



**Профілактика комп’ютерних вірусів**



Загальна інформація щодо профілактики

Ми живемо на стику двох тисячоліть, коли людство вступило в епоху нової науково-технічної революції.

До кінця двадцятого століття люди опанували багатьма таємницями перетворення речовини і енергії і зуміли використовувати ці знання для поліпшення свого життя. Але окрім речовини і енергії в житті людини величезну роль грає ще одна складова – інформація. Це найрізноманітніші відомості, повідомлення, вісті, знання, уміння.

В середині нашого сторіччя з'явилися спеціальні пристрої – комп'ютери, орієнтовані на зберігання і перетворення інформації і відбулася комп'ютерна революція.

Сьогодні масове застосування персональних комп'ютерів, на жаль, виявилося пов'язаним з появою програм-вірусів, що самовідтворюються, перешкоджають нормальній роботі комп'ютера, руйнують файлову структуру дисків і що завдають збитку інформації, що зберігається в комп'ютері.

Не дивлячись на прийняті в багатьох країнах закони про боротьбу з комп'ютерними злочинами і розробку спеціальних програмних засобів захисту від вірусів, кількість нових програмних вірусів постійно росте. Це вимагає від користувача персонального комп'ютера знань про природу вірусів, способи зараження вірусами і захисту від них.

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. Нижче перераховані основні правила безпеки, виконання яких дозволить вам уникати вірусних



Як боротися із вірусами

Кожного з нас цікавить така інформація, як правила боротьби з вірусами

Правило перше

Вкрай обережно ставтеся до програм і документів Word/Excel, які отримуєте з глобальних мереж. Перед тим, як запустити файл на виконання або відкрити документ/таблицю, обов'язково перевірте їх на наявність вірусів. Використовуйте спеціалізовані антивіруси для перевірки всіх файлів, що приходять по електронній пошті (і по Internet в цілому).
 Правило друге - захист локальних мереж

Для зменшення ризику заразити файл на сервері адміністраторам мереж слід активно використовувати стандартні можливості захисту мережі обмеження прав користувачів; установку атрибутів «тільки на читання» або навіть «тільки на запуск» для всіх виконуваних файлів (на жаль, це не завжди виявляється можливим) і т.д. Використовуйте спеціалізовані антивіруси, перевіряльники «на льоту» файли, до яких йде звернення. Якщо це з якої-небудь причини неможливо, регулярно перевіряйте сервер звичайними антивірусними програмами.

Правило третє.

 Краще купувати дистрибутивні копії програмного забезпечення у офіційних продавців, ніж безкоштовно або майже безкоштовно копіювати їх з інших джерел або купувати піратські копії. При цьому значно знижується ймовірність зараження, хоча відомі випадки купівлі інфікованих дистрибутивів. Як наслідок з цього правила випливає необхідність зберігання дистрибутивних копій програмного забезпечення (у тому числі копій операційної системи), причому копії бажано зберігати на захищених від записи дискетах.

 Правило четверте

Намагайтеся не запускати неперевірені файли, в тому числі отримані з комп'ютерної мережі. Бажано використовувати тільки програми, отримані з надійних джерел. Перед запуском нових програм обов'язково перевірте їх одним або декількома антивірусами

Не забувайте що, можна привести масу фактів, які свідчать про те, що загроза інформаційному ресурсу зростає з кожним днем, піддаючи в паніку відповідальних осіб в банках, на підприємствах і в компаніях у всьому світі. І загроза ця виходить від комп'ютерних вірусів, які спотворюють або знищують життєво важливу, цінну інформацію, що може привести не тільки до фінансових втрат, але і до людських жертв.





Більше можна дізнатися тут:

<http://ua.textreferat.com/referat-7822.html>

<http://www.unicyb.kiev.ua/~boiko/it/ref/Rubinets_referat.htm>

<http://www.crime-research.ru/articles/Kripco0204/>

Підготувала

Студентка групи М-12

Цибульська Тетяна