

***“Комп’ютерні віруси і антивіруси”***

# 1. Прояв комп'ютерних вірусів

Комп'ютерні віруси –— комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера

 При зараження комп'ютера вірусом дуже важливо своєчасно його знайти. І тому слід ознайомитися з основними ознаками появи вірусів:

· мерехтіння екрана.

· повільна робота комп'ютера.

· поява на екрані непередбачуваного повідомлення.

· блокування введення з клавіатури.

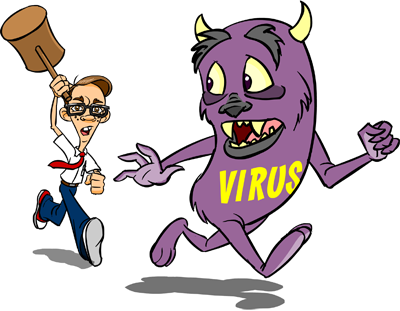
· зміна розмірів файла, дати створення програм.

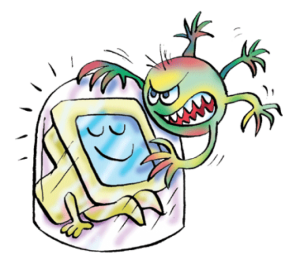
· значне збільшення файлів на диску.

· часті зависання і збої у роботі комп'ютера.

· знищення файлів чи часткова руйнація.

· блокування запису на жорсткий диск.

Особливо небезпечним і для користувача є така дія вірусу, як форматування жорсткого диска, що може спричинити до швидкої втрати всієї що зберігається там інформації. Оскільки від проникнення вірусу не застрахований жоден користувач, можна скоротити можливі наслідки від присутності на комп'ютері вірусу. І тому необхідно дотримуватися деяких правил:

· Кожен свій носій, коли він «побував» на іншому комп'ютері, слід перевірити будь-якою антивірусною програмою. Програми такі,що можуть не, лише знайти вірус, а й «вилікувати» носій.

· Аналогічні перевірки необхідно влаштовувати для файлів, отриманих через мережу.

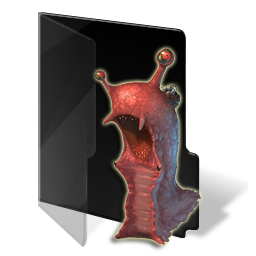
· Антивірусні програми необхідно періодично оновлювати, оскільки вони швидко старіють.

· Працюючи з електронною поштою не відкривати файли якщо тема листи і саме лист порожні, видаляти всі підозрілі файли.

· Не слід займатися неліцензійним і нелегальним копіюванням програмного забезпечення з інших комп'ютерів.

# 2. Методи захисту від комп'ютерних вірусів

Хоч би яким не був би вірус, користувачеві треба зазначити основні засоби захисту від комп'ютерних вірусів. Для захисту від вірусів можна використовувати:

· спільні кошти захисту, які корисні, і як страховка від фізичного псування дисків, неправильно працюючих програм чи хибних дій користувача;

· профілактичних заходів, дозволяють зменшити ймовірність зараження вірусом;

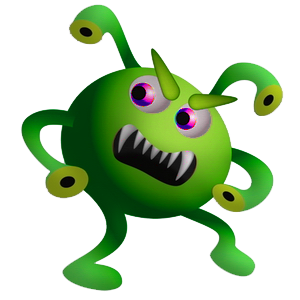
· спеціалізовані програми захисту від вірусів.

