Міністерство освіти і науки, молоді та спорту України
Вищий приватний навчальний заклад
Міжнародний економіко – гуманітарний університет
імені академіка Степана Дем'янчука

М.М Боровий

Технології комп'ютерної безпеки

Книга 6

Науковий керівник
……..Р.М.Літнарович,доцент,к.т.н.

Рівне 2012

УДК 004.353.4

Боровий М.М Технології комп'ютерної безпеки.Книга 6. МЕГУ, Рівне, 2012.-78 с.

Borovoy M.M Technologiesof computer security. Book 6. IEGU, Rivne, 2012.-78 p.

Рецензенти: В.Г.Бурачек, доктор технічних наук,професор
Є.С. Парняков, доктортехнічних наук,професор
В.О.Боровий , доктор технічних наук, професор

Відповідальний за випуск: Й.В. Джунь, доктор фізико-математичних наук, професор.

Послідовно розглядаються основні принципи побудови та функціонування комп'ютерних мереж. Монографія містить актуальний матеріал довідково-аналітичного характеру по наступних темах:
програмне забезпечення, пакет прикладних програм, текстові редактори і текстові процесори, відкривання папок, переміщення папок і файлів, LAN , Ethernet - приклад стандартного розв'язання мережевих проблем, комп'ютерні віруси і шкідливі програми, установка продукту на комп'ютер, як захистити від вірусів пошту, як перевірити окремий об'єкт, як перевірити CD-диск або дискету, як поводитися з вірусами, постійний захист, настройка постійного захисту комп'ютера, як перевірити стан захисту, ознаки зараження вірусом, компютерна безпека, види вторгнення, класифікація, безпека з фізичної точки зору, застарілі комп'ютери і їх утилізація, програмний доступ до інформації, користувачі і їх ідентифікація, для вирішення подібних завдань в Novell Netware, корпоративна безпека і її елементи.

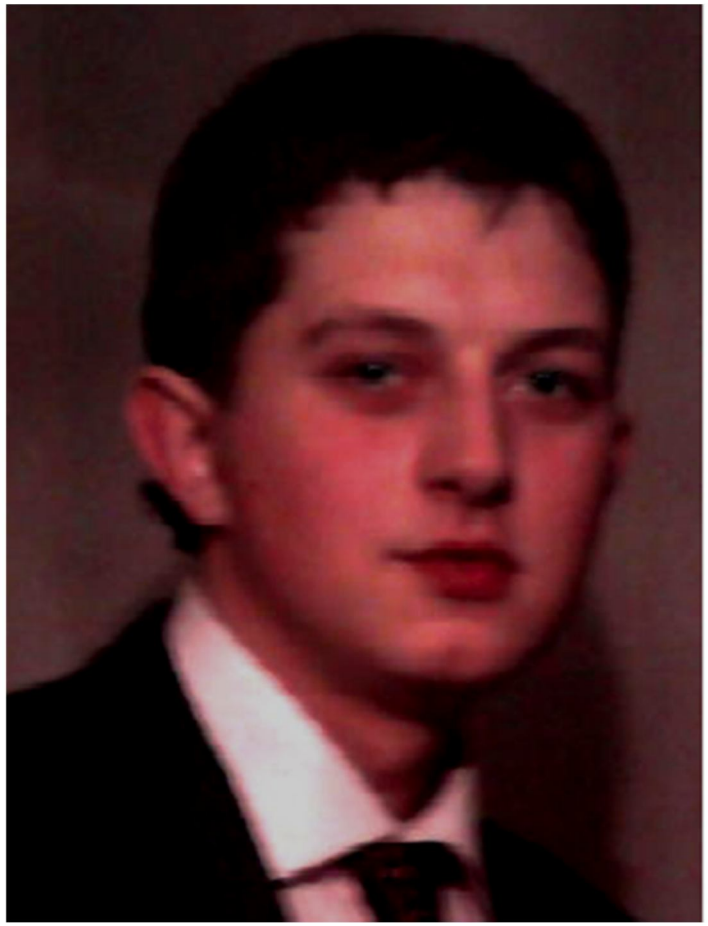
Ключові слова: Програмне забезпечення, Комп'ютерні віруси і шкідливі програми, Компютерна безпека.

Последовательно рассматриваются основные принципы построения и функционирования компьютерных сетей. Монография содержит актуальный материал Справочно-аналитического характера по следующим темам: программное обеспечение, пакет прикладных программ, текстовые редакторы и текстовые процессоры, открытие папок, перемещение папок и файлов, LAN, Ethernet - пример стандартного решения сетевых проблем, компьютерные вирусы и вредоносные программы, установка продукта на компьютер, как защитить от вирусов почту, Как проверить отдельный объект, как проверить CD-диск или дискету, как обращаться с вирусами, постоянная защита, настройка постоянной защиты компьютера, как проверить состояние защиты, признаки заражения вирусом, компьютерная безопасность, виды вторжения, классификация, безопасность с физической точки зрения, устаревшие компьютеры и их утилизация, программный доступ к информации, пользователи и их идентификация, для решения подобных задач в Novell Netware, корпоративная безопасность и ее элементы.

Ключевые слова: Программное обеспечение, Компьютерные вирусы и вредоносные программы, Компьютерная безопасность.

Consistently considers the basic principles of construction and operation of computer networks. This monograph contains the relevant material analytical reference on the following topics: Software, Software Package, text editors and word processors, opening folders, moving files and folders, LAN, Ethernet - an example of a standard solution of network problems, computer viruses and malicious software installing on your computer, as protect against viruses, e-mail, how to scan an object, how to check CD-ROM or floppy disk, how to deal with viruses, time protection to protect your computer setup permanent, how to check the protection status, the signs of the virus, computer security, the types of invasion,classification, security from the physical point of view, outdated computers and theirKDisposal, Programmatic access to information, users and their identification, to solve such problems in a Novell Netware, corporate security and its elements. like

Keywords: Software, Computer viruses and malicious programs, computer security.



Боровий Микола Миколайович

спеціаліст системотехнік,

магістрант інформаційних технологій

Зміст

Вступ

Термін "мережева технологія" частіше за все використовується в описаному вище вузькому значенні, але іноді застосовується і його розширене тлумачення як будь-якого набору засобів і правил для побудови мережі, наприклад, "технологія маршрутизації на скрізь", "технологія створення захищеного каналу", "технологія IP-мереж"

Протоколи, на основі яких будується мережа певної технології (у вузькому значенні), спеціально розроблялися для спільної роботи, тому від розробника мережі не потрібно додаткових зусиль по організації їх взаємодії. Іноді мережеві технології називають базовими технологіями, маючи на увазі те, що на їх основі будується базис будь-якої мережі. Прикладами базових мережевих технологій можуть служити поряд з Ethernet такі відомі технології локальних мереж як, Token Ring і FDDI, або ж технології територіальних мереж X.25 і frame relay. Для отримання працездатної мережі в цьому випадку досить придбати програмні і апаратні засоби, що відносяться до однієї базової технології мережеві адаптери з драйверами, концентратори, комутатори, кабельну систему і т. і., і з'єднати їх відповідно до вимог стандарту на дану технологію.

TCP/IP (Transport Control Protocol/Internet Protocol) - протоколи мережевого рівня, що застосовуються для передачі інформації між мережами. IP-протокол є основою

найбільшої глобальної комп'ютерної мережі Internet. Він реалізує принцип міжмережного з'єднання, зокрема маршрутизацію пакетів. При цьому кожному учаснику мережі привласнюється унікальна IP-адреса. Як транспортне середовище для передачі пакетів у IP-мережах можуть використовуватися магістралі Ethernet, Frame Relay, ATM. TCP-протокол описує процедуру контролю доставки пакета інформації від одного комп'ютера до іншого, грунтуючись тільки на адресній інформації, що знаходиться в пакеті. Цей протокол використовується також у випадку розбирання пакета на менші блоки (наприклад, елементи фіксованої довжини в мережі ATM) при передачі на канальному рівні, оскільки для правильної маршрутизації пакета його треба спочатку зібрати. На вихідному комутаторі відбувається зборка IP-пакетів, а потім вони передаються за IP-адресою.

1. Програмне забезпечення

Програмне забезпечення (ПЗ)- сукупність програм, мов програмування, спеціальних процедур, правил і документації, необхідних для використання програмних продуктів.

Усі програми, з якими працюють на сучасних комп'ютерах, можна розділити на 3 категорії:

Системні програми Інструментальні системи Прикладні програми

Прикладні програми - програми, необхідні користувачеві для його професійної діяльності. Одну частину прикладного програмного забезпечення складають так звані ППП- фахові пакети прикладних програм, іншу - прикладні програми загального призначення, наприклад, текстові та графічні редактори, табличні процесори, системи управління базами даних.

Прикладні програми.

Табличні процесори. Забезпечують зручну роботу з великими масивами чисел та іншої інформації, наданої у вигляді таблиць. При роботі з табличними процесорами на екран виводиться прямокутна таблиця, у комірках якої можуть знаходитись числа, пояснювальні тексти та формули для розрахунків певних значень. Усі табличні процесори дозволяють перераховувати значення елементів таблиць за певними формулами, будувати за даними

таблиць різноманітні графіки. Табличний процесор ms excel зі складу пакета Microsoft office має великі можливості для опрацювання діаграм і графіків та може використовувати таблиці, створені в інших табличних процесорах - lotus 1-2-3,Quattro pro.

Текстові процесори. Це потужні програми для роботи з текстом. Текстовий процесор MS WORD зі складу пакету MICROSOFT OFFICCE, чи не найпоширеніша у світі прикладна програма, можливості якої можуть бути порівняні з можливостями настільної видавничої системи

Системи управління базами даних. Такі програми дозволяють керувати великими інформаційними масивами - базами даних. Ms access зі складу пакета Microsoft office - зручний та потужний засіб управління базами даних, який має всі можливості реляційних баз даних і дозволяє створювати досить складні програмні застосування, з якими буде зручно працювати користувачеві.

Графічні редактори. Прикладні програми, що дозволяють створювати та редагувати малюнки на екрані комп'ютера. Звичайно користувачу надається можливості малювання прямих і кривих ліній, різноманітних геометричних фігур, створення написів різними шрифтом. Більшість графічних редакторів дозволяють обробляти зображення, отримані з допомогою сканерів.

Системи автоматизованого проектування (САПР). Програми, що дозволяють здійснювати креслення та

конструювання різноманітних механізмів з допомогою комп'ютера. Найпоширеніші САПР- AutoCAD, ArchiCad.

Для розв’язання конкретної задачі комп’ютер повинен послідовно виконати цілком визначений набір операцій. Ці операції є сукупністю дій, здійснюваних центральним процесором. Самі по собі окремі дії ЦП прості і виконуються дуже швидко. Потрібні дії та черговість їх виконання задає програма, що призначена для розв’язання цієї задачі.

Програми, що забезпечують можливість використання комп’ютерами, поділяються на два основних види. Перший вид – програми, що керують діями пристроїв апаратної частини комп’ютера. Сукупність таких програм називається операційною системою (ОС).

Другий вид – програми, що керують діями комп’ютера під час розв’язання за його допомогою конкретних задач. Такі програми називаються прикладними програмами

1.1Пакет прикладних програм

Основне призначення прикладних програм – це розв’язання задач у конкретній предметній галузі.

