Комп'ютерна вірусологія

Профілактика зараження комп’ютера вірусами

[Дії при зараженні]

Якщо ви відмітили, що ваш комп'ютер "поводиться підозріло"

1.Відключите комп'ютер від інтернету і локальної мережі, якщо він до неї був підключений.
2.Якщо симптом зараження полягає в тому, що ви не можете завантажитися з жорсткого диска комп'ютера (комп'ютер видає помилку, коли ви його включаєте), спробуйте завантажитися в режимі захисту від збоїв або з диска аварійного завантаження Microsoft Windows, який ви створювали при установці операційної системи на комп'ютер.
3.Перш ніж робити які-небудь дії, збережете результати вашої роботи на зовнішній носій (дискету, CD-диск, флеш-карту і ін.).
4.Встановите Kaspersky Internet Security, якщо ви цього ще не зробили.
5.Обновіть антивірусні бази програми. Якщо це можливо, для їх отримання виходите в інтернет не з свого комп'ютера, а з незараженого.

Профілактика зараження комп’ютера

Ніякі найнадійніші і розумніші заходи не зможуть забезпечити стовідсотковий захист від комп'ютерних вірусів і троянських програм, але, виробивши для себе ряд правив, ви істотно понизите вірогідність вірусної атаки і ступінь можливого збитку.

Одним з основних методів боротьби з вірусами є, як і в медицині, своєчасна *профілактика*. Комп'ютерна профілактика складається з невеликої кількості правив, дотримання яких значно знижує вірогідність зараження вірусом і втрати яких-небудь даних.

Правило № 1:

застережіть ваш комп'ютер за допомогою антивірусних програм і програм безпечної роботи в інтернеті. Для цього:

- Невідкладно встановіть одну з антивірусних програм найбільш поширені з яких є Антивірус Касперського, Антивірус DRWEB, Антивірус NOD, Антивірус Symantec, Антивірус Аваст.
- Регулярно обновляйте антивірусні бази, що входять до складу програми. Оновлення можна проводити кілька разів в день при виникненні вірусних епідемій - в таких ситуаціях сигнатури погроз на серверах оновлень Лабораторії Касперського оновлюються негайно.
- Задайте Лабораторії Касперського, що рекомендуються експертами, параметри захисту вашого комп'ютера. Постійний захист починає діяти відразу після включення комп'ютера і утрудняє вірусам проникнення на комп'ютер.
- Задайте Лабораторії Касперського, що рекомендуються експертами, параметри для повної перевірки комп'ютера і заплануйте її виконання не рідше одного разу на тиждень. Якщо ви не встановили компонент Анти-хакер, рекомендується зробити це, щоб захистити комп'ютер при роботі в інтернеті.

Правило № 2:

будьте обережні при записі нових даних на комп'ютер:

- Перевіряйте на відсутність вірусів всі наявні носії (дискети, CD-диски, флеш-карти і ін.) перед їх використанням.
- Обережно поводьтеся з поштовими повідомленнями. Не запускайте ніяких файлів, що прийшли поштою, якщо ви не упевнені, що вони дійсно повинні були прийти до вас, навіть якщо вони відправлені вашими знайомими.
- Уважно відноситеся до інформації, що отримується з інтернету. Якщо з якого-небудь веб-сайту вам пропонується встановити нову програму, звернете увагу на наявність у неї сертифікату безпеки.
- Якщо ви копіюєте з інтернету або локальної мережі виконуваний файл, обов'язково перевірте його за допомогою Kaspersky Internet Security.
- Уважно відносьтесь до вибору відвідуваних вами інтернет-ресурсів. Деякі з сайтів заражені небезпечними скрипт-вірусами або інтернет-черв'яками.

Правило № 3:

зменшіть ризик неприємних наслідків можливого зараження:

- Своєчасно робіть резервне копіювання даних. У разі втрати даних система достатньо швидко може бути відновлена за наявності резервних копій. Дистрибутивні диски, дискети, флеш-карти і інші носії з програмним забезпеченням і цінною інформацією повинні зберігатися в надійному місці.
- Обов'язково створіть диск аварійного відновлення з якого при необхідності можна буде завантажитися, використовуючи "чисту" операційну систему.
- *Користуйтеся сервісом Windows Update* і регулярно встановлюйте оновлення операційної системи Microsoft Windows.

Дякую за увагу☺