Загальні засоби захисту інформації мають дві основи різновиду:

· копіювання інформації – створення копій файлів і системних областей дисків;

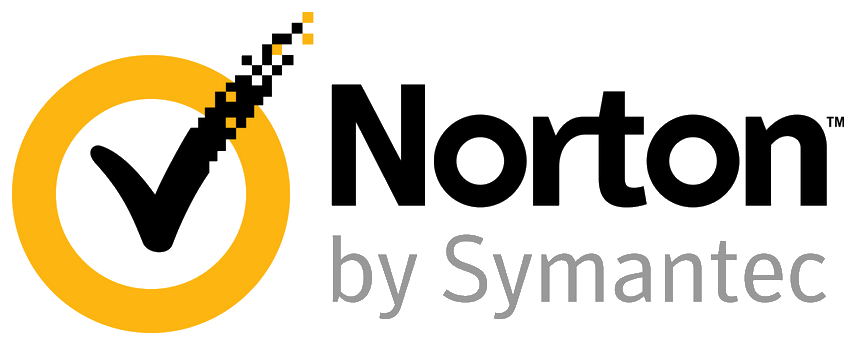
· розмежування доступу запобігає несанкціоноване використання інформації, захисту від змін програм, тож даних вірусами, неправильно які працюють з програмами.

Попри те що, спільні кошти захисту дуже важливі захисту від вірусів, проте їх недостатньо. Необхідно застосування спеціалізовані програми захисту від вірусів. Ці програми можна розділити на кілька видів: детектори, доктора, ревізори, фільтри, вакцини чииммунізатори.

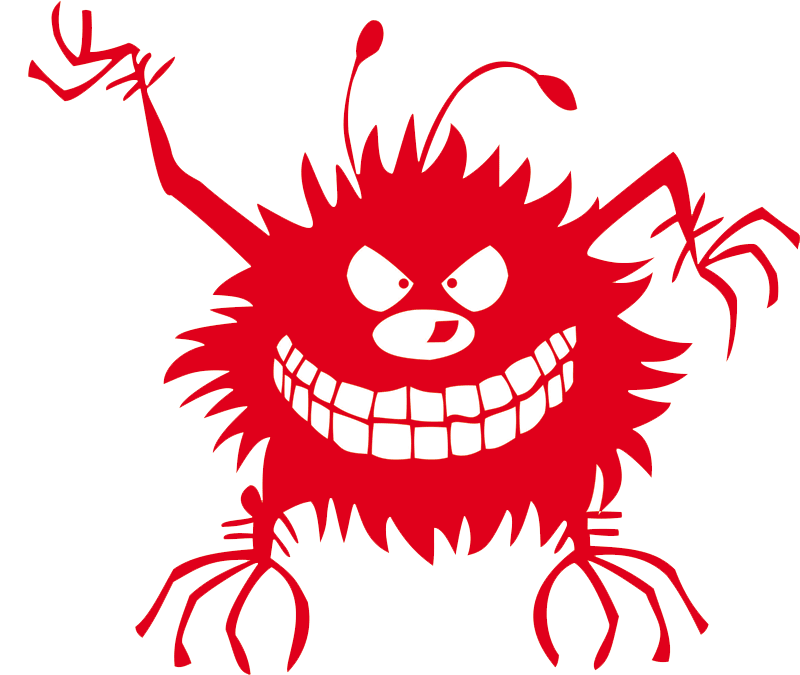
Програми – детектори дозволяють знайти файли, заражені вірусіами. При виявленні, в якомусь файлі на екран виводиться відповідне повідомлення. Багато детектори мають режими лікування чи знищення заражених файлів. Недоліком таких програм і те, що можуть виявляти ті віруси, які відомі розробникам таких програм.

Програми – доктора (фаги) як знаходять заражені вірусами файли, а й «лікують» їх, тобто. видаляють з файла тіло програми вірусу, повертаючи файли у початковий стан.

полифаги, призначені на допомогу пошуку і знищення великої кількості вірусів. Найвідоміші їхAidstest,Doctor Web, .

Програми – ревізори – це програми, які аналізують поточний стан файлів і системних областей диска і порівнюють його з туристичною інформацією, збереженої до цього часу одному з файлів даних ревізора. Порівняння станів зазвичай виробляють відразу після завантаження ОС. У цьому перевіряється довжина файлів, їх час створення та інші параметри. Виявлені зміни виводяться на екран. Аналізуючи повідомлення програми – ревізора, користувач може вирішити, чим викликані зміни. Широко поширена програмаAdinf.

