7. БЕЗПЕКА ТА ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ

Безпека мережі (Network security) – заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в нормальні дії або намагань руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Сьогодні всі шкідливі програми називають вірусами, хоча це не зовсім коректно. Це скоріше певна „торгова марка". Лабораторією Касперського створена досить велика вірусна енциклопедія, яку можна проглянути на сторінці http://www.viruslist.com/index.html.

Оскільки в сферу уваги інформаційної безпеки всі частіше попадають більш серйозні речі, ніж звичайні віруси, фахівці з комп'ютерного захисту ввели термін malware – "зловмисне програмне забезпечення", яким позначають будь-який код, що наносить шкоду комп'ютеру чи його власнику. Для опору посяганням на приватну інформацію користувача, необхідна глибока і добре продумана система оборони, що складає з декількох бар'єрів між зловмисним програмним забезпеченням і системою.

Захисні технології по рівню розвитку не обганяють інформаційні технології, а йдуть слідом за ними. Доки немає загрози, ніхто не буде витрачати зусилля та кошти для захисту.

При вирішенні проблем безпеки потрібно оцінити важливість того, що ви намагаєтесь захистити для вас і для потенційних крадіїв. Очевидно, що цінність інформації на комп'ютері звичайного користувача, сервері банка чи Центральної виборчої комісії різна.

Основні загрози безпеки: відкриття конфіденційних даних, втрата чи пошкодження даних, зміна даних, відмова в обслуговуванні, помилки програмного забезпечення та відмова від зобов'язань.

По даним звіту журналу Computer Economics, що вийшов в січні 2006 року, фінансові збитки від вірусів в світі (тільки витрати на відновлення інфраструктури) в 2005 році склали приблизно 14 млрд. доларів, а по оцінці ФБР сукупні збитки в цьому ж році склали 63 млрд. доларів.

7.1. Історія розвитку зловмисних програм

Прообразом сучасних вірусів можна вважати програму „Дарвін", яка з'явилась ще в 1962 році. Саме тоді інженери американської компанії Bell Telephone Laboratories В.А. Виготський, Г.Д. Макілрой та Р. Морріс створили гру, що символізувала ідею виживання і розвитку програмних кодів, створюваних гравцями. Гра передбачала наявність в пам'яті обчислювальної машини так званого супервізора, який визначав правила і порядок боротьби між собою програм супротивників, створюваних гравцями. Програми мали функції дослідження простору, розмноження та знищення. Сенс гри був у видаленні всіх копій програм супротивника і захваті „поля битви".

Вже в 70-х рр. були зареєстровані перші справжні віруси, здатні до роз-

множення, і навіть отримали власні імена: великий комп'ютер Univac 1108 захворів вірусом Pervading Animal, а на комп'ютерах сімейства IBM-360/370 – Christmas tree. На початку 80-х кількість активних вірусів налічувала сотні, а при появі персональних комп'ютерів – тисячі.

Термін „комп'ютерний вірус" з'явився в 1984 році, його вперше використав в своїй доповіді по інформаційній безпеці співробітник Лехійського університету США Ф. Коен.

На території бувшого Радянського Союзу віруси з'явились вже в 90-х роках, але спочатку не отримали широкого розповсюдження.

Перша серйозна епідемія, яка привернула до проблеми вірусів увагу всієї світової спільноти, сталася в 1996 році. Її викликав макровірус Cap, якай розповсюджувався в документах Microsoft Word. Йому вдалося паралізувати роботу десятків компаній по всьому світу.

Електронна пошта і Internet стали ідеальним середовищем для розповсюдження шкідливих кодів. Якщо в 1999 році лише 50% вірусів потрапляли в комп'ютер через електронну пошту, то сьогодні це приблизно 95-98%. Доля вірусів, що передаються через дискети зараз незначна.

Фахівці з інформаційної безпеки відмічають зміну напрямку у розвитку шкідливих програм. Спочатку віруси писались для задоволення, а основна мета сьогодні – отримання прибутку.

По даним Євгенія Касперського, за 2005р. приблизно вдвічі збільшилась кількість троянський програм і приблизно на стільки ж збільшився розмір антивірусних баз. Тільки 5% всіх шкідливих програм було написане для задоволення, 75% – для отримання грошей, 20% – для обох цілей.

7.2. Огляд шкідливих програм

Умовно і найбільш грубо віруси можна розділити на програмні і скриптові. Перші представляють собою окремі, автономні саморозмножуючі програми, часто з деструктивною дією. „Скриптові" – не являються окремими програмами, а є набором інструкції для якоїсь з популярних програм (Internet Explorer, Microsoft Office і т.п.). Загальна риса всіх скрипт-вірусів – прив'язка до однієї з вбудованих мов програмування.

В залежності від середовища існування розрізняють наступні типи вірусів:

- Файлові – впроваджуються в програмні, системні та файли драйверів. Починають розмножуватися при кожному запуску програми на виконання.
- Завантажувальні – заражають завантажувальний сектор диску (Boot сектор) або сектор, що містить програму системного завантажувача вінчестера (Master Boot Record). Вірус заміщає собою завантажувальну програму, відразу потрапляє в оперативну пам'ять і після завантаження операційної системи здійснює керування комп'ютером.
- Файлово-завантажувальні – можуть вноситися як в програми, так і в завантажувальні сектор. Це так звані поліморфні чи стелс-віруси.

- Макровіруси – вносяться в файли додатків, які мають свою мову програмування. Це документи Word, Excel та ін.
- Мережні – розповсюджуються по комп'ютерній мережі.

По способу розповсюдження програми можна розділити на: комп'ютерні віруси, мережні хробаки та троянські програми.

7.2.1. Комп'ютерні віруси

Комп'ютерний вірус – це невелика по розмірам програма, яка може самостійно розмножуватися, "приписуючи" себе до інших програм, тим самим заражаючи їх, а також виконувати різні небажані дії на комп'ютері.

Програму, в якій знаходиться вірус називається "*зараженою*". Коли така програма починає працювати, то спочатку управління отримує вірус. Вірус знаходить і "заражує" інші програми, а також виконує інші шкідливі дії (наприклад, пошкоджує файли, чи таблицю розміщення файлів на диску, "засмічує" оперативну пам'ять і т.д.). Доки на комп'ютері заражені відносно мало програм, наявність вірусу може бути практично непомітною. Але, через деякий час на комп'ютері появляються небажані події. Наприклад: деякі програми перестають працювати, чи починають працювати неправильно; на екран виводяться сторонні повідомлення, символи і т.д.; робота на комп'ютері суттєво сповільнюється; деякі файли виявляються пошкодженими і т.п.

Ці типи вірусів фактично втрачають свої позиції (в 2005р. займали приблизно 5%) і віддають першість більш фінансово-орієнтованим.

7.2.2. Троянські програми

Троянські програми, чи просто троянці – шкідливі програми, які самі не розповсюджуються, а маскуючись під популярну програму, спонукають користувачів переписати та встановити шкідника на власний комп'ютер самостійно.

По виконуваним діям троянські програми можна умовно розділити на

- утиліти несанкціонованого віддаленого адміністрування – дозволяють зловмиснику віддалено управляти зараженим комп'ютером;
- утиліти для проведення DDoS-атак (Distributed Denial of Service – атаки типу „відмова в обслуговуванні) – вибирають інформаційні ресурси жертви, в результаті чого система перестає виконувати свої функції і стає недоступною;
- шпигунські програми – таємно наглядають за діями користувача і записують в свій журнал цікаві для зловмисника дані;
- рекламні програми – дозволяють вбудувати рекламні об'яви в часто використовувані додатки;
- програми подзвону – намагаються за допомогою модему і телефонної лінії додзвонитися до платного серверу і заставити користувача заплатити послуги;
- сервери розсилки спаму – дають можливість перетворити чужий ПК в сервер розсилки спаму;

- багатокомпонентні троянці-завантажувачі – переписують з Internet і встановлюють в систему інші шкідливі коди чи додаткові компоненти

Розрізняють троянські програми, які постійно забезпечують доступ до зараженого комп'ютера, тримаючи на ньому відкритий порт транспортного протоколу та програми, які не тримають відкритих портів. Останні пересилають зловмиснику певну інформацію, наприклад паролі або копії текстів, що набираються з клавіатури.