При розв’язанні задач за допомогою комп’ютера її розбивають на кілька частин – підзадач. Кожна з цих під задач розв’язується за допомогою своєї прикладної програми. Розв’язання вихідної задачі забезпечується

сукупністю всіх використовуваних прикладних програм. Для розв'язування задач однакового типу створено системи прикладних програм, за допомогою яких розв'язуються різні конкретні задачі даного типу. Системи прикладних програм, що дозволяють розв'язувати задачі певного типу, називаються пакетами прикладних програм.

За типом розв'язуваних задач серед наявних нині прикладних програм виділяються такі основні групи:

· текстові редактори і текстові процеси

· електронні таблиці

· бази даних

· графічні пакети

· системи штучного інтелекту й експертні системи

· навчальні програми

· системи мультимедіа, комп'ютерні ігри та розваги.

У кожній із зазначених груп є багато прикладних програм, що різняться особливостями і можливостями.

Використання пакета прикладних програм потребує наявності певного набору пристроїв у апаратної частини, певного об'єму оперативної пам'яті комп'ютера, певної операційної системи. Під час вибору пакета прикладних програм для роботи користувач мусить враховувати можливості свого конкретного комп'ютера.

1.2.Текстові редактори і текстові процесори

Однією з найважливіших ділянок застосувань комп'ютерів є їх використання для створення та обробки різних текстів: складання листів і оформлення документів, створення журналів з кольоровими ілюстраціями та наукових книжок з формулами та кресленнями.

Пакети прикладних програм, що їх називають текстовими редакторами, дають змогу використовувати комп'ютер для розв'язування задач зазначеного типу.

Текстовий редактор – це програма**,** призначена для створення і обробки текстів.

За допомогою цих програм користувач створює нові тексти та редагує ті, що вже має. Текст, з яким працює користувач, перед ним на екрані дисплея. Користувач або набирає текст, або, використовуючи курсор для пересування по тексту, набирає і вставляє в текст пропущені літери чи слова, змінює розташування частин тексту, включає в текст формули, діаграми, малюнки, складає таблиці.

Текстові редактори дають змогу виводити на екран дисплея кілька текстів одночасно і компонувати з їхніх частин новий текст, автоматично розбивати текст на сторінки, складати зміст та правильно розташовувати посилання, управляти розмірами літер і шрифтів у різних частинах тексту, автоматично контролювати орфографію та

пунктуацію, сортувати рядки таблиць, друкувати текст або будь-яку його частину у заданому користувачем вигляді.

Окрім текстових редакторів, для обробки текстів нині використовують програми, що мають назву текстові процесори.

Відмінність між текстовими редакторами і текстовими процесорами досить умовна. Як правило, текстові редактори мають менше можливостей і використовуються для підготовки текстів нескладної форми. Текстові процесори є розширенням текстових редакторів у тому розумінні, що вони мають додаткові можливості, які можна використати під час підготовки складних за формою текстів.

Для використання текстових редакторів і текстових процесорів достатньо стандартного набору пристроїв комп’ютера. Текстові процесори потребують більшої оперативної пам’яті для зберігання, ніж текстові редактори.

В нашій країні найпоширенішими є текстові редактори Твір, Multi-Edit різних версій, Notepad, WordPad, текстові процесори Word, Word-Star, Tex.

керування папками, файлами та ярликами. меню пуск

Створення папок

Із погляду документ-орієнтовані ОС Windows 98 папки є контейнерами, в яких зберігаються інші інформаційні об'єкти: документи, додатки, інші папки та ярлики.

Документи і додатки створюються відповідними додатками (наприклад, текстовими та графічними редакторами, ЕТ, інструментальними системами програмування і т.д). Папки та ярлики створюються засобами самої ОС Windows 98.

Для створення нової папки всередині вже існуючої (у тому числі на робочому столі) досить клацнути правою клавішею миші на вільному місці робочої області відкритої папки і з контекстного меню, що з'явилося, вибрати пункт «Створити», а в ньому — підпункт «Папка», потім увести ім'я папки і натиснути на клавішу .

Другим дуже поширеним способом створення нової папки всередині відкритої під час використання багатьох додатків є натиснення на кнопку «Створити папку» панелі інструментів діалогового вікна при зберіганні документа. Ця кнопка дублює команду меню Файл — Створити.

1.3.**Відкривання папок**

Якщо потрібно відкрити папку, що міститься всередині вже відкритої, то слід у робочій області цієї папки знайти значок папки, що відкривається, і двічі клацнути на ньому мишею.

Для виконання зворотної дії (переходу з укладеної папки до папки вищого рівня) досить на панелі інструментів клацнути мишею на кнопці «Вверх»

Для відкривання довільної папки слід клацнути мишею у полі «Адресна строчка», що розташовується на панелі інструментів або під нею, і зі списку дисків, який з'явився, вибрати потрібний диск, клацнувши мишею на його значку. Потім у робочій області папки диска, яка відкрилася, треба вибрати потрібну папку, двічі клацнувши мишею на її значку, і т. д.

Для повернення до папки, що була відкрита перед цим, потрібно на панелі інструментів клацнути мишею накнопці «Назад». При цьому можна знову повернутися до вихідної папки, клацнувши мишею на кнопці «Вперед»

1.4.**Переміщення папок і файлів**

Переміщення папок і файлів з однієї папки (вихідної) до іншої (цільової) можна здійснити кількома способами.

Спосіб 1 (через буфер обміну). Клацнути правою клавішею миші на переміщуваному об'єкті у вихідній папці і з контекстного меню вибрати пункт «Вирізати». Потім, установивши курсор на вільному місці цільової папки, клацнути правою клавішею миші й вибрати пункт «Вставить».

Спосіб 2 (перетягання мишею):

а) відкрити вікна вихідної і цільової папок, натиснути на праву клавішу миші на переміщуваному об'єкті і, не відпускаючи її, перетягнути його на вільне місце робочої області цільової папки і відпустити клавішу. З контекстного меню, що з'явилося, вибрати пункт «Перемістити»;

б) Натиснути на ліву клавішу миші на переміщуваному об'єкті і перетягнути його на вільне місце робочої області цільової папки. В цьому разі контекстне меню не з'являється.

Перервати операцію перетягання можна одним із способів:

• перемістити об'єкт у вихідну папку;

• із контекстного меню вибрати пункт «Відмінити»;

• не відпускаючи клавішу миші, натиснути на клавішу <Esc> або на іншу клавішу миші.

Копіювання папок і файлів виконується аналогічно переміщенню. У способі 1 замість пункту «Вирізати» вибрати пункт «Копіювати», а в способі 2а замість пункту «Перемістить» — також пункт «Копіювати». При копіюванні лівою клавішею миші натиснути додатково на клавішу <Ctrl> й утримувати її.

Примітки. 1. При переміщенні та копіюванні папок і файлів необов'язково відкривати цільову папку. Перетягувати об'єкт можна на її значок.

2. Якщо при перетяганні значка файлу накласти його па значок додатка, то Windows 98 запускає на виконання цей додаток для оброблення даного файлу. Наприклад, текст документа буде оброблятися в текстовому редакторі Word, якщо його помістити на значок Word, або роздруковуватися на принтері, якщо його помістити на значок принтера. Вилучення папок і файлів найчастіше здійснюється

1) перетягнути об'єкт лівою клавішею миші на значок «Кошика»;

2) позначити об'єкт і натиснути на клавішу ;

3) позначити об'єкт і в меню вікна відкритої папки вибрати пункт «Файл—Видалить» або на панелі інструментів клацнути мишею на відповідній кнопці;

4) клацнути правою клавішею миші на об'єкті, що вилучається, і в контекстному меню вибрати пункт «Видалити».

При використанні способів 2—4 видається запит на підтвердження переміщення у «Кошик» об'єкта, що вилучається. Із «Кошика» надалі його можна буде відновити на колишньому місці. Якщо точно відомо, що відновлення не знадобиться, то відразу можна вилучати об'єкт остаточно. Для цього під час вилучення необхідно додатково утримувати натиснуту клавішу .

Щоб перейменувати папку або файл, треба ввійти в режим редагування його імені одним із таких способів:

* позначити об'єкт і клацнути лівою клавішею миші на його імені або натиснути на клавішу ;

* клацнути правою клавішею миші на об'єкті й вибрати пункт «Перейменувати».

Потім змінити ім'я і натиснути на клавішу <Enter>.

Windows 98 запам'ятовує всі дії щодо перейменування, копіювання, переміщення і вилучення файлів. Це дає змогу скасувати ці дії у порядку, зворотному їх виконанню. Для цього досить викликати контекстне меню й у ньому вибрати відповідний пункт або в меню відкритої папки вибрати пункт «Правка—відмінити видалення», чи на панелі інструментів клацнути мишею на кнопці «Відмінити».

Ethernet - приклад стандартного розв'язання мережевих проблем.Мережева технологія це узгоджений набір стандартних протоколів іреалізовуючих їх програмно-апаратних засобів (наприклад, мережевих адаптерів, драйверів, кабелів і розйом), достатній для побудовиобчислювальної мережі. Епітет “достатній” підкреслює ту обставину, щоцей набір являє собою мінімальний набір засобів, за допомогою яких можнапобудувати працездатну мережу. Можливо, цю мережу можна поліпшити,наприклад, за рахунок виділення в ній підмереж, що відразу зажадає крім протоколів

стандарту Ethernet застосування протоколу IP, а також спеціальних комунікаційних пристроїв маршрутизаторів. Поліпшена мережа буде, швидше за все, більш надійною і швидкодіючою, але за рахунок надбудов над засобами технології Ethernet, яка склала базис мережі.Термін “мережева технологія” частіше за все використовується в описаному вище вузькому значенні, але іноді застосовується і його розширене тлумачення як будь-якого набору засобів і правил для побудови мережі,наприклад, “технологія маршрутизації на скрізь”, “технологія створення захищеного каналу”, “технологія IP-мереж”.

Протоколи, на основі яких будується мережа певної технології (у вузькому значенні), спеціально розроблялися для спільної роботи, тому від розробника мережі не потрібно додаткових зусиль по організації їх взаємодії. Іноді мережеві технології називають базовими технологіями,маючи на увазі те, що на їх основі будується базис будь-якої мережі.Прикладами базових мережевих технологій можуть служити поряд з Ethernet такі відомі технології локальних мереж як, Token Ring і FDDI, або технології територіальних мереж X.25 і frame relay. Для отримання працездатної мережі в цьому випадку досить придбати програмні і апаратні засоби, що відносяться до однієї базової технології мережеві адаптери здрайверами, концентратори, комутатори, кабельну систему і т. п., із'єднати їх відповідно до вимог стандарту на дану технологію.

Стандарт Ethernet був прийнятий в 1980 році. Число мереж, побудованих наоснові цієї технології, до даного моменту оцінюється в 5 мільйонів, а кількість комп'ютерів, працюючих в таких мережах, в 50 мільйонів.

Основний принцип, встановлений в основу Ethernet, - випадковий метод доступу до середи передачі даних, що розділяється. Як така середа може використовуватися товстий або тонкий коаксіальний кабель, віта пара, оптоволокно або радіохвилі (до речі, першою мережею, побудованою напринципі випадкового доступу до середи, що розділяється, була радіомережа Aloha Гавайського університету).

