Как защитить свой компьютер от вредоносных программ

Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

Рекомендации по обеспечению безопасной работы в Интернете:

- Установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы
- Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов
- Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять
- Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой
- Используйте сложные пароли, не связанные с вашей жизнью
- Расширение файла – это важно! Особую опасность могут представлять файлы со следующими расширениями: *ade, *adp, *bas, *bat; *chm, *cmd, *com, *cpl; *crt, *eml, *exe, *hlp; *hta, *inf, *ins, *isp; *jse, *lnk, *mdb, *mde; *msc, *msi, *msp, *mst; *pcd, *pif, *reg, *scr; *sct, *shs, *url, *vbs; *vbe, *wsf, *wsh, *wsc.