Ріст кількості щомісячно знайдених нових модифікацій троянських програм за перші шість місяців 2006 року склав 9%.

7.2.3. Мережні хробаки

Мережні хробаки не змінюють файли на дисках, а розповсюджуються в комп'ютерній мережі, впроваджуються в операційну систему комп'ютера, знаходять адреси інших комп'ютерів і розсилають по цим адресам свої копії, використовуючи різне середовище розповсюдження.

Віруси-хробаки мають манери справжніх хакерів, находячи діри в обороні підключених до мережі комп'ютерів і проникаючи в беззахисні порти.

Internet-хробаки розповсюджуються по Internet, LAN-хробаки – по локальній мережі, IRC-хробаки – через чати.

Автором першого „хробака" вважають Роберта Моріса, сина провідного фахівця по комп'ютерній безпеці. Його програмка почала гуляти по мережі Internet 2 листопада 1988 року, заразивши 6000 комп'ютерів. На допиті в ФБР Моріс Р. обґрунтовував свої дії перевіркою систем безпеки, і оскільки не було нанесено великої шкоди (якщо не рахувати паралізованої роботи мережі і витрат на очистку комп'ютерів), серйозного покарання не отримав.

А в 2004 році його „колега" 19-літній Джері Парсон – автор однієї з версій хробака Blaster – отримав 3 роки в'язниці і декілька мільйонів доларів штрафу.

Сьогодні жертвами хробаків є десятки мільйонів комп'ютерів. А такі монстри, як Blaster, Sasser чи Sober мають десятки видів модифікацій і паралізують роботи цілих мереж. Як правило, вони відносно нешкідливі для даних (не рахуючи постійні перезавантаження комп'ютера, які викликає Blaster), але їх „переміщення" по мережі генерує масу зайвого трафіку, займаючи канали зв'язку.

7.3. Технології інформаційної безпеки

Методи захисту від комп'ютерних вірусів та втрати інформації:

1. Загальні засоби захисту інформації, які потрібні не тільки для захисту від вірусів, а як страховка від фізичного пошкодження дисків, неправильно працюючих програм чи помилкових дій користувача. Є два різновиди таких засобів:
   - копіювання інформації – створення копій файлів і системних областей дисків;
   - розподіл доступу – запобігає несанкціонованому використанню інформації.

2. Криптографічний захист конфіденційних даних.
3. Профілактичні заходи, що дозволяють зменшити вірогідність зараження.
4. Спеціалізоване програмне та апаратне забезпечення.

7.3.1. Захист операційних систем

Одна з самих потужних атак макровірусів була зареєстрована в березні 1999 року, коли вірус Melissa за декілька годин розповсюдився по всьому світі. Саме його поява спонукала Microsoft оснастити програми Microsoft Office захистом від запуску макросів. При відкритті будь-якого документа, що містить вбудовані макроси, на екрані з'являється попередження (рис. 7.1) і запит на відкриття файлу з макросами. До речі, якщо в параметрах програми вказаний високий рівень захисту, то незважаючи на згоду відкриття, макроси все одно блокуються.

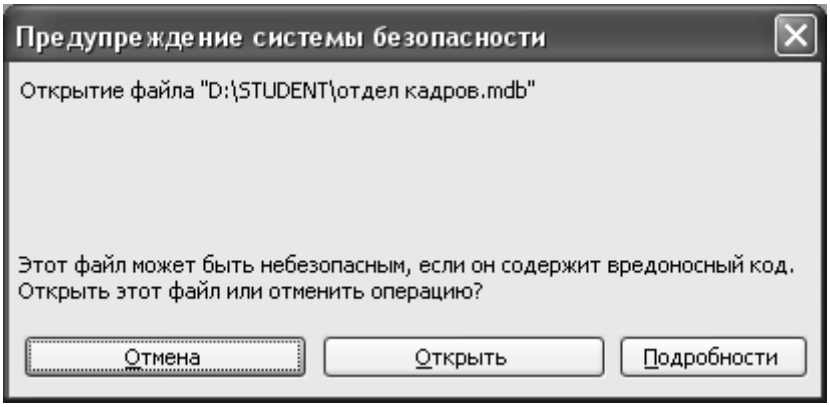

Рис. 7.1. Попередження про наявність макрокоманд в файлах.

Часто виникає питання, яким же чином вірус може потрапити в комп'ютер? Наприклад, вірус Blaster може перезавантажити комп'ютер, через мережу, навіть не проникаючи в нього.

Протокол TCP, який є основним для сучасної мережі, передбачає використання 65536 (2^{16}) портів. Крім того, можуть використовуватись інші протоколи, наприклад UDP, в асортименті якого знаходиться така ж кількість. Перші 100 портів (0-99) відносяться до категорії стандартних – їх використання жорстко регламентується і назавжди закріплені за певним службами, наступні 100-1024 називають „широко використовуваними" і пропонують трохи менше повноважень своїм клієнтам. Інші, приблизно 60000 – віддаються стороннім програмам, і не завжди надійно захищені.

В ідеальному варіантів відкритими для використання можуть бути лише ті порти, які зарезервовані за певними відомими системі програмами, інші „двері" повинні бути надійно заблоковані. Але на практиці, в системі захисту Windows (як інших операційних систем) є багато „дірок", які дозволяють зловмиснику отримати доступ до інформації через „недозволений" канал. Наприклад, Blaster, атакує комп'ютер через порт 135 чи 139.

Крім того, існують спеціальні програми для сканування портів, за допомогою яких можна знайти вхід практично в будь-який комп'ютер.

Розробники систем „латають" ці „дірки" спеціальними програмами, які

часто просто називають „латками”, а взагалі це оновлення для використовуваної версії операційної системи. Для цього досить зайти на сайт Windows Update (http://windowsupdate.microsoft.com), чи клацнути по значку Windows Update в меню Сервис програми Internet Explorer.

Крім того, практично всі сучасні системи дозволяють створювати різні профілі користувачів та надавати їм певні права доступу до програмного та апаратного забезпечення. Причому, деякі функції регулюються додатковим програмним забезпеченням. Наприклад, Адміністратор безпеки (рис. 7.2)