У стандарті Ethernet суворо зафіксована топологія електричних зв'язків. Комп'ютери підключаються до середи, що розділяється відповідно до типової структури “загальна шина” (мал. 1.13). За допомогою шини, що розділяється в часі будь-які два комп'ютери можуть обмінюватися даними.

Управління доступом до лінії зв'язку здійснюється спеціальними контролерами мережевими адаптерами Ethernet. Кожний комп'ютер, а більш точно, кожний мережевий адаптер, має унікальну адресу. Передача даних----> Page: мережевий адаптер, має унікальну адресу. Передача даних відбувається з швидкістю 10 Мбіт/с. Ця величина є пропускною спроможністю мережі Ethernet.

Суть випадкового методу доступу складається в наступному. Комп'ютер в мережі Ethernet може передавати

дані по мережі, тільки якщо мережа вільна, тобто якщо ніякий інший комп'ютер в даний момент не займається обміном. Тому важливою частиною технології Ethernet є процедура визначення доступності середи.

Після того як комп'ютер пересвідчився, що мережа вільна, він починає передачу, при цьому “захоплює” середу. Час монопольного використання середи, що розділяється одним вузлом обмежується часом передачі одного кадру. Кадр це одиниця даних, якими обмінюються комп'ютери в мережі Ethernet. Кадр має фіксований формат і нарівні з полем даних містить різну службову інформацію, наприклад адресу одержувача і адресу відправника.

Мережа Ethernet влаштована так, що при попаданні кадру в середу передачі даних, що розділяється всі мережеві адаптери одночасно починають приймати цей кадр. Всі вони аналізують адресу призначення, розташовану в одному з початкових полів кадру, і, якщо ця адреса співпадає з їх власною адресою, кадр вміщується у внутрішній буфер мережевого адаптера.Таким чином комп'ютер-адресат отримує призначені йому дані.

Іноді може виникати ситуація, коли одночасно два або більше за комп'ютер вирішують, що мережа вільна, і починають передавати інформацію. Така ситуація, звана колізією, перешкоджає правильній передачі даних по мережі. У стандарті Ethernet передбачений алгоритм виявлення і коректної обробки колізій. Імовірність

виникнення колізії залежить від інтенсивності мережевого трафіка.

Після виявлення колізії мережеві адаптери, які намагалися передати свої кадри, припиняють передачу і після паузи випадкової тривалості намагаються знов отримати доступ до середи і передати той кадр, який викликав колізію.

Головним достоїнством мереж Ethernet, завдяки якому вони стали такою популярною, є їх економічність. Для побудови мережі досить мати по одному мережевому адаптеру для кожного комп'ютера плюс один фізичний сегмент коаксіального кабелю потрібної довжини. Інші базові технології,наприклад Token Ring, для створення навіть невеликої мережі вимагають наявності додаткового пристрою концентратора.

Крім того, в мережах Ethernet реалізовані досить прості алгоритми доступу до середи, адресації і передачі даних. Простота логіки роботи мережі введе до спрощення і, відповідно, здешевлення мережевих адаптерів і їх драйверів. По тій же причині адаптери мережі Ethernet мають високу надійність. І нарешті, ще однією чудовою властивістю мереж Ethernet є їх хороша розширюваність, тобто легкість підключення нових вузлів.

Інші базові мережеві технології Token Ring, FDDI, 100VGAny-LAN, хоч і володіють багатьма індивідуальними рисами, в той же час мають багато загальних властивостей з Ethernet. Насамперед це застосування регулярних фіксованих топологій (ієрархічна

зірка і кільце), а також серед передачі -----> Page: також серед передачі даних, що розділяються. Істотні відмінності однієї технології від іншої пов'язані з особливостями методу доступу, що використовується до середи,що розділяється. Так, відмінності технології Ethernet від технології Token Ring багато в чому визначаються специфікою закладених в них методів розділення середи випадкового алгоритму доступу в Ethernet і методу доступу шляхом передачі маркера в Token Ring.

1.5.**LAN**

LAN (Local Area Network) - локальна мережа передачі даних, чи локальна обчислювальна мережа (ЛОМ). ЛОМ єкомунікаційною системою, що підтримує в межах будинку чи деякої топологічно обмеженої території один або кілька високошвидкісних каналів передачі інформації. Трьома базовими компонентами ЛОМ є плати мережного інтерфейсу (NIC), що встановлені на кожному підключеному до мережі ПК, кабелі і серверне устаткування, а також програмне забезпечення керування мережею.

TCP/IP

TCP/IP (Transport Control Protocol/Internet Protocol) - протоколи мережного рівня, що застосовуються для передачі інформації між мережами. IP-протокол є основою найбільшої глобальної комп'ютерної мережі Internet. Він реалізує принцип міжмережного з'єднання, зокрема маршрутизацію пакетів. При цьому кожному учаснику

мережі привласнюється унікальна IP-адреса. Як транспортне середовище для передачі пакетів у IP-мережах можуть використовуватися магістралі Ethernet, Frame Relay, ATM. TCP-протокол описує процедуру контролю доставки пакета інформації від одного комп'ютера до іншого, грунтуючись тільки на адресній інформації, що знаходиться в пакеті. Цей протокол використовується також у випадку розбирання пакета на менші блоки (наприклад, елементи фіксованої довжини в мережі ATM) при передачі на канальному рівні, оскільки для правильної маршрутизації пакета його треба спочатку зібрати. На вихідному комутаторі відбувається зборка IP-пакетів, а потім вони передаються за IP-адресою.

Token Ring

Token Ring - це технологія організації локальних мереж, що використовує принцип керуючого кадру (маркера) і загальне середовище передачі даних, з'єднуюче всі пристрої мережі в єдине кільце. Право на використання кільця визначається за допомогою маркера, що послідовно передається від одного пристрою до іншого. Пристрій може почати передачу даних тільки після одержання маркера. Споконвічно мережі Token Ring могли працювати з двома бітовими швидкостями - 4 Мбіт/с і 16 Мбіт/с. Сьогодні доступні більш високі швидкості. Як середовище передачі може бути використаний кабель будь-якої конструкції: кручена пара, коаксіал чи оптоволокно.

1.6.Ethernet - приклад стандартного розв'язання мережевих проблем

Мережева технологія це узгоджений набір стандартних протоколів і реалізовуючих їх програмно-апаратних засобів (наприклад, мережевих адаптерів, драйверів, кабелів і роз'єм), достатній для побудови обчислювальної мережі. Епітет “достатній” підкреслює ту обставину, що цей набір являє собою мінімальний набір засобів, за допомогою яких можна побудувати працездатну мережу. Можливо, цю мережу можна поліпшити, наприклад, за рахунок виділення в ній підмереж, що відразу зажадає крім протоколів стандарту Ethernet застосування протоколу IP, а також спеціальних комунікаційних пристроїв маршрутизаторів. Поліпшена мережа буде, швидше за все, більш надійною і швидкодіючою, але за рахунок надбудов над засобами технології Ethernet, яка склала базис мережі.

Термін “мережева технологія” частіше за все використовується в описаному вище вузькому значенні, але іноді застосовується і його розширене тлумачення як будь-якого набору засобів і правил для побудови мережі, наприклад, “технологія маршрутизації на скрізь”, “технологія створення захищеного каналу”, “технологія IP-мереж”

Протоколи, на основі яких будується мережа певної технології (у вузькому значенні), спеціально розроблялися для спільної роботи, тому від розробника мережі не потрібно додаткових зусиль по організації їх взаємодії.

Іноді мережеві технології називають базовими технологіями, маючи на увазі те, що на їх основі будується базис будь-якої мережі. Прикладами базових мережевих технологій можуть служити поряд з Ethernet такі відомі технології локальних мереж як, Token Ring і FDDI, або ж технології територіальних мереж X.25 і frame relay. Для отримання прецездатної мережі в цьому випадку досить придбати програмні і апаратні засоби, що відносяться до однієї базової технології мережеві адаптери з драйверами, концентратори, комутатори, кабельну систему і т. п., і з'єднати їх відповідно до вимог стандарту на дану технологію.

Стандарт Ethernet був прийнятий в 1980 році. Число мереж, побудованих на основі цієї технології, до даного моменту оцінюється в 5 мільйонів, а кількість комп'ютерів, працюючих в таких мережах, в 50 мільйонів.

Основний принцип, встановлений в основу Ethernet, - випадковий метод доступу до середи передачі даних, що розділяється. Як така середа може використовуватися товстий або тонкий коаксіальний кабель, віта пара, оптоволокно або радіохвилі (до речі, першою мережею, побудованою на принципі випадкового доступу до середи, що розділяється, була радіомережа Aloha Гавайського університету).

У стандарті Ethernet суворо зафіксована топологія електричних зв'язків. Комп'ютери підключаються до середи, що розділяється відповідно до типової структури

“загальна шина” (мал. 1.13). За допомогою шини, що розділяється в часі будь-які два комп'ютери можуть обмінюватися даними. Управління доступом до лінії зв'язку здійснюється спеціальними контролерами мережевими адаптерами Ethernet. Кожний комп'ютер, а більш точно, кожний мережевий адаптер, має унікальну адресу. Передача даних відбувається з швидкістю 10 Мбіт/с. Ця величина є пропускною спроможністю мережі Ethernet.

Суть випадкового методу доступу складається в наступному. Комп'ютер в мережі Ethernet може передавати дані по мережі, тільки якщо мережа вільна, тобто якщо ніякий інший комп'ютер в даний момент не займається обміном. Тому важливою частиною технології Ethernet є процедура визначення доступності середи.

Після того як комп'ютер пересвідчився, що мережа вільна, він починає передачу, при цьому “захоплює” середу. Час монопольного використання середи, що розділяється одним вузлом обмежується часом передачі одного кадру. Кадр це одиниця даних, якими обмінюються комп'ютери в мережі Ethernet. Кадр має фіксований формат і нарівні з полем даних містить різну службову інформацію, наприклад адресу одержувача і адресу відправника.

Мережа Ethernet влаштована так, що при попаданні кадру в середу передачі даних, що розділяється всі мережеві адаптери одночасно починають приймати цей кадр. Всі вони аналізують адресу призначення, розташовану в

одному з початкових полів кадру, і, якщо ця адреса співпадає з їх власною адресою, кадр вміщується у внутрішній буфер мережевого адаптера. Таким чином комп'ютер-адресат отримує призначені йому дані.

Іноді може виникати ситуація, коли одночасно два або більше за комп'ютер вирішують, що мережа вільна, і починають передавати інформацію. Така ситуація, звана колізією, перешкоджає правильній передачі даних по мережі. У стандарті Ethernet передбачений алгоритм виявлення і коректної обробки колізій. Імовірність виникнення колізії залежить від інтенсивності мережевого трафіка.

Після виявлення колізії мережеві адаптери, які намагалися передати свої кадри, припиняють передачу і після паузи випадкової тривалості намагаються знов отримати доступ до середи і передати той кадр, який викликав колізію.

