпринять различные профилактические меры. Однако нужно помнить, что однократного применения этих средств недостаточно. Необходимо постоянно пользоваться антивирусами, а кроме того, необходимо регулярно обновлять антивирусное программное обеспечение. Обычно обновления можно получать у поставщика антивирусных программ по подписке.

Старайтесь не открывать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами. Желательно также, чтобы при работе с новым программным обеспечением в памяти резидентно находился какой-либо антивирусный монитор. Если запускаемая программа заражена вирусом, то такой монитор поможет обнаружить вирус и остановить его распространение.

Следует обязательно включать антивирусные программы перед использованием электронной почты или Интернета. Крайне осторожно относитесь к программам и документам Word/Excel, которые получаете из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте их на наличие вирусов.

  2. Обновление программного обеспечения.

Обновление программного обеспечения позволяет решить большинство известных вопросов безопасности. Регулярно проверяйте наличие доступных обновлений для вашей операционной системы и другого используемого вами программного обеспечения на веб-узле поставщика данного программного продукта.

Обновление операционных систем семейства Windows.  
Существует два взаимодополняющих средства, которые применяются совместно и помогают своевременно обновлять программное обеспечение путем установки самых последних обновлений продуктов корпорации Майкрософт: Средства обновления Microsoft Windows® (Microsoft Windows® Update) и автоматическое обновление.

Windows Update - интерактивный веб-узел, с которого можно загружать и устанавливать обновления Windows, постоянно поддерживая на высоком уровне безопасность и производительность компьютера. Windows Update работает со следующими операционными системами:

|  |
| --- |
| http://www.itaec.ru/images/e_punct_b.gif   Microsoft Windows NT® Server 4.0 |
| http://www.itaec.ru/images/e_punct_b.gif  Windows Millennium Edition (Windows Me) |
| http://www.itaec.ru/images/e_punct_b.gif  Windows 2000 |
| http://www.itaec.ru/images/e_punct_b.gif  Windows XP |
| http://www.itaec.ru/images/e_punct_b.gif  Microsoft Windows Server™ 2003 |

Windows Update позволяет в любое время просматривать, выбирать и устанавливать самые последние улучшения, усовершенствования системы, обновления безопасности и драйверы для компьютера. Значок Windows Update обычно находится в меню "Пуск". Если значка Windows Update в меню нет, можно обратиться по адресу [http://windowsupdate.microsoft.com](http://windowsupdate.microsoft.com/) . Откройте веб-страницу и далее следуйте инструкциям.

Автоматическое обновление - часть службы корпорации Майкрософт, которая автоматически доставляет на компьютер важные обновления операционной системы Windows. Служба помогает решить проблемы, которые могут быть причиной уязвимости компьютера перед атаками сетевых "червей" и компьютерных вирусов. В связи с этим корпорация Майкрософт настоятельно рекомендует использовать службу автоматического обновления и устанавливать ее с возможностью планового автоматического обновления, как описано ниже. Кроме того, следует также периодически посещать узел [Windows Update](http://windowsupdate.microsoft.com/" \t "_blank) и обновлять компьютер дополнительными обновлениями и улучшениями.

Основное преимущество применения автоматического обновления заключается в том, что наиболее важные обновления безопасности компьютера загружаются и устанавливаются автоматически. Служба автоматического обновления находит обновления, наиболее подходящие для данного компьютера, автоматически загружает их и устанавливает в указанное время. Важно не забывать до наступления времени обновления сохранять копии данных, так как для завершения процедуры установки процесс автоматического обновления может потребовать перезагрузки компьютера.