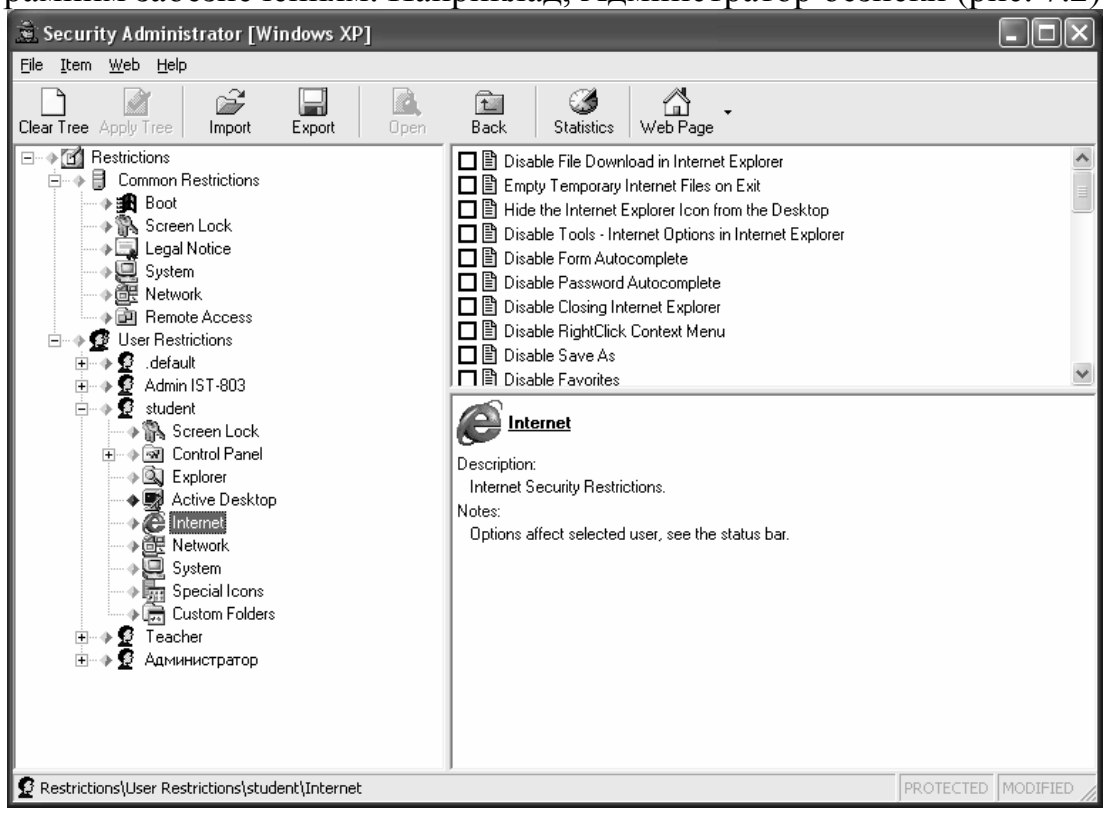

Рис. 7.2. Адміністратор безпеки

7.3.2. Налагодження параметрів безпеки в браузері Internet Explorer

Налагодження системи мережної безпеки складається із трьох пунктів, дістатися до яких можна таким шляхом: меню **Сервис-> Свойства обозревателя.** У цьому діалоговому вікні нашу увагу зосередимо на закладках **Безопасность, Конфиденциально** та **Дополнительно**.

1. Вибираємо закладку **Безопасность.** Вказуємо на верхній панелі зону **Интернет** і на нижній панелі натискаємо кнопку **Другой**. Ці маніпуляції надають змогу дістатися до параметрів (рис. 7.3-7.4), які керують виконанням активних кодів, вбудованих у HTML-сторінки. По кожному з парметрів є три можливих варіанти: Запретить, Предлагать та Разрешить. Перший варіант – відключить всі запропоновані елементи, другий – потребує постійних уточнень користувача для практично всіх дій, третій – для ризикових людей.

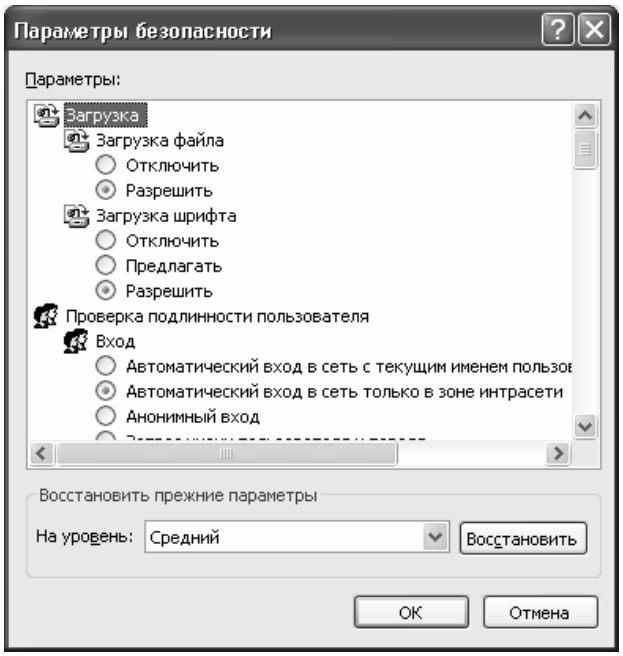

Рис. 7.3. Настроювання параметрів завантаження

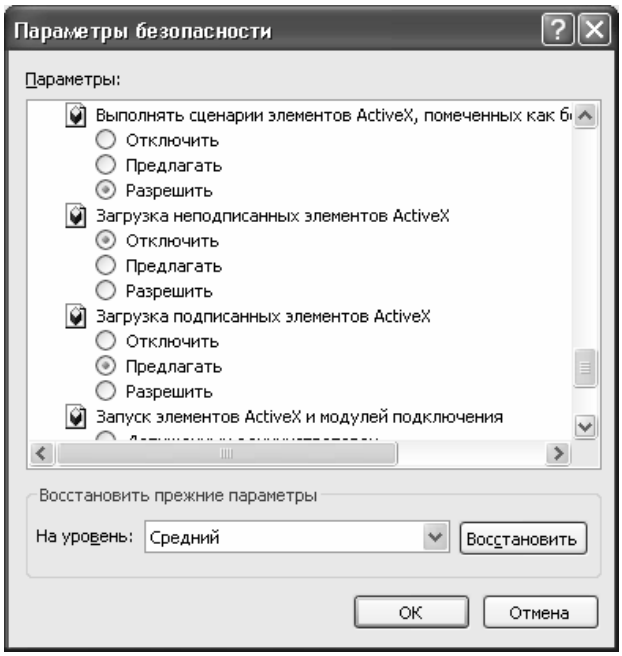

Рис. 7.4. Настроювання завантаження активних елементів сторінок

2. Вкладка **Конфиденциальность** використовується для настройки рівня мережної анонімності при прийомі *cookies* (мітки, які залишають на комп'ютері користувача деякі сайти Internet, призначені для ідентифікації користувача при повторному вході) – від повного їх блокування до прийому від будь-якого Web-сайта.

На вкладці **Дополнительно** (рис. 7.5) слід звернути увагу на дві групи параметрів – **Обзор** та **Безопасность**.

Група **Обзор** може стати в нагоді при встановлення параметрів відображення елементів на сторінці, тобто при пришвидшення завантаження, можна відмовитись від малюнків, анімаційних блоків, звуку і т.п. Але, треба відмітити, що на банерну рекламу, як правило, ці настроювання не діють.

Натисніть кнопку двічі **ОК**, і вважатимемо налагодження безпеки у броузері закінченим.

При роботі з системами електронної комерції, часто канали

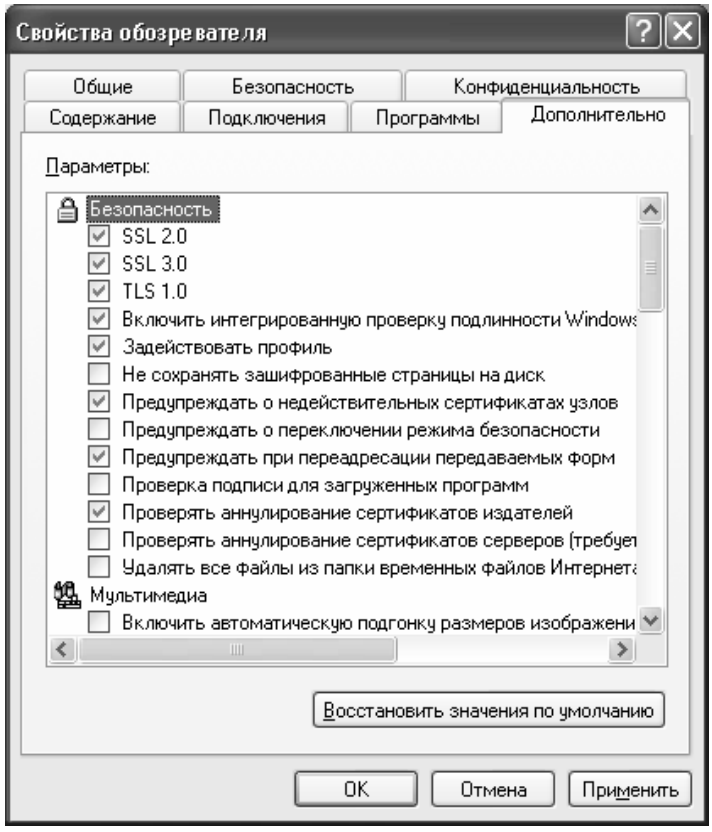

Рис. 7.5. Настроювання додаткових параметрів безпеки

зв’язку захищаються додатковим програмним забезпеченням. В цьому випадку на екран виводиться відповідне повідомлення (рис. 7.6). При виході з безпечної зони на екрані з’являється відповідне попередження (рис. 7.7).