Головним достоїнством мереж Ethernet, завдяки якому вони стали такою популярною, є їх економічність. Для побудови мережі досить мати по одному мережевому адаптеру для кожного комп'ютера плюс один фізичний сегмент коаксіального кабелю потрібної довжини. Інші базові технології, наприклад Token Ring, для створення навіть невеликої мережі вимагають наявності додаткового пристрою концентратора.

Крім того, в мережах Ethernet реалізовані досить прості алгоритми доступу до середи, адресації і передачі даних. Простота логіки роботи мережі веде до спрощення і,

відповідно, здешевлення мережевих адаптерів і їх драйверів. По тій же причині адаптери мережі Ethernet мають високу надійністю. І нарешті, ще однією чудовою властивістю мереж Ethernet є їх хороша розширюваність, тобто легкість підключення нових вузлів.

Інші базові мережеві технології Token Ring, FDDI, 100VGAny-LAN, хоч і володіють багатьма індивідуальними рисами, в той же час мають багато загальних властивостей з Ethernet. Насамперед це застосування регулярних фіксованих топологій (ієрархічна зірка і кільце), а також серед передачі даних, що розділяються. Істотні відмінності однієї технології від іншої пов'язані з особливостями методу доступу, що використовується до середи, що розділяється. Так, відмінності технології Ethernet від технології Token Ring багато в чому визначаються специфікою закладених в них методів розділення середи випадкового алгоритму доступу в Ethernet і методу доступу шляхом передачі маркера в Token Ring.

2. Комп'ютерні віруси і шкідливі програми.

Комп'ютерним вірусом називається програма (деяка сукупність виконуваного коду/інструкцій), що здатна створювати свої копії (не обов'язково цілком співпадаючі з оригіналом) і впроваджувати їх у різні об'єкти/ресурси комп'ютерних систем, мереж і т.д. без ведена користувача. При цьому копії зберігають здатність подальшого поширення.

Із збільшенням кількості людей, що користуються комп'ютером, і можливостей обміну між ними даними по електронній пошті і через інтернет зросла загроза зараження комп'ютера вірусами, а також псування або розкрадання інформації іншими шкідливими програмами.

Щоб знати, якого роду небезпеки можуть загрожувати вашим даним, корисно взна-ти, які бувають шкідливі програми і як вони працюють. В цілому шкідливі програми можна розділити на наступні три класи: Щоб знати, якого роду небезпека може загрожу-вати вашим даним, корисно взнати, які бувають шкідливі програми і як вони працюють.

В цілому шкідливі програми можна розділити на наступні три класи:

Черв'яки - дана категорія шкідливих програм для розповсюдження використовує мережні ресурси. Назва цього класу була дана виходячи із здатності черв'яків "переповзати" з комп'ютера на комп'ютер, використовую-чи мережі, електронну пошту і інші інформаційні канали. Також завдяки цьому черв'яки володіють виключно високою швидкістю розповсюдження.

Черв'яки проникають на комп'ютер, вичисляють мережні адреси інших комп'юте-рів і розсилають за цими адресами свої копії. Крім мережних адрес часто вико-ристовуються дані адресної книги поштових клієнтів. Представники цього класу шкідливих програм іноді створюють робочі файли на дисках системи, але можуть взагалі не звертатися до ресурсів комп'ютера (за винятком оперативної пам'яті).

Віруси - програми, які заражають інші програми - додають в них свій код, щоб отримати управління при запуску заражених файлів. Це просте визначення дає можливість виявити основну дію, виконувану вірусом - *зараження*.

Швидкість розповсюдження вірусів дещо нижче, ніж у черв'яків.
Троянські програми - програми, які виконують на комп'ютерах несанкціоновані користувачем дії, тобто залежно від деяких умов знищують інформацію на дисках, приводять систему до "зависання", крадуть конфі-денційну інформацію і т.д. Даний клас шкідливих програм не є вірусом в традиційному розумінні цього терміну (тобто не заражає інші програми або дані); троянські програми не здатні самостійно проникати на комп'ютери і розповсюджуються зловмисниками під виглядом "корисного програмного забезпечення". При цьому шкода, що наноситься ними, може у багато разів перевищувати втрати від традиційної вірусної атаки.

Останнім часом найпоширенішими типами шкідливих програм, що псують комп'ю-терні дані, стали черв'яки. Далі по поширеності слідують віруси і троянські програми. Деякі шкідливі програми суміщають в собі характеристики двох або навіть трьох з перерахованих вище класів.

Основними джерелами розповсюдження шкідливих програм є електронна пошта і інтернет, хоча зараження може також відбутися через дискету або CD-диск. Ця обстави-на зумовлює зсув акцентів антивірусного захисту з простих регулярних перевірок комп'ютера на присутність вірусів на складнішу задачу постійного захисту комп'ютера від можливого зараження.

Далі як позначення вірусів, троянських програм і черв'яків ми використовуватимемо термін "вірус". Акцент на конкретний вид шкідливої програми робитиметься тільки у разі коли це необхідне.

Антивірус Касперського призначений для антивірусного захисту персональних комп'ютерів, що працюють під керуванням операційної системи Windows. Ця програма є детектором та фагом одночасно і призначена для виявлення і лікування програм, які заражені відомими типами вірусів. Крім того програма містить евристичний аналізатор, який, базуючись на загальних відомостях про характерис-тики та властивості вірусів, дозволяє інколи знаходити нові, невідомі їй екземпляри.

Захист від вірусів і шкідливих програм - виявлення і знищення шкідливих програм, що проникають через змінні і постійні файлові носії, електронну пошту і протоколи Інтернету. Можна виділити наступні варіанти роботи програми (вони можуть використовуватися як окремо, так і в сукупності):
Постійний захист комп'ютера - перевірка всіх об'єктів що запус-каються і відкриваються, і об’єктів, що зберігаються на комп'ютері, на присутність вірусів.
Перевірка комп'ютера за вимогою - перевірка і лікування як усього комп'ютера в цілому, так і окремих дисків, файлів або каталогів. Таку перевірку ви можете запускати самостійно або настроїти її регулярний автоматичний запуск.
Відновлення працездатності після вірусної атаки. Повна перевірка і лікування з рекомендованими експертами Лабораторії Касперського настройками дозволяє вам видалити усі віруси, що вразили ваші дані при вірусній атаці.
Перевірка і лікування вхідної/вихідної пошти - аналіз на присутність вірусів і лікування вхідної пошти до її надходження в поштову скриньку і вихідну пошту в режимі реального часу. Крім того, програма дозволяє

перевіряти і лікувати поштові бази різних поштових клієнтів за вимогою.
Відновлення антивірусних баз і програмних модулів - поповнення антивірусних баз інформацією про нові віруси і способи лікування заражених ними об'єктів, а також відновлення власних модулів програми. Відновлення виконується із серверів відновлень Лабораторії Касперського або з локально-го каталогу.
Рекомендації з настроювання програми і роботі з нею - поради від експертів Лабораторії Касперського, що супроводжують вас у процесі роботи з Антивірусом Касперського , і настроювання, що рекомендуються, відповідному оптимальному антивірусному захистові.

У випадку виявлення заражених або можливо заражених файлів, коли антивірусні бази не обновляються критично довгий термін, або коли давно не проводилася повна перевірка комп'ютера, у головному вікні Антивірусу Касперського завжди можна знайти рекомендації по виконанню тих або інших дій і обґрунтування для їхнього здійснення. Відразу після установки продукту і його запуску набирають сили настроювання антиві-русного захисту, що рекомендуються експертами.
Карантин - поміщення об'єктів, можливо заражених вірусами або їхніми модифікаціями, у спеціальне безпечне сховище, де їх можна лікувати, видаляти, відновлювати у вихідний каталог, а також відправляти експертам Лабораторії Касперського на дослідження. Файли на карантині зберігаються в спеціальному форматі і не представляють небезпеки.
Формування звіту - фіксування всіх результатів роботи Антивірусу Касперського у звіті. Докладний звіт про результати перевірки включає загальну статистику по перевірених об'єктах, зберігає настроювання, з якими була

виконана та або інша задача, а також послідовність перевірки й обробки кожного об'єкта окремо. Звіт формується і за результатами відновлень.

Версія 5.0 Антивірусу Касперського дещо відрізняється від попередньої версії 4.5 наступними задачами:
Ведення інформаційної бази по перевірених об'єктах. Антивірус Касперського тепер не перевіряє повторно ті об'єкти, що були проаналізовані під час попередньої перевірки і з тих пір не змінилися, не тільки при постійному захисті, але і при перевірці за вимогою. Така організація роботи помітно підвищує швидкість роботи програми.
Перевірка і лікування вхідної та вихідної пошти довільної поштової системи, приймаючої пошту по протоколі POP3 і відправляючої поштові повідомлення по протоколі SMTP. У попередній версії антивірусний захист пошти забезпечувався тільки для поштових програм, сумісних з Microsoft Exchange.
Лікування заражених архівів. Антивірус Касперського Personal дозволяє лікувати заражені файли в архівах типів zip, arj, cab, rar. У попередній версії програма дозволяла тільки виявляти заражені файли в архівах і лікувати заражені об'єкти в zip-архівах.
Антивірус Касперського перевіряє архіви, що саморозпаковуються, але не лікує їх.
Простий інтерфейс. Продукт являє собою одну програму, у той час як попередня версія продукту складалася з набору програм, кожна з яких виконувала одну функцію антивірусного захисту. Новий підхід дозволив домогтися простоти в звертанні і керуванні усіма найбільш важливими функціями антивірусу. Тепер, наприклад, можна встановлювати рівень антивірусного захисту не

шляхом редагування настроювань, а використовуючи шкалу рівнів і повзунок.
Рекомендовані настройки и поради експертів. Для спрощення роботи з програмою в даній версії продукту за замовчуванням установлені рекомендовані експертами Лабораторії Касперського настроювання. Немає необхідності настроювати продукт перед його використанням. У ситуаціях, коли антивірусний захист установлений на низькому рівні, програма видає відповідне повідомлення і пропонує різні варіанти підвищення рівня захисту.
Продовження ліцензії на використання продукту. Антивірус Касперського вер-сії 5.0 дозволяє установлювати ліцензійний ключ, продовжувати тим самим ліцензію на використання продукту.
Відправка об’єктів на експертизу в Лабораторію Касперського. В даній версії можна відправляти для дослідження в Лабораторію Касперського можливо заражені об'єкти, виявлені Антивірусом Касперського, а також файли, які є підозрілими на зараження.
Заборонено видалення заражених складених об'єктів. В даній версії не можна видалити заражені складені об'єкти (архіви, поштові бази, файли поштових форматів) за допомогою Антивірусу Касперського. Однак як і раніше можна видалити кожен з їх окремо . Виняток складають архіви, що саморозпаковуються.

Основні задачі розв’язувані за допомогою Антивірусу Касперського:

Автоматичне регульоване оновлення антивірусних баз і програмних модулів через Інтернет.
Повна перевірка комп’ютера.
Перевірка окремих об’єктів.