Програми – фільтри – це резидентні програми, які сповіщають користувача при спробах будь-якої програми записатися на диск чи відформатувати його, також оповіщає про інші підозрілі дії. До переваг програмних засобів можна віднести універсальність стосовно, як до відомим, і невідомим вірусам. До вад – часту видачу запитів за проведення будь-якої операції

Програми – вакцини – церезидентські програми,які передбачають зараження файлів. Вакцини застосовують, якщо відсутні програми – доктора. Вакцинація можлива тільки в відоми х вірусів.

# 3. Антивірусні програми

>Антивірусна програма – частина програмного забезпечення, що встановлюється на комп'ютер, щоб шукати на дисках й у вхідних файлах комп'ютерні віруси й видаляти їх для виявлення. Програми виявляють віруси пропонуючи вилікувати файли, а при неможливості видалити. Бажано, щоб антивірусна програма виявляла будь-який вірус, причому з максимально високою ймовірністю.

Антивірусні програми залежно від розробника застосовують різні способи виявлення вірусів. Та більшість переглядає файли чи пам'ять комп'ютера, аби виявити присутність відомого вірусу, дізнаючись його за характерною частини коду.

Можливість отримати старий вірус порівняно невелика, але щодня з'являються нові віруси. Задля підтримки ефективності антивірусної програми рекомендується оновлювати антивірусні програми чи його бази даних про віруси. При виборі антивірусної програми необхідно враховувати як відсоток виявлення вірусів, а й виявляти нові віруси, кількість вірусів у антивірусної базі, частоту її відновлення, наявність додаткових функцій.

Нині серйозний антивірус мусить уміти розпізнавати щонайменше 25000 вірусів. Чимало їх ми вже припинила своє існування. Існує безліч антивірусних програм. Розглянемо найвідоміші їх.

>AIDSTEST

У нашій країні, як було зазначено вище, особливої популярності придбали антивірусні програми, поєднують у собі функції детекторів та докторів конкретних. Найвідомішою є програмаAIDSTESTД.Н. Лозинського. Україна має на кожномуIBM-совместимом персональному комп'ютері є одне з версій програмних засобів. Один із останніх версія виявляє більш 8000 вірусів.

>Aidstest для свого нормально функціонувати вимагає, щоб у пам'яті буврезидентних антивірусів, блокуючих запис в програмні файли, тому вони мають вивантажити, або, вказавши опцію вивантаження самоїрезидентной програмі, або скористатися відповідної утилітою.

Після запускуAidstest перевіряє себе оперативну пам'ять на наявність відомих йому вірусів і знешкоджує їх. У цьомупарализуются лише функції вірусу, пов'язані з розмноженням, інші побічні ефекти можуть залишатися. Програма по закінченні знешкодження вірусу у пам'яті видає запит про перезавантаженні. Слід обов'язково наслідувати цієї поради, якщо оператор ПЕОМ перестав бути системним програмістом, які займаються вивченням властивостей вірусів. До чого слід перезавантажитися кнопкоюRESET, бо за «теплою перезавантаженні» деякі віруси можуть зберігатися. До того ж, краще запустити автомобіль іAidstest ззащищенной від записи дискети, бо за запуску з зараженого диска вірус може записатись у пам'ять резидентом і перешкоджати лікуванню.

>Aidstest тестує своє тіло на наявність відомих вірусів, і навіть по спотворень у своїй коді судить про своє зараження невідомим вірусом. У цьому можливі випадки удаваної тривоги, наприклад при стискуванні антивірусуупаковщиком. Програма немає графічного інтерфейсу, і режими її задаються з допомогою ключів. Вказавши шлях, можна перевірити не весь диск, а окремий підкаталог.

Як показало практика, найоптимальніший режим для щоденної роботи задається ключами /g (перевірка всіх файлів, Не тільки з розширеннямEXE,COM,SYS) і />s (повільна перевірка). Збільшення часу при таких опціях мало відчутно, зате можливість виявлення значно вище.

**Успіхів вам**



Підготував:

студент групи Ф-11

Гой Віталій