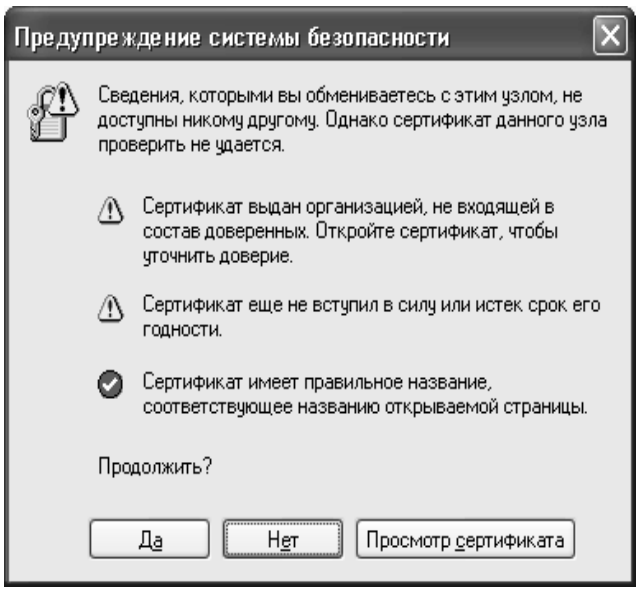

Рис. 7.6. Попередження системи безпеки

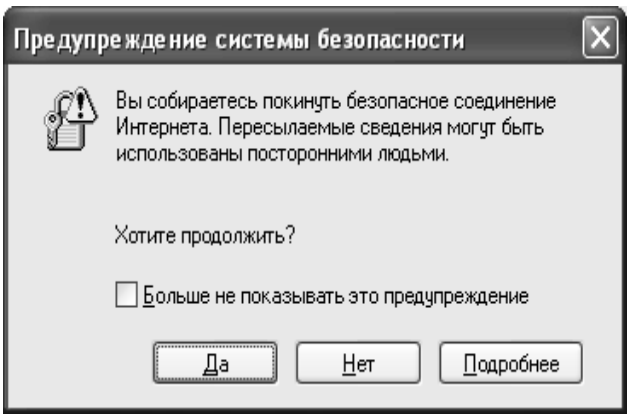

Рис. 7.7. Попередження про вихід з безпечної зони

7.3.3. Антивіруси

Однією з перших захисних технологій, до сих популярних на ринку, є антивірусний захист, що з’явився в середині 80-х років. Для захисту від вірусів розробляються спеціальні антивірусні програми, що дозволяють виявляти віруси, лікувати заражені файли і диски, запобігати підозрілим діям. Всі сучасні антивіруси оснащені механізмом автоматичного оновлення антивірусних баз даних через Internet. По даним лабораторії Касперського середній час виходу оновлення для антивірусної програми зараз складає десь 1 годину 22 хвилини. Більш того, якщо епідемія небезпечна, то urgent-оновлення випускається приблизно за 30 хвилин. Найпопулярнішими в Україні і країнах СНД є такі антивіруси:

- Антивірус Касперського;
- Антивірус Doctor Web;
- Panda Antivirus;
- Norton Antivirus;
- McAfee VirusScan.

У кожної з цих програм є свої переваги і недоліки. Кожна з них заслуговує на увагу споживачів. І, що важливіше, кожен з перелічених вище антивірусів може забезпечити ефективний захист вашого ПК.

Пакет AVP (AntiViral Toolkit Pro)

Мабуть самий популярний і потужний пакет, створений в Росії в лабораторії Є. Касперського. Антивірус AVP (AntiVirus Program) відноситься до поліфагів, у процесі роботи перевіряє оперативну пам'ять, файли, в тому числі архівні,

на гнучких, локальних, мережних і CD-ROM дисках, а також системні структури даних, такі як завантажувальний сектор, таблицю розділів і т.д. Програма має евристичний аналізатор, котрий, за твердженнями розробників антивірусу здатний знаходити майже 80% усіх вірусів. Здійснює пошук і вилучення найрізноманітніших вірусів, у тому числі: поліморфних, або вірусів, що самошифруються; стелс-вірусів, або вірусів-невидимок; нових вірусів для Windows; макровірусів, що заражають документи Word і таблиці Excel.

Крім того, програма AVP здійснює контроль файлових операцій у системі у фоновому режимі, виявляє вірус до моменту реального зараження системи, а також визначає невідомі віруси за допомогою евристичного модуля.

Для перевірки на наявність вірусів диску чи дискети потрібно:

Завантажити програму *Пуск → Программы → AntiViral Toolkit Pro → AVP Сканер.*

В діалоговому вікні (рис. 7. 8) задати параметри сканування:

- на вкладці **Область**(1) – виділити диски, які потрібно перевірити;
- на вкладці **Объекты**(2) – виділити об’єкти перевірки (пам’ять, сектори, файли, упаковані файли);
- на вкладці **Действие** (3) зазначити, що саме повинна робити програма з інфікованими об’єктами (*Только отчет,Запрос на лечение, Лечить без запроса* або *Удалять без запроса*);
- натиснути кнопку **Пуск**(4).

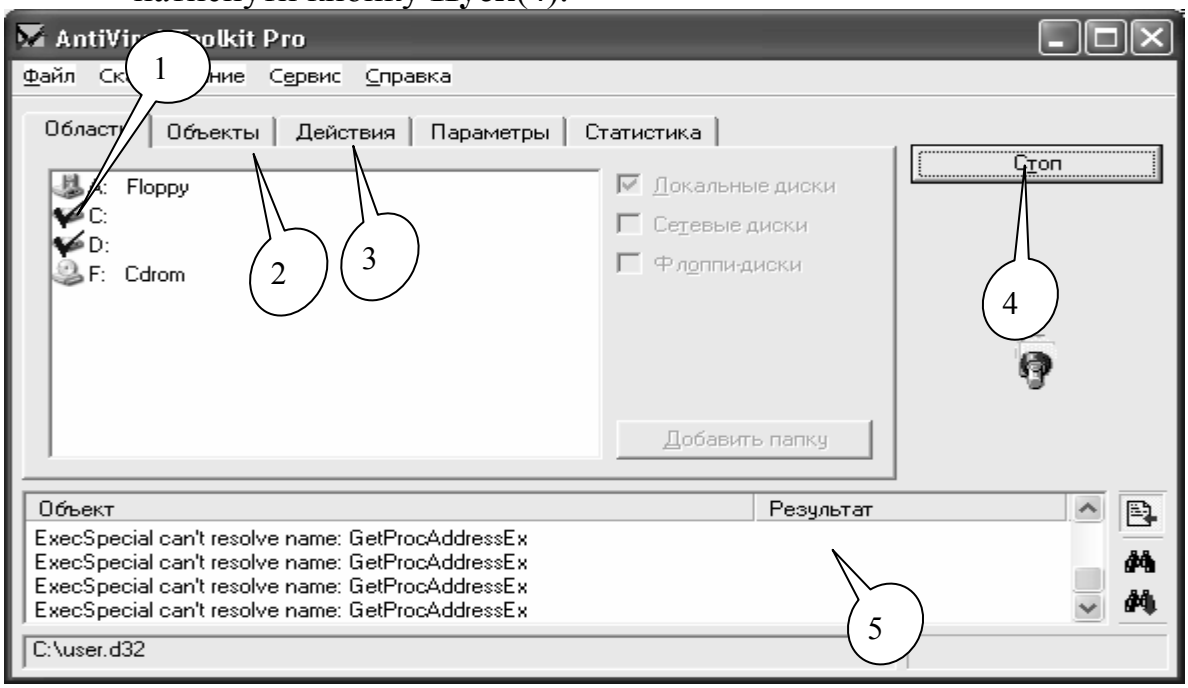

Рис. 7.8. Настроювання параметрів сканування

Після зазначених дій почнеться процес сканування. Якщо з об’єктами, що перевіряються все гаразд, по завершені перевірки під кнопкою *Пуск* з’явиться зелений напис ОК із галочкою, а зона перегляду буде порожньою (5). Якщо ж під час перевірки будуть виявлені віруси, то інформація про них (ім’я зараженого файлу і назва вірусу) буде виведена в зону перегляду.

Для перевірки на вірус окремого файлу потрібно викликати для нього контекстове меню і задати сканування.