Перевірка змінних носіїв(дискет, CD-дисків,…)
Перевірка електронної пошти.
Зміна рівнів захисту комп’ютера від вірусів.
Знаходження і лікування відомих типів вірусу.
Виявлення невідомих екземплярів вірусу.
Відправка запитів у Лабораторію Касперського.
Відправка підозрілих файлів і об’єктів у Лабораторію Касперського для аналізу.
Поміщення файлів на карантин, і виймання файлів із карантину.
Перевірка коректності роботи Антивірусу(вірус-тест)
Настройка звукових оформлень.
Відключення і включення перевірки пошти, сценаріїв і інших об’єктів.
Включення і виключення Антивірусу Касперського.
Для нормального функціонування Антивірусу Касперського потрібно щоб апаратне і відповідне програмне забезпечення комп'ютера відповідало перерахованим нижче вимогам.

Загальні вимоги:

МБ вільного місця на жорсткому диску;
CD-ROM-пристрій (для установки Антивірусу Касперського з CD-диска).
Microsoft Internet Explorer версії 5.5 (для відновлення антивірусних баз і програмних модулів через Інтернет)
Windows 98:
процесор Intel Pentium 133 Мгц або вище;
32 МБ оперативної пам'яті.

Windows ME:

- процесор Intel Pentium 150 Мгц або вище;

- 32 МБ оперативної пам'яті.

Windows NT Workstation 4.0 (Service Pack 6a):

- процесор Intel Pentium 133 Мгц або вище;
- 32 МБ оперативної пам'яті.

Windows 2000 Professional (Service Pack 2 або вище):

- процесор Intel Pentium 133 Мгц або вище;
- 64 МБ оперативної пам'яті.

Windows XP Home Edition або XP Professional (Service Pack 1 або вище):

- процесор Intel Pentium 300 Мгц або вище;
- 128 МБ оперативної пам'яті.

2.1. Установка продукту на комп'ютер

Щоб встановити Антивірус Касперського Personal на комп'ютер, на CD-диску з продуктом запускаємо файл kavsetup.exe.

Програма установки працює в діалоговому режимі. Кожне вікно містить набір кнопок для управління процесом установки. Програма установки працює в діалоговому режимі. Кожне вікно містить набір кнопок для управління процесом установки. Стисло пояснимо їх призначення:

Далі > - прийняти дію і перейти до наступного кроку процедури установки.

- < Назад - повернутися на попередній крок установки.
- Відміна - відмовитися від установки продукту.
- Завершити - завершити процедуру установки програми на комп'ютер.

Розглянемо детально кожен крок процедури установки пакету.

Крок 1. Перевірка версії встановленої операційної системи.

Перш ніж приступити до установки програми, на комп'ютері виконується пере-вірка відповідності встановлених операційної системи і Service Pack програмним вимо-гам для установки Антивіруса Касперського Personal.

У випадку якщо який-небудь з тих, що вимагаються Service Pack для операційної системи не встановлений, на екран буде виведене відповідне повідомлення. Встановіть необхідний Service Pack за допомогою сервісу Windows Update, після чого повторіть установку Антивіруса Касперського Personal.

Крок 2. Пошук інших антивірусних програм

Даний крок процедури установки виконується тільки в тому випадку, якщо на вашому комп'ютері встановлене інше антивірусне програмне забезпечення.

Наступний етап попередньої роботи перед установкою програми полягає в пошуку інших встановлених антивірусних продуктів, у тому числі і продуктів Лабо-раторії Касперського, сумісне використовування з якими Антивіруса Касперського Personal може привести до виникнення конфліктів.

При виявленні встановленого на вашому комп'ютері Антивіруса Касперського раніших версій (наприклад, версії 4.5) на екран буде виведене повідомлення, що вима-гає видалення даного програмного забезпечення, оскільки його сумісне використовуван-ня з Антивірусом Касперського Personal 5.0 неможливе.

Натисніть на кнопку ОК і видаліть ранішу версію Антивірусу, після чого знову запустіть файл kavsetup.exe.

При виявленні на комп'ютері встановленого антивірусного програмного забезпе-чення іншого виробника на екран буде виведене повідомлення з рекомендацією видали-ти його, перш ніж встановлювати Антивірус Касперського Personal.

Рекомендуємо перервати процес установки і видалити вказану програму. Для цьо-го натисніть на кнопку Відміна, видаліть вказаний програмний продукт, після чого знову запустите файл kavsetup.exe.

При виявленні на комп'ютері вже встановленого Антивіруса Касперського Personal версії 5.0 на екран буде виведено відповідне повідомлення. Якщо продовжити установку, то дана копія програми видалить встановлену раніше.

Крок 3. Стартове вікно процедури установки.

Якщо на комп'ютері не знайдено інших антивірусних програм, відразу після вико-нання файлу kavsetup.exe на екрані буде відкрите стартове вікно, що містить інформацію про запуск програми установки Антивіруса Касперського Personal на ваш комп'ютер.

Для продовження установки натисніть на кнопку Далі продовження установки натисніть на кнопку Далі >. Відмова від установки продукту виконується по кнопці Відміна.

Крок 4. Проглядання Ліцензійної Угоди.

Наступне вікно програми установки містить Ліцензійну Угоду між користувачем і Лабораторією Касперського. Уважно прочитайте його, і, за умови, згоди зі всіма пунктами Угоди, натискаємо на кнопку Згоден. Процедура установки буде продовжена.

Крок 5. Відомості про користувача.

На даному етапі установки визначаються ім'я користувача і назва організації. За замовчуванням використовуються дані, вказані в реєстрі операційної системи, які можна змінити.

Для продовження установки натисніть на кнопку Далі >.

Крок 6. Прочитання важливої інформації про програму.

На даному етапі установки пропонується ознайомитися з важливою інформацією про програму, перш ніж приступати до роботи з нею.

У даному діалоговому вікні приведені основні можливості Антивірусу Касперського, особливості його роботи і т.д.

Після прочитання інформації натисніть на кнопку Далі >.

Даний крок процедури установки виконується тільки в тому випадку, якщо програма установки Антивірусу Касперського Personal не змогла самостійно знайти ліцензійний ключ!

На цьому кроці установки продукту виконується інсталяція ліцензійного ключа Антивірусу Касперського Personal. Ліцензійний ключ є особистим "ключем" користува-ча, в якому знаходиться службова інформація, необхідна для повнофункціональної роботи програми, а саме:

- інформація про підтримку (хто здійснює і де можна її одержати);
- назва і номер ліцензії, а також дата її закінчення.

Без ліцензійного ключа програма працювати не буде.

У стандартному вікні вибору файлів вкажіть ліцензійний ключ і натискаємо на кнопку Далі > для продовження установки програми.

У випадку якщо на момент установки програми немає ліцензійного ключа (наприклад, ключ замовлений в Лабораторії Касперського по інтернету, але ще не одержаний), можна встановити його пізніше, при першому запуску програми. Пам'ятайте, що без ключа не можна приступити до роботи з Антивірусом Касперського.

Крок 8. Вибір директорії установки.

Наступний етап установки Антивірусу Касперського визначає директорію на комп'ютері, в яку буде встановлений продукт. За замовчуванням заданий шлях: C:\ProgramFiles\Kaspersky Lab\Kaspersky Anti-Virus Personal.

Щоб змінити шлях, натисніть на кнопку Огляд..., в стандартному вікні вибору вкажіть директорію установки продукту і натисніть на кнопку Далі >.

Після цього буде запущена процедура копіювання файлів Антивірусу Касперського Personal на комп'ютер.

Крок 9. Завершення процедури установки.

Вікно Завершення установки містить інформацію про закінчення процесу установки Антивіруса Касперського Personal на комп'ютер.

Щоб завершити установку программи

1. Виберіть один з варіантів завершення роботи:
   Так. Перезавантажити комп'ютер зараз
   Ні. Перезавантажити комп'ютер пізніше
2. Натисніть на кнопку Завершити.

Перш ніж перейти до основних прийомів захисту комп’ютера від вірусів нагадаємо на які типи поділяються антивірусні програми.

Засоби захисту від вірусів поділяються на такі групи, як детектори, фаги, ревізори, охоронці, вакцини.
Детектори (сканери). Їх метою є постановка діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст – “вірусолог”.

Фаги (поліфаги). Програми спроможні найти і знищити вірус (фаги) або декілька вірусів (поліфаги). Сучасні версії, як правило, проводять евристичний аналіз файлів – вони досліджують файли на предмет коду, характерного для віруса.

Ревізори. Цей тип антивірусів контролює всі (відомі на момент випуску програми) можливі способи зараження комп’ютерів. Таким чином, можливо знайти вірус, створений вже після виходу програми-ревізора.

Охоронці. Резидентні програми, постійно знаходяться в пам’яті комп’ютера і контролюють всі операції.

Вакцини. Використовуються для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше). Як відомо, ні один з даних типів антивірусів не забезпечує 100% захисту комп’ютера, і їх бажано використовувати в зв’язку з іншими пакетами. Вибір тільки одного, “найкращого” Антивірусу вкрай помилковий.

2.2.Як захистити від вірусів пошту

Антивірус Касперського дозволяє захистити пошту, що надходить на комп'ютер і виходить з нього, у режимі реального часу.

Щоб захистити від вірусів пошту, досить включити постійний захист і перевірити в Настройці параметрів захисту, що прапорець виключити постійний захист пошти знятий.

Антивірус Касперського користується такими правилами для роботи з поштою:

- Антивірус Касперського захищає від вірусів пошту незалежно від того, який з поштових клієнтів ви використовуєте[1]. Пошта перевіряється в момент її надходження, а також при її відправленні - неважливо, чи відправляєте ви її самостійно чи це намагається зробити якась із програм вашого комп'ютера.
- При виявленні зараженого об'єкта в поштовому повідомленні над ним виконується дія, що рекомендується: Антивірус Касперського намагається лікувати такий об'єкт, а якщо лікування неможливе - видаляє його з пошто-вого повідомлення.
- При роботі з поштою віддалених веб-серверів за допомогою Інтернет-браузера, наприклад, за допомогою Microsoft Internet Explorer, програма буде перевіряти тільки вкладені у вхідні повідомлення файли в момент їхнього запуску або запису на диск.

Поштові бази, перенесені з інших комп'ютерів і не підключені в даний момент, можна перевірити за запитом.

Щоб перевірити поштові скриньки програм Microsoft Outlook або Microsoft Outlook Express, необхідно:

1. Переконатися, що в Настройці параметрів перевірки не встановлений прапорець Не перевіряти поштові скриньки.
2. Скористатися гіперпосиланням Перевірити об'єкти в лівій частині закладки Захист.
3. У відкрившумося вікні Вибір об’єктів для перевірки встановите прапорець е поштові скриньки.
4. Натисніть на кнопку Перевірити.

У цьому випадку на комп'ютері будуть перевірені поштові скриньки Microsoft Outlook, Microsoft Outlook Express.

У результаті обробки поштових баз Microsoft Outlook, Microsoft Outlook Express незалежно від обраної дії над об’єктами завжди змінюється дата і час їхньої модифікації.

Щоб перевірити поштові бази іншої поштової програми (наприклад, The Bat) або бази, принесені, наприклад, з роботи на дискеті, необхідно:

1. Скористайтеся гіперпосиланням Перевірити об'єкти в лівій частині закладки Захист.
2. У вікні, що відкрилося, Вибір об'єктів для перевірки виберіть диск або каталог, на якому зберігаються бази.
3. Натисніть на кнопку Перевірити.

