Прилуцька Н.С., Яценко О.І.,
асистенти кафедри прикладної математики та інформатики,
Житомирський державний університет імені Івана Франка

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Розвиток новий інформаційних технологій і загальна комп'ютеризація призвели до того, що інформаційна безпека не тільки стає обов'язковою, а й є однією з основних характеристик інформаційної системи (ІС).

В умовах, коли комп'ютерні системи стають основою безпеки цілих країн, а бази даних – головним капіталом багатьох компаній, антивірусний захист встає поруч із питаннями загальної

економічної безпеки як країни вцілому так і окремих установ та організацій. Особливо ця проблема актуальна для установ та підприємств, що мають справу з конфіденційними даними про клієнтів. Крадіжка, знищення, перекручення інформації, збій і відмова комп'ютерних систем – ті проблеми, які несуть з собою віруси і вірусоподібні програми.

Загрози інформаційній безпеці умовно можна поділити на два види: загрози, що носять випадковий характер (їх джерелом можуть бути ненавмисні помилки в програмному забезпеченні, вихід з ладу апаратних засобів, неправильні дії користувачів) та загрози навмисні, які, на відміну від випадкових, переслідують мету навмисного нанесення пошкодження інформаційній системі, викрадення даних, нанесення збитків фізичним чи юридичним особам.

Найбільш поширеним навмисним способом ушкодження ІС є використанням так званих інформаційних інфекцій (шкідливих програм). До них відносяться: логічні бомби, троянські коні, віруси, черви, та ін. Кожен рік шкідливі комп'ютерні програми наносять мільярдні збитки економіці. На сьогоднішній день найбільшої шкоди завдали віруси MyDoom (2003 р., 38 млрд. збитків), SoBig (2003 р., $37,1 млрд. збитків), «Я люблю тебя» (2000 рік, 15 млрд. збитків) [1].

Тому великі організації відносяться до проблеми захисту інформаційних ресурсів дуже серйозно. Але проблема полягає в тому, що, незважаючи на наявність антивірусного програмного забезпечення, загроза вірусних атак, як і раніше, нікуди не зникає. Однією з причин цього є встановлення розрізненого антивірусного програмного забезпечення (ПЗ) та відсутність технічної підтримки встановленого ПЗ. В результаті антивірусні програми не оновлюються вчасно, і, як результат, не виявляють нові шкідливі програми [2].

Для виконання завдання захисту ІС, в загальному випадку, антивірусний захист повинен будуватися за ієрархічним принципом:

1-й рівень ієрархії – служби загальнокорпоративного рівня;

2-й рівень ієрархії – служби підрозділів або філій;

3-й рівень ієрархії – служба кінцевих користувачів.

Служби всіх рівнів поєднуються в єдину обчислювальну систему за допомогою локальної обчислювальної мережі роботу якої забезпечує спеціальний персонал, а також передбачені засоби централізованого адміністрування.

Антивірусна система повинна надавати такі види сервісів на

–загальнокорпоративному рівні:

1. постійне оновлення антивірусних баз;
2. управління поширенням антивірусного ПЗ;
3. управляння оновленням антивірусних баз;

4. контроль за роботою антивірусної системи.

–на рівні підрозділів:

1. оновлення антивірусних баз кінцевих користувачів;
2. оновлення антивірусного ПЗ кінцевих користувачів.

–на рівні кінцевих користувачів: автоматичний антивірусний захист даних користувача

Програмно-технічні компоненти системи антивірусного захисту повинні забезпечувати формування інтегрованого обчислювального середовища, що задовольняє наступним загальним принципам створення автоматизованих систем:

- система в цілому повинна бути здатною функціонувати незалежно від функціонування окремих її вузлів і володіти засобами відновлення після відмови;

- система антивірусного захисту повинна формуватися з урахуванням того, що кількість об’єктів захисту з часом зростає;

- система повинна формуватись з урахуванням можливості поповнення і оновлення функцій і складу без порушення функціонування обчислювального середовища;

- антивірусна система має бути сумісною з максимальною кількістю мережевих ресурсів;

- система має бути однорідною, тобто всі її компоненти повинні бути стандартними промисловими системами та мати широку сферу застосування.

- система антивірусного захисту не повинна порушувати логіку роботи інших використовуваних додатків;

- система повинна забезпечувати можливість повернутися до використання попередньої версії антивірусних баз;

- система повинна функціонувати в режимі функціонування об’єкта на якому вона встановлена та забезпечувати оповіщення адміністратора системи при збоях в роботі [2].

Крім того, система повинна забезпечувати регулярне оновлення використовуваної антивірусної бази, містити в собі механізми пошуку раніше невідомих загроз, як найбільш поширених і небезпечних в даний час.

Список використаної літератури

1. 10 наиболее разорительных компьютерных вирусов [Электронный ресурс] – Режим доступа : URL : http://www.vestifinance.ru/articles/16340/.

2. Организация системы антивирусной защиты банковских информационных систем [Электронный ресурс] – Режим доступа : URL : http://citforum.ru/security/virus/bank/.