

**УДК 631.356.22**

**Андрій Огородник, Людмила Гончар**

Тернопільський національний економічний університет, Україна

## **МЕТОДИ ТА ПРОГРАМНІ ЗАСОБИ ДЛЯ ПОРІВНЯЛЬНОГО АНАЛІЗУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

**Andrey Ogorodnik, Lyudmyla Gonchar**

### **METHODS AND PROGRAMMATIC FACILITIES ARE FOR COMPARATIVE ANALYSIS OF SYSTEMS OF PRIV**

Надійний захист від комп'ютерних вірусів може бути забезпечений системою антивірусного захисту, що складається з трьох антивірусних бар'єрів і передбачає встановлення антивірусного програмного забезпечення на активних елементах інформаційних систем, що мають доступ до можливих джерел комп'ютерних вірусів.

Перший бар'єр системи антивірусного захисту – захист при роботі з Internet. На сервері електронної пошти Internet встановлюється антивірусна програма, яка в режимі реального часу перевіряє листи електронної пошти, HTML(Web)-сторінки, Java-аплети і вилучає з них комп'ютерні віруси. В разі виявлення в листах електронної пошти користувача комп'ютерних вірусів, йому, відправнику та черговому адміністратору ЛОМ та черговому адміністратору антивірусного захисту інформації надсилається попереджувальний електронний лист з інформацією про результати лікування комп'ютерних вірусів.

Інформація про появу та лікування або вилучення комп'ютерних вірусів із листів електронної пошти заноситься у файл протоколу антивірусної програми, який автоматично надсилається адміністратору антивірусного захисту.

Другий бар'єр системи антивірусного захисту – захист серверів. Антивірусні програми встановлюються на сервери (файлові, поштові, баз даних, Web), які працюють із файлами таких типів, що можуть бути заражені комп'ютерними вірусами. Антивірусна програма повинна перевіряти файли під час створення, запису та прийому/передачі файлу. При відсутності такого режиму роботи антивірусна програма серверів автоматично, раз на добу (або частіше), повинна проводити антивірусну перевірку всіх файлів сервера.

Третій бар'єр системи антивірусного захисту – захист комп'ютерів користувачів. Антивірусні програми встановлюються на всі комп'ютери користувачів за винятком технологічних комп'ютерів, які не працюють із файлами, що можуть бути заражені комп'ютерними вірусами.

На комп'ютери користувачів, які працюють із файлами, що отримані з можливих джерел комп'ютерних вірусів, встановлюється антивірусний монітор, який в режимі реального часу перевіряє файли, із якими працює користувач, та оперативно блокує спроби комп'ютерних вірусів проникнути на комп'ютер користувача.

Антивірусні програми комп'ютерів користувачів, що не мають підключення до ЛОМ, працюють автономно. При отриманні файлів оновлень антивірусних програм адміністратори антивірусного захисту організацій та установ встановлюють їх на комп'ютери користувачів. Користувачі запускають отримані модулі оновлення на виконання. При виконанні модулі оновлення автоматично знаходять і оновлюють антивірусні програми без запитів до користувачів.

Система антивірусного захисту передбачає автоматизоване управління процесами встановлення, оновлення, конфігурування, пошуку та лікування комп'ютерних вірусів на комп'ютерах, на яких установлені антивірусні програми, за винятком тих, що не потребують антивірусного захисту.