[1]Антивірус Касперського захищає в режимі реального часу всю пошту, що надхо-дить по протоколі POP3 і вихідну по протоколі SMTP.

2.3.Як перевірити окремий об'єкт

Вибрати об'єкт для перевірки можна як за допомогою Антивірусу Касперського, так і стандартними засобами операційної системи Windows (наприклад, у вікні програми Провідник або на Робочому столі і т.д.).

Щоб запустити перевірку об'єкту, вибраного засобами Windows встановлюємо кур-сор миші на імені вибраного об'єкту, правою кнопкою миші відкриваємо контекстне меню Windows і виберіть пункт Перевірити на віруси.

Щоб вибрати об'єкт перевірки за допомогою Антивірусу Касперського,

1. Потрібно скористатися гіперпосиланням Перевірити об'єкти, розташованим в лівій частині закладки Захист. У вікні, що відкрилося Вибір об'єктів для перевірки знаходиться список об'єктів, які можна перевіряти, а також кнопки редагування списку і кнопки управління перевіркою.
2. Виберіть об'єкти, які необхідно перевірити.
3. Якщо потрібно можна додати новий об'єкт в список, натискуючи на кнопку Додати і у вікні проглядання файлів, що відкрилося, вказуючи потрібний файл або каталог.
4. Натискуємо на кнопку Перевірити для запуску перевірки.

Через дискети, CD і інші змінні диски легко заразити комп'ютер вірусом. Якщо дискета (або завантажувальний CD-диск) заражена завантажувальним вірусом, залишена в дисководі і комп'ютер перезавантажили, результати можуть бути самі сумні.

Тому, рекомендовано перевіряти всі змінні диски перед їхнім використанням.

Це можна зробити запустивши перевірку змінних дисків з головного вікна Антивірусу Касперського, а також з контекстного меню Windows, відкритого, наприклад, у вікні програми Провідник, на Робочому столі і т.д.

Для перевірки змінних дисків з контекстного меню Windows, потрібно:
вибрати диски (можна вибрати відразу і CD-диск і дискету), правою кнопкою миші відкриваючи контекстне меню Windows і вибрати пункт Перевірити на віруси.

Щоб перевірити CD-диск або дискету на присутність вірусів з головного вікна Антивірусу Касперського, необхідно:Вставити CD-диск у CD-ROM-пристрій або дискету в дисковод. Програма може перевірити CD-диск і дискету одночасно.

Скористатися гіперпосиланням Перевірити змінні диски, розташованим в лівій частині закладки Захист.

або

По гіперпосиланню Перевірити об'єкти перейти у вікно Вибір об'єктів для перевірки, вибираючи змінні диски і натискаючи на кнопку Перевірити.

Відразу після запуску перевірки на екрані відкриється вікно Перевірка, де буде відображатися процес виконання дії над обраними об'єктами списку.
Якщо для перевірки вибрано тільки один змінний диск (пристрій), тоді по закінченні перевірки Антивірус Касперського запропонує вставити наступний диск (пристрій).
Звернемо увагу на деякі особливості роботи програми:
Якщо диск або дискета не вставлена перед запуском перевірки, або змінний накопичувач, дисковод або CD-

ROM, відключений, перевірка проводитися не буде, і програма не видасть ніякого додаткового повідомлення з цього приводу.

Якщо вставити дискету в дисковод уже після запуску перевірки, вона не буде перевірена. Те ж відноситься до CD-диска й інших знімних дисків.

Якщо вийняти дискету з дисководу або відключили змінний диск під час його перевір-ки, програма занесе в звіт повідомлення про помилку, але не видасть на екран ніякого додаткового повідомлення. Програма перейде до перевірки наступного змінного диска, якщо такий є.

У момент монтування змінного диска в систему (коли диск визначається операцій-ною системою як новий пристрій) Антивірус виконує перевірку такого диска і на присут-ність boot-вірусу.

2.4.Як поводитися з вірусами

Порядок дій Антивірусу Касперського при виявленні зараженого об'єкту, шкідливої програми або об'єкту, можливо зараженого вірусом або його модифікацією, цілком і повністю залежить від заданих настройок постійного захисту і перевірки на вимогу. В даному розділі розглянемо випадки, коли в процесі перевірки Антивірус Касперського пропонує на вибір дії над об'єктом.

Такі ситуації виникають тоді, коли внаслідок дії над об'єктом було вибрано:

- в настройках постійного захисту:

Забороняти доступ і запрошувати дію у користувача

- в настройках перевірки на вимогу: Запрошувати дію у користувача

Отже, при виявленні зараженого об'єкту, шкідливої програми або об'єкту, можливо зараженого вірусом або його модифікацією, на екран виводиться повідомлення, що містить:

- докладний опис об'єкту з вказівкою імені вірусу, яким він можливо заражений або точно заражений, або імені шкідливої програми, якою він є;
- набір дій, які можна виконати над об'єктом. Одна з пропонованих дій завжди є такою, що рекомендується експертами Лабораторії Касперського для обробки об'єкту. Поряд з такою дією вказано слово (рекомендується). На вибір можуть бути запропоновані наступні дії (набір пропонованих дій залежить від виду знайденого об'єкту):

Лікувати - намагатися лікувати заражений об'єкт, якщо його лікування можливо.

Видалити - видалити заражений або можливо заражений об'єкт.

Пропустити - не виконувати над об'єктом ніяких дій, лише зафіксувати інформацію про нього в звіті.

Помістити на карантин - перенести об'єкт, можливо заражений вірусом або його модифікацією, на карантин для подальшої перевірки, відновлення, відправки на

дослідження в Лабораторію Касперського або видалення.

Таку вибрану дію можна застосувати до всіх заражених або можливо заражених об'єктів, встановивши відповідний прапорець. Так, наприклад, щоб застосувати вибрану дію для всіх заражених об'єктів, які програма не може вилікувати, встановіть прапорець

Застосувати до всіх заражених об'єктів, лікування яких неможливе (в рамках даної сесії).

2.5.Постійний захист

Відразу після старту (про що свідчить червоний значок в Системній панелі) Антивірус Касперського перевіряє на присутність вірусів всі об’єкти, виконувані при старті операційної системи, а також пам’ять комп’ютера і власні модулі.

Постійний захист комп'ютера функціонує відповідно до настройок, експертами Лабораторії Касперського, що рекомендуються, а саме:

- на присутність вірусів перевіряються об'єкти , що відкриваються, зберігаються і запускаються, жорсткого і змінних дисків комп'ютера, причому ті з них, які потенційно можуть бути заражені. Перевіряються наступні об'єкти:
  - завантажувальні сектори дисків (дані об'єкти перевіряються відразу після старту програми);
  - запаковані файли і приєднані або вбудовані в інші файли об'єкти (OLE-об’єкти);
  - вхідні поштові повідомлення (по прибуттю).

При постійному захисті не перевіряються ті об'єкти, які явно не можуть містити вірусів.

- при виявленні зараженого об’єкту доступ до нього блокується, і на екран видається запит на його обробку;
- при виявленні об'єкту можливо зараженого вірусом або його модифікацією, програма блокує до нього доступ і видає запит на обробку;
- результати роботи програми фіксуються в звіті.

Постійний захист включений з моменту старту операційної системи і до завершення роботи з комп'ютером.

Можна самостійно відключити постійний захист. Для цього:

- клацнути правою кнопкою миші по значку в Системній панелі;
- в відкрившомуся контекстному меню вибераємо пункт Вимкнути постійний захист.

Постійний захист комп'ютера буде відключений. Свідченням відключення стане перехід значка з активного стану (червоний колір значка) в пасивний (сірий колір значка).

Не рекомендується відключати постійний антивірусний захист, оскільки це значно підвищує ризик зараження комп'ютера вірусами.

2.6.Настройка постійного захисту комп'ютера

Постійний захист комп'ютера означає, що всі потенційно небезпечні з погляду антивірусної безпеки дії відстежуватимуться Антивірусом Касперського. До числа таких дій входить відкриття файлу, збереження зміненого файлу, проглядання тієї, що входить і відправка витікаючої пошти, а також запуск файлів на комп'ютері і сценаріїв в Microsoft Internet Explorer. Коли користувач або якась програма намагається виконати одну з перерахованих дій, Антивірус перехоплює його, перевіряє об'єкт, і, залежно від результатів перевірки, дозволяє або забороняє запрошувану дію, або видає на екран повідомлення.

2.7.**Як перевірити стан захисту**

Інформація про стан постійного захисту знаходиться на правій панелі закладки Захист головного вікна Антивірусу Касперського.
Стан постійного захисту позначається наступними значками:

постійний захист включений, настройки відповідають тим, що рекомендуються;

постійний захист включений, але настройки не відповідають тим, що рекомендуються;

постійний захист відключений або не працює. В першому випадку рекомендується включити постійний захист, а в другому - налаштувати параметри постійного захисту і запустити його.

2.8.**Оновлення антивірусних баз**

Пошук вірусів і лікування заражених об'єктів виконуються на підставі записів антивірусних баз, що містять опис всіх відомих на даний момент шкідливих програм і способів лікування уражених ними об'єктів.

Украй важливо підтримувати бази в актуальному стані, оскільки щодня з'являються нові віруси.

Оновлення антивірусних баз - ще одна важлива функція, виконувана Антивірусом Касперського. За умовчанням бази копіюються з серверів оновлень Лабораторії Касперського і встановлюються на комп'ютері кожні три години. Можна змінити частоту оновлення антивірусних баз, або запускати оновлення самостійно. Можна самостійно відновити антивірусні бази. Для цього:

клацнути правою кнопкою миші по значку в Системній панелі. У відкрившомуся контекстному меню вибрати пункт Відновити антивірусні бази.
або:
відкриваємо закладку Захист головного вікна програми і в лівій її частині скористаємося гіперпосиланням Завантажити оновлення.
або:
в правій частині закладки Захист скористайтеся гіперпосиланням відновити антивірусні бази.

	Збільшення розміру пам’яті
	Уповільнення роботи комп’ютера
	Затримки при виконанні програм
	Незрозумілі зміни в файлах
	Зміна дати модифікації файлів без причини
	Незрозумілі помилки Write-protection
	Помилки при інсталяції і запуску WINDOWS
	Відключення 32-розрядного допуску до диску
	Неспроможність зберігати документи Word в інші каталоги, крім TEMPLATE
0	Погана робота дисків

2.9.Ознаки зараження вірусом

Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити такі зміни :

1	Зникнення файлів
2	Форматування HDD
3	Неспроможність завантажити комп’ютер
4	Неспроможність завантажити файли
5	Незрозумілі системні повідомлення, музикальні ефекти і т.д.

2.10. Типи антивірусів

Засоби захисту від вірусів поділяються на такі групи, як детектори, фаги, ревізори, охоронці, вакцини.

Детектори (сканери). Їх метою є постановка діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст – “вірусолог”.

Фаги (поліфаги). Програми спроможні знайти і знищити вірус (фаги) або декілька вірусів (поліфаги). Сучасні версії, як правило, проводять евристичний аналіз файлів – вони досліджують файли на предмет коду, характерного для вірусу.

Ревізори. Цей тип антивірусів контролює всі (відомі на момент випуску програми) можливі способи зараження комп'ютерів. Таким чином, можливо знайти вірус, створений вже після виходу програми-ревізора.