Потрібно пам’ятати, що антивірусна програма визначає тільки “відомі” віруси, тому антивірусні бази потрібно обновлювати. В деяких випадках, коли присутня файлова помилка, чи незнайомий вірус, видається інформація про підозру на вірус.

До складу пакету входить також модуль *AVP Monitor*, який завантажується при включенні комп’ютера, постійно міститься в пам’яті комп’ютера і контролює звернення до файлів (рис. 7.9) та завантажувальних секторів. Перед тим як дозволити доступ до об’єкта, модуль перевіряє його на наявність вірусу. Якщо в об’єкті буде виявлений вірус, монітор запропонує вилікувати заражений об’єкт, видалити об’єкт або заблокувати доступ до нього. Тобто *AVP монітор* дозволяє виявити і виділити вірус до моменту його реального проникнення до системи.

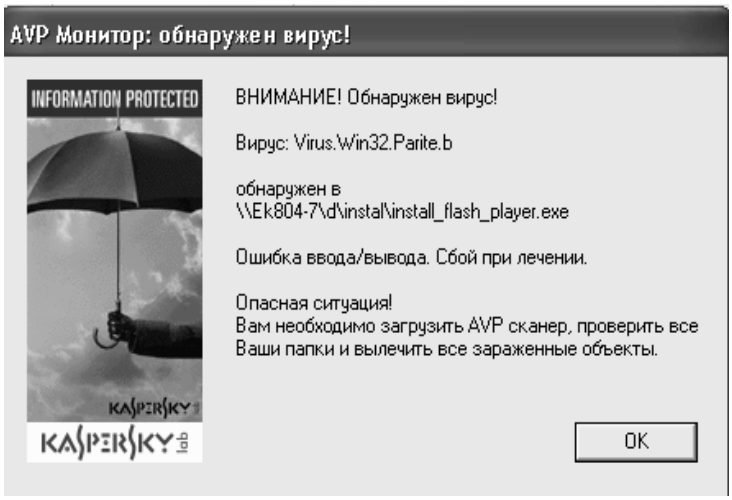

Рис. 7.9. Ідентифікація вірусу AVP монітором

Остання версія системи має досить цікавий інтерфейс (рис. 7.10), чотири основних компонента захисту, незалежні один від одного, які можуть бути відключені або видалені.

Рис. 7.10. Новий антивірус Касперського

Перший відповідає за безпеку файлів на комп’ютері, другий – за відправлення і приймання поштових повідомлень, третій – за роботу в Interneti, четвертий компонент забезпечує, так званий проактивний захист.

Компонентами проактивного захисту є перевірка VBA-макросів, контроль за змінами в системному реєстрі, перевірка цілісності додатків і аналіз їх активності.

Департамент спеціальних телекомунікаційних систем та захисту інформації (ДСТСЗІ) СБ України 6.08.01 підтвердив відповідність "Антивіруса Касперського" нормативним документам, що регламентують вимоги до засобів технічного захисту інформації. Крім того, експерти ДСТСЗІ дозволили використовувати цю програму при побудові систем антивірусного захисту у складі комплексних систем захисту інформації

До недоліків системи можна віднести серйозні вимоги до ресурсів комп'ютера.

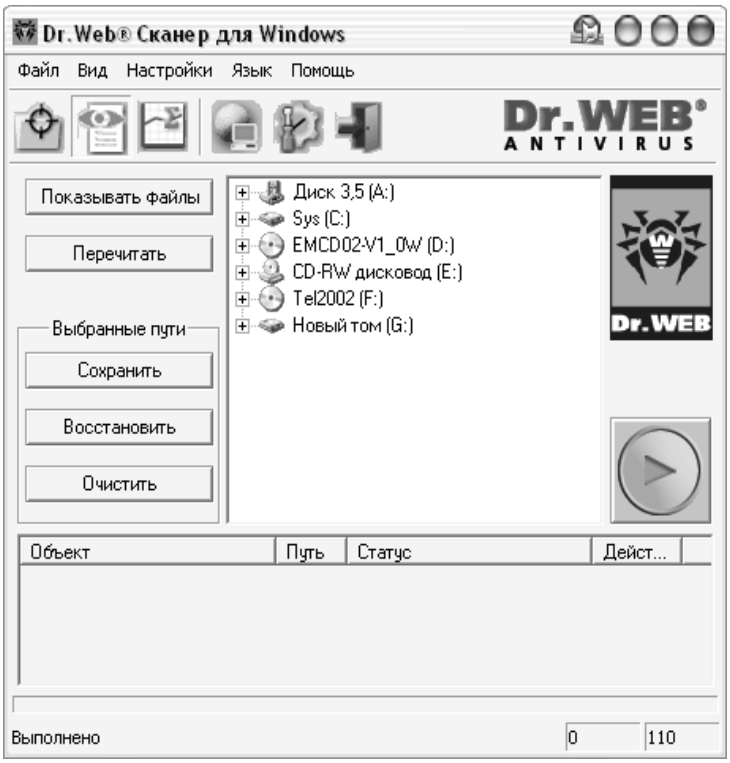

Рис. 7.11. Антивірус DrWeb

DRWEB

Один з кращих антивірусів (рис. 7.11) із сильним алгоритмом знаходження вірусів. Поліфаг, здатний перевіряти файли в архівах, документи Word і робочі книги Excel, виявляє поліморфні віруси, котрі в останній час, отримують все більше поширення. Достатньо сказати, що епідемію дуже небезпечного вірусу OneHalf зупинив саме DrWeb. Евристичний аналізатор DrWeb, досліджуючи програми на наявність фрагментів коду, характерних для вірусів, дозволяє знайти майже 90% невідомих вірусів. При завантаженні програми в першу чергу DrWeb перевіряє самого себе на цілісність, після чого тестує оперативну пам'ять. Програма може працювати у діалоговому режимі, має дуже зручний інтерфейс користувача, який можна настроювати.

Сканер Avast

Є порівняно новим антивірусним сканером (рис. 7.12). При його роботі, в правому нижньому куті екрану є відповідний індикатор невеликого розміру.

Захист доступу Avast базується на так званих резидентних провайдерах. Це спеціальні модулі, що використовуються для захисту специфічних підсистем комп'ютера, таких як електронна пошта, файлова система і т.п.

При знаходженні проблемного файлу на екран виводиться відповідне повідомлення (рис. 7.13), з можливими рекомендованими користувачу діями.