Охоронці. Резидентні програми, постійно знаходяться в пам'яті комп'ютера і контролюють всі операції.

Вакцини. Використовуються для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше). Як відомо, ні один з даних типів антивірусів не забезпечує 100% захисту комп'ютера, і їх бажано використовувати в зв'язку з іншими пакетами. Вибір тільки одного, "найкращого" антивірусу вкрай помилковий.

Тепер про деякі характеристики антивірусних пакетів. Перше, на що треба звернути увагу, це кількість розпізнаваючих сигнатур – послідовність символів, гарантовано виявляючих вірус. Треба помітити, що виробники використовують різні системи підрахунку сигнатур : якщо в одних різні версії або близькі по

характеристиках версії вірусів рахуються за одну сигнатуру, то другі підраховують всі варіації. Найкращі із пакетів розпізнають біля 10 тисяч вірусів, що декілька менше загального числа існуючих сьогодні шкідливих програм. Другий параметр – наявність евристичного аналізатора невідомих вірусів, його присутність дуже корисна, але суттєво уповільнює час роботи програми.

Спробуємо розібратися з кращими антивірусами, котрі на даний момент найбільш поширені на українському ринку та в мережі INTERNET. Мова піде про комплексні антивірусні пакети, які забезпечують максимальний рівень захисту вашої інформації.

Серед російських розробників найбільш відомими є комплект від «Лабораторії Касперського» і «Др. Веб». Почнемо з продуктів «Лабораторії Касперського», оскільки ці програми вже стали деяким стандартом, і подавляюча більшість комп'ютерів в нашій країні укомплектовано саме їх антивірусами.

3.Компютерна безпека

Мережа і забезпечення її безпеки вимагає не тільки постійної роботи, але і особливої уваги, яку слід приділяти дрібницям. В той час, коли погроз немає і вся система працює в штатному режимі, постійна робота з мережею включає прогнозування можливих ходів недоброзичливців, формування і створення різних мерів захисту, і, що важливо, - навчання користувачів, яке повинне здійснюватися постійно.

В тому випадку, якщо вторгнення в систему недоброзичливців відбулося, то системний адміністратор, що відповідає за безпеку, повинен виявити «слабку ланку» системи захисту, а так само визначити причину проникнення і те, яким чином це відбулося. Для формування політики безпеки першою дією, яку повинен зробити адміністратор, буде так звана інвентаризація наявних ресурсів, які і мають бути захищені. Фахівець здійснює ідентифікацію всіх користувачів мережі,

організовує їм доступ до наявних ресурсів, а так само аналізує можливі джерела небезпеки, які загрожують кожному з наявних ресурсів. Оперуючи всією зібраною інформацією, стає можливим починати створення політики безпеки, дотримувати яку зобов'язані всі користувачі без виключення.

Варто підкреслити, що політика безпеки мережі не є набором простих правил, які так чи інакше можуть бути всім зрозумілі. Безпека подібного рівня повинна мати форму повноцінного друкарського документа зі всіма необхідними особливостями і нюансами. А для того, щоб кожен з користувачів не забував про складене зведення правил політики безпеки, необхідне що б вони завжди були, що називається, на вигляді. Наприклад, можна розіслати копії складених правил безпеки по всіх призначених для користувача робочих місцях офісу.

Потрібний за якістю рівень безпеки мережі обов'язково повинен включати наступні аспекти:

* ризик і його оцінка. Простіше кажучи - виявлення предмету захисту (що захищаємо і від кого). Цей аспект має на увазі виявлення цінностей, розташованих в мережі і знаходження потенційних джерел риски;

* відповідальність. Всі рішення по ухваленню тих або інших дій стосовно політики безпеки (будь то нові облікові записи, або виявлення порушників) повинні здійснюватися

відповідальними особами, яких і необхідно вказати;

* мережеві ресурси і правила їх використання. У зведенні правил політики безпеки обов'язково мають бути присутніми (у очевидній формі) пояснення, які б показали користувачеві, що він має права робити, а що ні. Наприклад, використання ресурсів мережі в особистих цілях і вживання інформації не за призначенням - не допускається;

* аспекти юридичного характеру. Необхідно заручитися підтримкою грамотного юриста, яка б дозволила відповісти на всі питання про інформацію, що зберігається або оброблюваній в мережі. Всі отримані відомості обов'язково мають бути включені в документи про політику безпеки мережі;

* відновлення системи безпеки і всі супутні процедури. Слід точно позначити дії, які мають бути прийняті у разі порушення системи захисту. Плюс до цього мають бути визначені заходи, які будуть прийняті на аресу тих, хто став винуватцем порушення, що відбулося.

3.1. Види вторгнення. Класифікація

Залежно від мети вторгнення, існує можливість визначити їх класи, які діляться на п'ять основних типів:

* апаратні засоби. Сервери, робочі станції, периферійні пристрої (принтери, сканери), мережеві кабелі і різноманітні дискові накопичувачі. У тому числі і мережеве устаткування: комутатори, маршрутизатори, мости;

* програмне забезпечення. То або інше програмне забезпечення, встановлене на будь-якому з комп'ютерів, який включений в мережу, може стати можливим «ключем» для проникнення недоброзичливця. І не має значення, чи куплені ці програми у сторонніх розробників, або створені власним IT-відділом. Важливо відзначити, що операційні системи, що є базою для роботи всіх необхідних програмних продуктів, потребують регулярного оновлення (установка «патчів»);

* інформація. Найважливішою цінністю володіють дані, операція якими відбувається в комп'ютерній мережі. Якщо будь-яке програмне забезпечення і самі операційні системи можна відновити (або переустановити), то цілісність даних,

як правило, не підлягає відновленню. Наприклад, список клієнтів, що потрапив до рук недоброзичливців, може вилитися в справжню катастрофу для всього бізнесу;

* люди. Користувачі, що працюють в єдиній мережі, завжди знаходяться в зоні риски. Про це варто пам'ятати завжди;

* документи. Статистика показує, що різні паролі, дані і зачую конфіденційну інформацію дуже часто переносять на паперовий носій (роздрук, записи на листах паперу і багато що інше). І, як правило, рано чи пізно вся подібна «паперова» інформація потрапляє в сміття і просто викидається. Недоброзичливець може цим скористатися і оволодіти закритою для нього інформацією. Слід знати, що будь-які паперові носії, перш ніж бути викинуті, мають бути знищені. Наприклад, за допомогою спеціального утилізатора паперу.

Політика безпеки, яку дійсно можна назвати хорошою і ефективною, винна, перш за все, бути зрозуміла всім користувачам. Проте, не все так просто, адже далеко не всі можуть все зрозуміти досконально. Для вирішення цієї проблеми рекомендується проводити постійні повторні ознайомлення робочого персоналу з наявною політикою

безпеки. Це може бути виконано не тільки на спеціальних інструктажах, але і безпосередньо на самому робочому місці. І найголовніше - не розцінювати подібні дії як просту формальність. Користувачі повинні розуміти всю узяту на себе відповідальності і сприяти збереженню інформації.

3.2. Безпека з фізичної точки зору

Несанкціонований доступ, а точніше його запобігання - це, перш за все, фізичне блокування доступу до мережі, що захищається. Плюс позбавлення доступу до комп'ютерів і серверів мережі, кабелів повідомлень і різних периферійних пристроїв. У тому випадку, коли мережа і підключення до неї виходять за рамки контрольованої зони (наприклад, вихід в інтернет через провайдера), необхідні особливі заходи, такі як організація віртуальних тунелів або шифрування. На додаток до цього, все устаткування, яке так чи інакше бере участь в обміні даними, повинне завжди знаходитися під контролем.

Банальним, але в той же час надзвичайним дієвим

засобом подібного контролю може стати надійний дверний замок. Всі сервери і сховища даних повинні знаходитися в закритих приміщеннях. У них повинні мати доступ тільки компетентні особи із строгим рівнем допуску. Подібними заходами захисту мають бути забезпечені і пристрої функціонування мережі (концентратори, маршрутизатори і інші пристрої). Всі комп'ютери повинні знаходитися в приміщеннях, що закриваються на замок, за якими здійснюватиметься спостереження. Існує багато способів організації контролю і спостереження за приміщеннями, наприклад - реєстраційний журнал і вказівка в нім всіх відвідувачів. Різні резервні копії даних, розміщені на носіях (лазерні диски, стрічки, касети), повинні зберігатися в закритих місцях без загального доступу, наприклад - в сейфах.

3.3. **Застарілі комп'ютери і їх утилізація**

Достатньо часто парку обчислювальної техніки може потрібно комп'ютерна допомога. Ремонт, відновлення і багато інших операцій повинні проводитися тільки компетентними фахівцями. Проте, не рідкісні і ті випадки,

коли необхідна модернізація устаткування (комп'ютери, сервери, сховища даних), або ж повна заміна застарілої техніки на нову. Все «списане» устаткування, як правило, передається в користування стороннім організаціям (комп'ютерні клуби, школи і інше). Будь-яка політика безпеки, організована на підприємстві або організації, повинна містити жорсткі правила по знищенню даних, які раніше або зараз представляють конфіденційність. Зрозуміло, подібні дії мають бути проведені зі всіма жорсткими дисками і іншими накопичувачами інформації списуваної техніки, щоб виключити ризик розповсюдження конфіденційної інформації. Так само мають бути описані алгоритми утилізації носіїв інформації з резервними копіями важливих даних. У багатьох випадках буде незамінна процедура фізичного знищення подібних носіїв. Це буде хорошим гарантом, який повністю виключить «просочування» конфіденційної інформації.

3.4.**Програмний доступ до інформації**

Окрім фізичного обмеження доступу до мережі слід прийняти заходи по програмному обмеженню. Проте, як

показує статистика, як би добре не була побудована система подібного обмеження, завжди відшукається людина, яка буде здатна її обійти. Отже, необхідно мати засоби контролю і спостереження за всіма подіями, що відбуваються в мережі і, у разі потреби, зуміти визначити вторгнення і його глибину.

Мають місце декілька алгоритмів управління мережевим доступом:

* захист ресурсів;

* ідентифікація на фізичному рівні;

* паролі і облікові записи користувачів.

Такий елемент як володіння ресурсами в багатьох операційних системах є ключовою ланкою політики безпеки. Так, наприклад, серверні операційні системи від компанії Microsoft (Windows 200/2003) мають інструменти по відстежуванню дій користувачів, які контактують з тими або іншими ресурсами (наприклад, файли). Творці файлів мають безліч засобів вплинути на їх захист: обмежити доступ, заборонити його і багато що інше. Операційні системи Unix/linux так само мають подібні інструменти, хоч і відрізняються ними від MS Windows.

3.5. **Користувачі і їх ідентифікація**

В тому випадку, якщо які-небудь особливо секретні дані не зберігаються в мережі, то для їх доступу, а так само для доступу до інших ресурсів достатньо лише логіна і пароля. Подібна система проста і у багатьох випадках є оптимальним рішенням. Операційні системи Windows 2000/2003/xp дозволяють створювати так звані домени, які є відособленими зонами управління зі встановленим рівнем захисту. Системний адміністратор може дуже гнучко управляти правами доступу домена, вирішуючи або забороняючи доступ конкретним користувачам не тільки на рядові обчислювальні машини, але і на сервер (сервери). Так само, можливі і такі дії, як довірчі стосунки між декількома доменами, де системні адміністратори можуть вирішити доступ для користувачів до ресурсів інших доменів. Подібні дії вимагають дозволів на рівні облікових записів і співпраці відповідальних осіб (системних адміністраторів). Серверні операційні системи Microsoft (Windows 200/2003 і пізніші) підтримують групові політики безпеки, що надзвичайно ефективно дозволяє

оперувати правами доступу до важливих ресурсів.

3.6. **Для вирішення подібних завдань в Novell Netware**

використовується спеціальна служба Novel Directory Services. Кожен користувач отримує унікальне реєстраційне мережеве ім'я і представляється в певному каталозі об'єктом User. У даному об'єкті розташовується все інформація про користувача, будь то логін, з'єднання і інше.

Unix і подібні операційні системи не містять в своїй структурі доменних систем. Замість цього, кожен хост системи містить так званий файл паролів, де присутня інформація про всіх користувачів, у тому числі і їх паролі в зашифрованому вигляді. Так, наприклад, для доступу до інших мережевих ресурсів, користувач Unix повинен використовувати проксі, або ж пройти реєстрацію на комп'ютері іншої частини мережі, що відноситься до необхідних ресурсів. Варто пам'ятати, що такі мережеві утиліти, як FTP і Telnet можуть пересилати ідентифікаційну інформацію користувачів відкритим текстом без якого-небудь шифрування, а значить - можуть стати об'єктом уваги для недоброзичливців.

Звичайні мережеві операції (друк файлів, їх копіювання),

а так само реєстрація на якій-небудь видаленій системі в операційній системі Unix виконується утилітами видаленої роботи. Зазвичай, вони називаються «r-командами», де їх імена завжди починаються з букви «r».

Утиліти подібного класу надзвичайно ефективні в мережевому середовищі, якщо одному користувачеві доводиться здійснювати роботу на декількох обчислювальних машинах мережі. Проте, враховуючи той факт, що для виконання тієї або іншої команди на видаленому комп'ютері користувачеві цілком досить мати обліковий запис, то це може викликати проблеми із загальною безпекою системи.

Файл /etc/hosts.equiv, або ж .rhosts, а точніше запис в нім визначає права доступу. Комп'ютер, до якого виконується видалене підключення, «довіряє» тому комп'ютеру з якого виконується r-команда. Якщо комп'ютер знаходить відповідний запис в даному файлі, то вирішує доступ до запрошуваних ресурсів. Кожен із записів файлу /etc/hosts.equiv дозволяє ідентифікувати користувача, оскільки містить його ім'я і хост, які мають повноваження на виконання необхідної команди. Саме з цієї причини зовсім не обов'язковий пароль. Простіше кажучи, якщо

користувач має реєстрацію на видаленому комп'ютері, то аутентифікація їм вже пройдена. Файл .rhosts розташовується в «домашньому» каталозі користувача і має такий самий алгоритм роботи. Вся робота видалених користувачів (їх доступ і права) грунтуються на записах наявних в цьому файлі.

В наші дні, в операційних системах Unix і Linux з'явилися спеціальні утиліти Secure Shell (утиліти захисної оболонки), які хоч і схожі по своєму дії з r-командами, але відрізняються від них наявністю шифрування і спеціальними алгоритмами аутентифікації.

Дані алгоритми безпеки системи мають схожість з довірчими стосунками, реалізованими в Windows Nt/2000/server 2003/xp, проте механіка їх роботи все ж таки різна. Так, наприклад, в системі Unix/linux недоброзичливець достатньо легко може представитися видаленим комп'ютером і за допомогою r-команд дістати доступ до інформації, що захищається.

На серверах Windows здійснюються різноманітні фонові процеси, які виконують строго певні функції. Вони називаються службами. Операційні системи Unix так само мають схожі інструменти, які виконують подібну роботу і

називаються «демонами». Всі дані процеси, як правило, виконуються автоматично і без інформування про це користувача. В деяких випадках вони можуть стати винуватцями порушень системи захисту.

Слідує чітко знати всі основні фонові процеси операційних систем і уміти оперувати з ними. Так, наприклад, в системах Unix існують певні демони, які так чи інакше стосуються роботи мережевих протоколів Tcp/ip. Можливі такі випадки, коли вони можуть негативно позначитися на безпеці всієї системи. Їх можна відключити і тим самим вирішити багато проблем.

Наприклад, служба tftp є спрощеною моделлю FTP. Дана спрощена служба відрізняється своєю компактністю і легкістю реалізації в апаратних засобах комп'ютера (перепрограмований ПЗП). У багатьох випадках використання цієї служби достатнє ефективно, але ця служба не має доступу до механіки (в порівнянні з FTP), що управляє, і не оперує обліковими даними користувача (логін і пароль). Враховуючи, що аутентифікації як такий немає, можуть виникнути серйозні проблеми з безпекою всієї системи.

Сервери, що працюють під управлінням операційних

систем Windows, мають в своєму розпорядженні дві утиліти з набору Resource Kit, які дозволяють запускати практично будь-які програми у фоновому режимі. Одна з них - це INSTRV.EXE, яка встановлює виконувані програми. А друга - SRVANY.EXE, яка перетворює необхідну програму на службу.

Слід зазначити, що окрім технічного обслуговування обчислювальної техніки, будь то ремонт комп'ютерів і їх своєчасна модернізація, слід розробити чітку концепцію корпоративної безпеки.

3.7.Корпоративна безпека і її елементи. Зразок

Основна мета: забезпечити надійні гарантії по правильному використанню обчислювальною технікою і телекомунікаційних ресурсів «Компанії» штатом її співробітників і іншими користувачами.

Всі користувачі зобов'язані оперувати обчислювальним засобам з урахуванням всіх норм і правил, і тим самим здійснювати на ній ефективну роботу. Дана політика безпеки стосується всіх користувачів обчислювальних машин, телекомунікаційних ресурсів і служб. Порушення політики безпеки може стати причиною дисциплінарної дії,

звільнення і/або порушення кримінальної справи. В міру необхідності дана політика безпеки може видозмінюватися і переглядатися. Перевірку комп'ютерної системи мають право здійснювати керівники компанії. Під їх компетентність потрапляє електронна пошта і багато інших інтерфейсів обміну даними. Подібна перевірка здійснюється з метою гарантувати повне дотримання всіх норм встановленої політики безпеки. Телекомунікаційна і обчислювальна системи є власністю Компанії і можуть бути використані тільки у вирішенні строго робочих завдань. Штат співробітників Компанії не повинен розраховувати на конфіденційність тієї інформації, яку вони створюють, відправляють або отримують за допомогою обчислювальних і комунікаційних засобів, що належать Компанії. Всім користувачам комп'ютерів Компанії належить керуватися приведеними нижче заходами безпеки і правилами, які стосуються обчислювальної техніки і телекомунікаційних ресурсів. Всі програмні ліцензії мають бути строго дотримані користувачами. Мають бути враховані авторські права і закони, що підкріплюють інтелектуальну власність. Будь-яку інформацію, що є невірною, непристойною,

образливою, загрозливою або протизаконною, забороняється зберігати, отримувати або передавати за допомогою електронних ліній зв'язку (будь то електронна пошта або багато що інше), що належать Компанії. Будь-яка інформація, створена на комп'ютерах Компанії, будь то файли або листи електронної пошти, може бути проаналізована і вивчена керівниками Компанії. Програмне забезпечення, яке не отримало дозвіл на установку у системного адміністратора, не може бути встановлене на комп'ютери Компанії. Забороняється пересилка будь-якої інформації, без дозволу на те її власників. Будь-яка електронна кореспонденція від юриста Компанії або адвоката, що представляє її, повинна містити на кожній сторінці (у колонтитулі) позначку: "Захищено адвокатським правом/без дозволи не пересилати". Користувачі не мають права змінювати або копіювати яку-небудь інформацію (без відповідного не те дозволи), що належить іншим користувачам. Без особливого попереднього дозволу забороняється зберігати на комп'ютерах Компанії яку-небудь сторонню комерційну інформацію, будь то оголошення, рекламні матеріали і так далі. Так само, забороняється зберігання і пересилка

шкідливих програм - вірусів. Користувач несе відповідальність за власний обліковий запис і інформацію, що ідентифікує його (наприклад, особистий пароль на вхід в систему). Так само, забороняється роздруковувати подібну інформацію паперові носії і зберігати її в загальних мережевих ресурсах. Можливість входу в інші комп'ютерні мережі не дає користувачам права на підключення і взаємодію з цими мережами без наявності відповідного на те дозволу адміністратора.

Літературні джерела

1.Саєнко Г.В., Волобуєва Т.Б. Курс користувачів персональним комп’ютером. 1994-207с.

2. Журнал “Компьютерное Обозрение” №35(108) за 10 жовтня 1997 р. 108с.

3. Руденко В.Д.,Макарчук О.М. , Патланжоглу М.О. Практичний курс інформатики., 2003.-325с.

4. Саєнко Г.В., Волобуєва Т.Б. Курс користувачів персональним комп’ютером.. 2006 р.С.-275с.

5. Руденко В.Д.,Макарчук О.М. , Патланжоглу М.О.

Практичний курс інформатики, 2005-127с.

6. Караванова Т. П. Розвиток творчості учнів при вивченні інформатики: Авторська програма поглибленого вивчення інформатики.—Чернівці: ОНМІПО, 2006.—44с.

7. Рудненко В.Д., Макарчук О.М., Патланжоглу М.О. Практичний курс інформатики / За ред. Мадзігона В.М. - К.:Фенікс, 2007. -304 с.

8. Глушаков С.В. Персональний комп'ютер. Навчальний курс.-Харків:Фомо; М.:ООО. Фирма "Издательство Аст", 2004.-499с.

9. Гордієнко Г.В. Входження України у всесвітню систему інформації. // Нова політика. - 1999 р. - №5 – С. 64-67.

10. Демінський С.О. Гроші в Мережі. // Політика і культура. - 2001. - №5 (88) / 13-19 лютого. - С. 34-36.

11.Демонополізація “Інтернету”. // Молода дипломатія. - 2000. - №4 (18). – 17 с.

Інформаційна тривога. // Пробудись. - 1998. - 8 січня. – С. 3-12.

12. http//www.ifcity.info.

13. http//w3c.org.

Боровий Микола Миколайович

Спеціаліст системотехнік, магістрант інформаційних технологій ,ІН-11М

Технології комп’ютерної безпеки

Книга 6

Комп’ютерний набір,верстка і макетування та дизайн в редакторі Microsoft®Office®Word 2007 М.М.Боровий.
Науковий керівник Р.М. Літнарович, доцент,кандидат технічних наук

Міжнародний Економіко-Гуманітарний Університет ім. акад.. Степана Дем’янчука

Кафедра математичного моделювання

33027, м.Рівне, Україна

Вул.акад. С.Дем’янчука,4, корпус 1

Телефон:(+00380)362 23-73-09

Факс:(+00380)362 23-01-86

E-Mail:mail@regi.rovno.ua

E-Mail:mukola-90@mail.ru