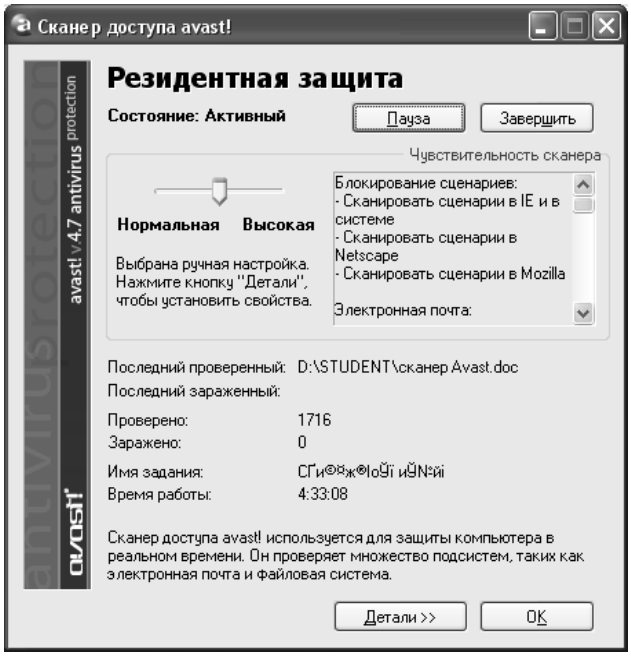

Рис. 7.12. Сканер Avast

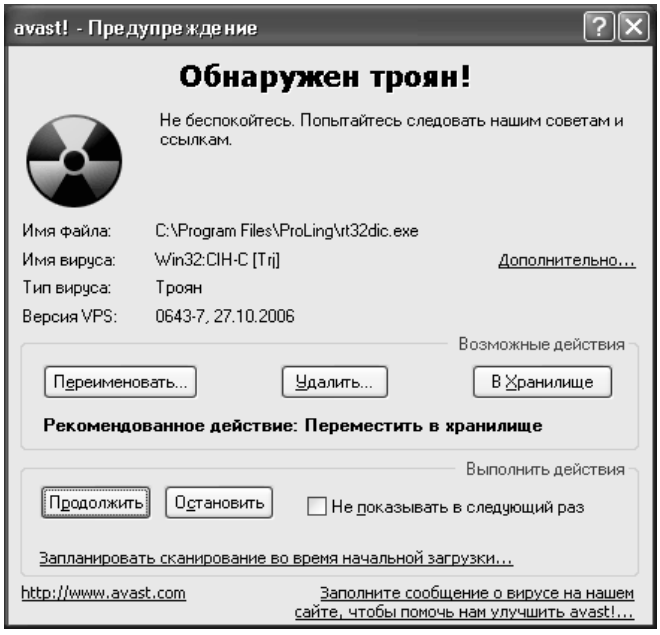

Рис. 7.13. Повідомлення про вірус

7.3.4. Міжмережні екрани

Міжмережний екран - це програмний або апаратно-програмний комплекс, що дозволяє розділити мережу на дві чи більше частин і реалізувати набір правил, що будуть визначати умови проходження пакетів з однієї частини в іншу.

Власник комп'ютера, що має вихід в Internet, установлює міжмережний екран (рис. 7.14), щоб запобігти одержанню сторонніми конфіденційних даних, котрі зберігаються на комп'ютері, а також для контролю за зовнішніми ресурсами, до яких мають доступ інші користувачі даної комп'ютерної системи.

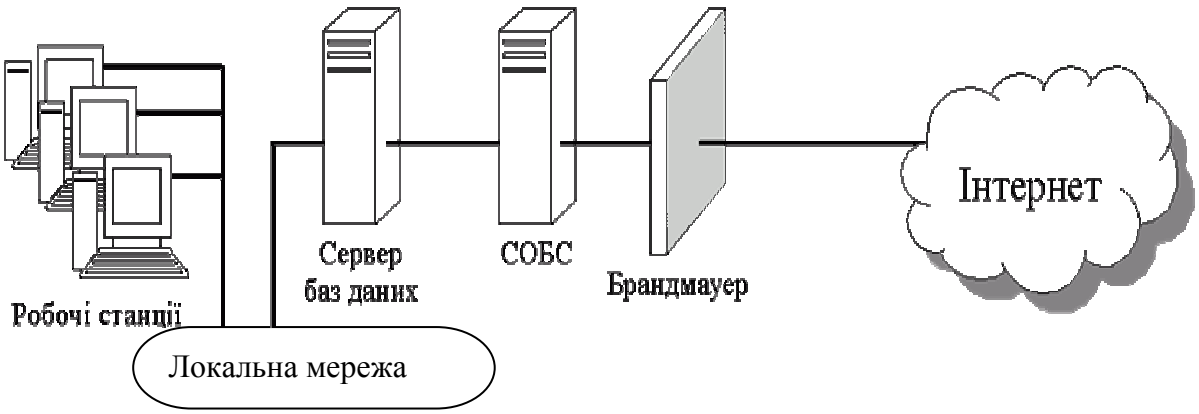

Рис. 7.14. Логічна схема розташування брандмауера

Міжмережні екрани здатні вирішувати ряд завдань стосовно захисту від найбільш імовірних атак для внутрішніх мереж. У вітчизняній літературі частіше зустрічаються терміни іноземного походження: брандмауер (німецького походження) і firewall (англійське). Поза комп'ютерною сферою брандмауером

(чи firewall) називають протипожежну стіну, зроблену з вогнестійких матеріалів, щоб перешкодити поширенню пожежі. У сфері використання комп'ютерних технологій міжмережний екран становить собою бар'єр, що захищає від умовної пожежі – спроб зловмисників несанкціоновано вторгнутися у внутрішню мережу для вчинення протиправних дій. Міжмережний екран покликаний створити безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

В ідеалі система має запобігати будь-якому несанкціонованому вторгненню. Однак, враховуючи широкий спектр Web-сервісів, необхідних користувачам, ftp, telnet, SNMP, Network File System, IP телефонія, електронна пошта тощо, досягнути певного рівня запобігання несанкціонованому втручанню дуже важко.

Насправді мірою ефективності firewall є зовсім не його здатність відмовити в наданні сервісів, а його властивість надавати сервіси користувачам у ефективному, структурованому й надійному середовищі. Системи firewall мають аналізувати вхідний та вихідний мережний трафік і правильно визначати, які з транзакцій є санкціонованими, а які - ні.

Зарубіжні фахівці вважають, що багато проблем, пов'язаних з безпекою Internet, можна зняти або зробити менш серйозними за допомогою широко відомих методів та засобів контролю безпеки – хостів firewall.

Для встановлення між мережних екранів використовується цілий ряд апаратних та програмних засобів.

Так, на рис. 7.15. зображений міжмережний екран Zyxel ZyWALL P1. Продуктивність - 80 Мбіт/с. Продуктивність VPN - 30 Мбіт/с. Wan-порт 10/100. Управління, Web-інтерфейс, Підтримка SNMP та VPN.

Рис. 7.15. Міжмережний екран Zyxel

Найбільш розповсюджені наступні програмні системи: Outpost, McAfee, Norton, Sygate и ZoneAlarm.

Outpost Firevall Pro v3.51

Потужний брандмауер (рис. 7.16) для безпечної роботи в мережі. Має безліч функцій: контроль додатків, що користаються Internet, контроль компонентів, прихованих процесів, п'ять режимів роботи, набір стандартних правил для визначених додатків, детектор атак, контроль умісту, й ін.

За замовчуванням використовує модулі:

- DNS, що блокує й оповіщає про неправильні DNS запити;
- Детектор атак, що запобігає атаки на ваш комп'ютер (portscan, nuke, winnuke і ін.);
- Інтерактивні елементи, де ви можете визначити, що робити з різними елементами Web-сторінки (Active, Java, Java script, Gif, Flash, Referers, сховані фрейми, зовнішні об'єкти, cookies і спливаючі вікна), причому ви має можливість задати особливі параметри для будь-якого окремо узятого сайта (наприклад, у вас встановлено блокування Flash, а ви за-

йшли на сайт із Flash іграми, те просто внесіть адресу сайта в список і виберіть "дозволити" для flash);

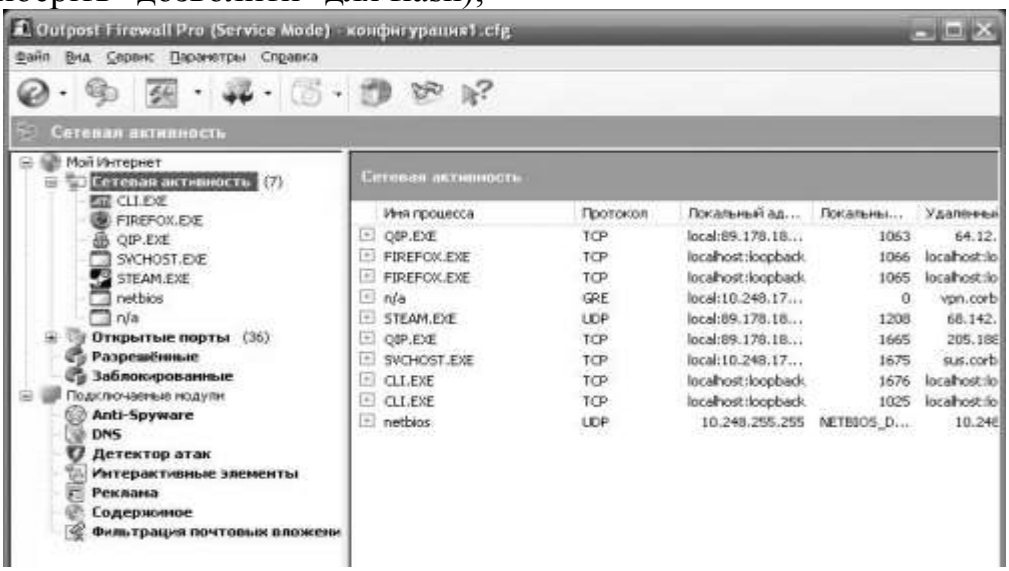

Рис. 7.16. Робоче вікно брандмауера Outpost

- Реклама, де блокуються банери (88x31 і ін.) і реклама (певні слова), причому знову ж ви можете додати і видалити слова і розміри банерів (наприклад, бувають баннеры 90x35 чи 90x50; додайте їх у список і вони не будуть завантажуватися);
- Журнал усіх подій, де ви можна переглянути всі події і дії програми;
- Вміст, де ви можете заблокувати сайти з визначеним змістом чи адресою, і фільтрація поштових вкладень, де визначаються типи файлів, що прикріплюються, і дії ("повідомити" і "перейменувати").
- В описуваній версії також є антишпигунський сканер.

Zone alarm pro 6 – один із самих потужних і надійних брандмауерів (рис. 7.17) для безпечної роботи в Мережі. Має дружній і легко зрозумілий інтерфейс, гнучке настроювання параметрів захисту, блокування різноманітних Pop-up, Cookies, Java-аплетів, Java-скриптів, ActiveX, Gif-анімації, контроль програм і компонентів, антишпигунський сканер та інше.

Рис. 7.17. Вікно Zone alarm pro 6

При роботі з безкоштовною версією програми користувач повинен вказати тільки потрібний рівень безпеки – слабкий, звичайний чи високий.

В платній версії добавлено багато сервісних компонентів, зокрема вбудований антивірус, можливість ведення списків заблокованих портів, та ін.

7.3.5. Системи контролю змісту та антиспаму

Спам – розсилка якого-небудь повідомлення (частіше рекламного чи комерційного характеру) багатьом адресатам для яких це повідомлення небажане.

При чому проблема спаму стосується не тільки електронної пошти, а й ICQ, SMS-повідомлення, Тобто проблема стосується кожного, хто використовує електронні засоби спілкування. Відомо, що навіть у самих надійних провайдерів може бути "витік" баз поштових адрес.

Небажана пошта це не завжди спам, оскільки до неї можуть відноситися:

1. пошта, направлена помилково (технічними службами чи людьми);
2. технічна кореспонденція (повідомлення про доставку кореспонденції, про помилковість e-mail адреси, і т.і.);
3. автоматичні повідомлення від антивірусних програм про наявність вірусів у відправленій кореспонденції;
4. листи від ділових партнерів, що зв’язались з Вами вперше.

Оскільки ця проблема виникла досить давно, існує дві групи програм, призначених для боротьби з спамом. Перші містять базу "чорних" адрес спамерів, яка постійно оновлюється, і при надходженні від них листа видаляють його. Інші, навпаки, пропонують користувачу створити "білий" список адресатів, а інші повідомлення блокують.

Anti-Spammer (рис. 7.18) – працює як самостійний додаток, не вбудовуючись в поштовий клієнт, але в той же час може працювати разом з поштовою програмою.

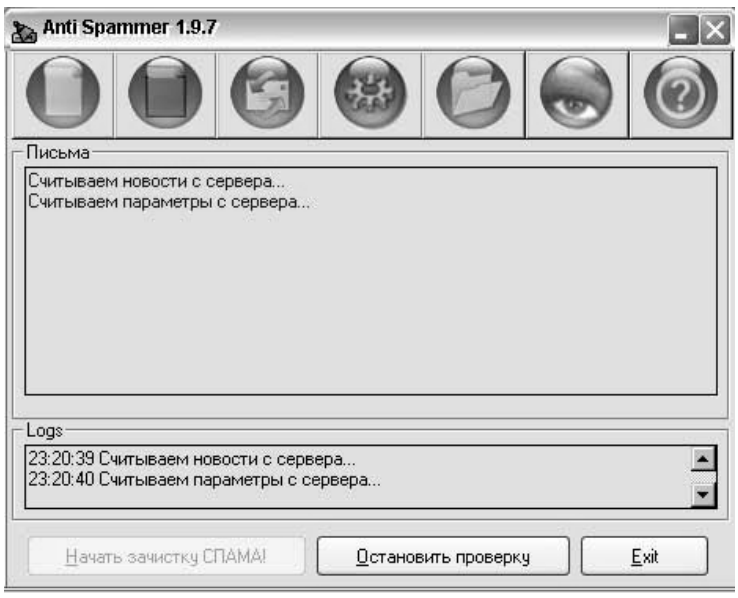

Рис. 7.18. Робоче вікно Anti-Spammer

Обробляє небажані повідомлення за принципом "білого" списку (хоча "чорний" список теж використовується). Вам необхідно додати в програму облікові записи пошти (їх кількість не обмежена), а після цього занести в базу утиліти адреси ваших кореспондентів і вказати тему, листи з якою будуть пропускатися.

Програма зчитує адресу відправника і тему кожного з листів, після чого перевірить адреси на відповідність "білому" списку. Другий етап - порівняння теми листа. Якщо адреса чи тема листа збігаються з занесеними в список, лист пропускається, якщо ж ні, адреса відправника заноситься в "чорний" список. Далі програмою адресату відправляється повідомлення про те, що лист не був отриманий і що для його

одержання повідомлення потрібно відправити ще раз, указавши задану тему листа. Сам лист видаляється чи скачується і зберігається в програмі.

Після обробки Anti-Spammer вхідної пошти, можна запускати поштову програму.

Spam Washer є посередником між сервером і поштовим клієнтом, однак може служити і заміною поштовику, дозволяє фільтрувати вхідну пошту, використовуючи при цьому як убудовані правила, так і створювані користувачем.

7.3.6. Автентифікація користувача

Першим етапом на шляху захисту ресурсів інформаційної системи є організація перевірки, чи є користувач, який входить в систему, тим, за кого він себе видає. Сама процедура перевірки носить назву *автентифікації* користувача.

Автентифікацію користувача можна вважати основою програмно-технічних засобів безпеки, оскільки багато інших сервісів розраховані на обслуговування саме іменованих суб'єктів. Як правило, процедура перевірки (рис. 7.19-7.20) складається з двох етапів: ідентифікації та верифікації.

Під *ідентифікацією* розуміють процедуру представлення користувача системі. Звичайно це відбувається шляхом уведення імені, під яким користувач зареєстрований в системі.

Верифікація – це процедура, яку система виконує для того, щоб переконатися, що користувач, який входить в систему є саме тим, чиє ім’я він ввів при ідентифікації. Для цього користувачу пропонується ввести пароль, який буде порівняний з паролем в записі обліку цього користувача.

Використання для автентифікації клієнта двох елементів утруднює нелегальне проникнення в систему, оскільки для успіху потрібно подолати два незалежні бар’єри.

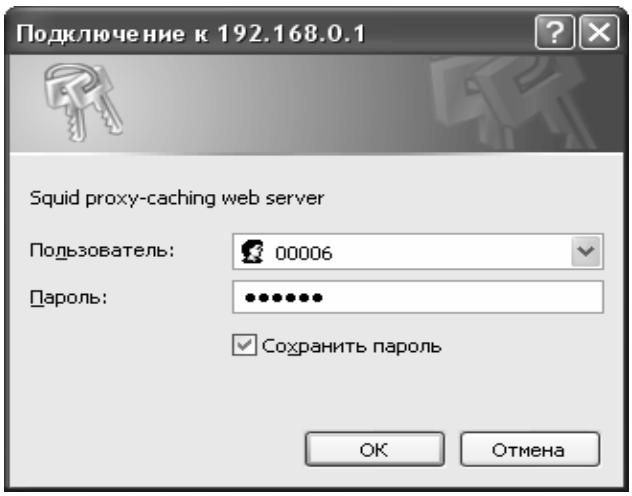

Рис. 7.19. Авторизація при підключенні до Internet

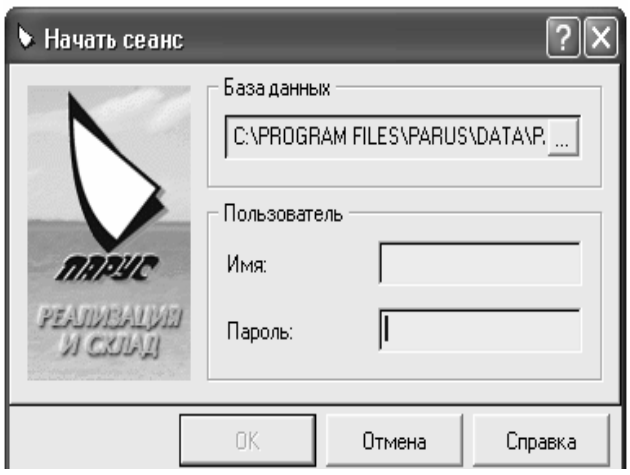

Рис. 7.20. Перевірка користувача, що входить в інформаційну систему Парус

У мережному середовищі, коли сторони територіально рознесені, у розглянутого сервісу є два основних аспекти:

1) що служить верифікатором (тобто використовується для підтвердження сутності суб'єкта);

2) як організований (і захищений) обмін даними.

Суб'єкт може підтвердити себе, використавши:

- щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ і т.п.);
- щось, чим він володіє (особисту картку чи інший пристрій аналогічного призначення);
- щось, що є частину його самого (голос, відбитки пальців і т.п., тобто свої біометричні характеристики).

Процедури автентифікації практично завжди використовуються коли потрібно якимсь чином обмежити доступ. Тут можна згадати про введення логіну та паролю при відкритті поштової скриньки, вибір сеансу користувача системи та введення паролю, користування пластиковою карточкою в банкоматі та ін. Звичайно, система паролів реалізується простіше та потребує менше ресурсів, ніж біометрична верифікація, але і пароль підібрати легше.

В одному з міст США в порядку експерименту була введена біометрична верифікація при знятті готівки в банкоматі, кількість крадіжок знизилась на 70%. Звичайно, при виборі потрібно керуватись співвідношенням можливих збитків при несанкціонованому проникненні і потрібними витратами на систему.

7.3.7. Шифрування даних

Однією з головних проблем безпеки в комп’ютерних мережах завжди була проблема передачі закритої інформації через відкриті канали зв’язку. Причому основними механізмами порушень безпеки при передачі є: перехоплення, модифікація чи фальсифікація.

Унеможливити читання даних сторонніми особами дозволяють процедури шифрування.

Шифрування (ciphering, encryption) – це перетворення даних у форму, що не дає можливості безпосереднього сприйняття зашифрованої інформації.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм – математична функція, яка комбінує відкритий текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв’язаного (шифрованого) тексту.

Придумати новий алгоритм складно, тому стандартні алгоритми використовують з багатьма ключами. Надійність алгоритму шифрування залежить від довжини використовуваного ключа.

Довжина ключа – кількість біт у ключі, яка визначає число можливих комбінацій.

Для зберігання ключів існують і апаратні засоби. Це мініатюрні пристрої, серед яких найбільш поширені пластикові старт-картки, що приєднуються до USB-портів комп’ютера. Вони ж можуть використовуватися і для зберігання паролів. Ці пристрої можуть бути простими і мати обмежений набір функцій чи

досить потужними. Основна перевага, що зловмисник може атакувати їх тільки при приєднанні до комп'ютера, тобто має знати і час підключення.

Оскільки шифрування здійснюється з використанням криптографічного ключа (cryptographic key, cryptokey або просто key), то з використанням ключа здійснюється і зворотна процедура дешифрування, тобто приведення зашифрованої інформації до первинного варіанта.

Прикладом використання криптографії є банківські послуги і платежі в діалоговому режимі. Електронний бізнес може існувати тільки за умови конфіденційності інформації, одним із найкращих методів забезпечення якої є криптографія.

Існує два методи шифрування даних – перестановка і заміна. При використанні алгоритму перестановки змінюється порядок бітів при пересиланні. Наприклад, Ви з адресатом зарані домовились про перечення першої літери в кінець слова, тому при відправці повідомлення „Книга" повідомлення буде мати вигляд „Нигак". Якщо при шифруванні використовувати алгоритм заміни, необхідно мати певний шаблон для заміщення символів, що відправляються. якщо при кодування використовувати їх порядкові номери в алфавіті, то повідомлення буде мати вигляд „15 18 11 4 1".

При використанні одного з методів, досить легко підібрати ключ, тому найбільш розповсюдженим методом є чергове використання методик заміни та перестановки. Для визначення ключа, для використання при шифруванні і дешифруванні повідомлення, застосовують складні математичні формули.

Розрізняють симетричну і асиметричну криптографію. В першому випадку для шифрування і дешифрування використовується один ключ. В другому – передбачається використання загального (для шифрування) і таємного (для дешифрування) ключа. Загальний і таємний ключ пов'язані один з одним математичною функцією. Загальний ключ повинен бути відомий кожному бажаючому відправити повідомлення. Зашифроване за допомогою загального ключа повідомлення можна прочитати тільки при застосування таємного ключа. Оскільки адресат не зацікавлений в розголошені таємного ключа, тільки він може прочитати повідомлення.

Алгоритми асиметричного шифрування можуть використовуватися для створення цифрових підписів. Цифровий підпис – конкретна реалізація криптографічної системи з відкритим ключем. Для зв'язку імені конкретного суб'єкту з відкритим ключем використовується цифровий сертифікат. Цифровий сертифікат – це ім'я, відкритий ключ та підпис. Видачу цифрових сертифікатів здійснюють державні чи комерційні сертифікаційні центри. Найбільш розповсюдженим стандартом, що описує формат сертифікатів відкритих ключів є стандарт X.509.

Відомі сертифікаційні центри (VeriSign, Cybertrust і Nortel) видають цифрові сертифікати, що містять ім'я власника, назву сертифікаційного центру, відкритий ключ, термін дії сертифіката (від 6 місяців до року), клас та ідентифікаційний номер цифрового сертифіката. Сертифікат може належати до одного з чотирьох класів. Для отримання сертифікату першого класу досить надати ім'я

і адресу електронної пошти. Для четвертого рівня – посвідчення особистості, дату народження, карту соціального страхування, перевірка кредитоздатності, посаду власника в установі та ін. чим вищий клас сертифікату, тим більші вимоги верифікації, і тим вище рівень довіри до нього.

Видача сертифікату здійснюється за певну плату. Сертифікаційні центри також несуть відповідальність за ведення і публікацію списків недійсних сертифікатів.

7.4. Індивідуальні завдання №7

Налагодження безпечних параметрів доступу до Internet в браузері. Використання антивірусних програм та міжмережних екранів

1. Встановити безпечні параметри доступу до Internet в браузері Internet Explorer.
2. Визначити, чи мають подібні можливості настроювання інші використовувані Вами браузери.
3. Перевірити, який додатковий захист встановлено на вашому комп'ютері: антивіруси, брандмауери, антиспамери і т.п. По-можливості, перевірте які вони мають функції.
4. Визначити, коли в останнє оновлювалась антивірусна база даних.
5. Перевірити дискету та папку Student на наявність вірусів.
6. Перелічити в яких випадках, при виконанні лабораторних робіт Ви стикались с процедурою авторизації. Скопіювати одне з вікон у звіт.

Контрольні запитання

1. Дайте визначення вірусу. Як вони себе поводять?
2. Що таке антивіруси. Для чого вони призначені?
3. Які заходи потрібно застосовувати для зниження вірогідності попадання вірусу в комп'ютер?
4. Чим відрізняється брандмауер від антивірусної програми?
5. Особливості дії троянських програм.
6. В чому небезпека мережних хробаків?
7. Як Ви вважаєте, які програми найбільш небезпечні для корпоративних мереж та звичайних користувачів.
8. Які додаткові профілактичні засоби безпеки, на вашу думку, потрібно використовувати?
9. Як перевірити комп'ютер на вірус?
10. Чи обов'язкове спільне використання процедур ідентифікації та верифікації? Якщо ні, привести приклади.
11. Що таке шифрування?
12. В чому різниця між симетричним і асиметричним шифруванням?
13. Що таке цифровий сертифікат?
14. Яка роль сертифікаційних центрів?