Державна академія статистики,
обліку та аудиту
Д А С О А

В. М. Ахрамович

Інформаційна безпека

Навчальний посібник

Київ – 2009

Державна Академія статистики, обліку та аудиту

Д А С О А

В.М. Ахрамович
Інформаційна безпека

Навчальний посібник

Київ 2009

ББК 32. 884
С59

Рецензенти: В.Б. Зваридчук, канд. фізико-мат. наук, доц.
Г.І. Пітомець, канд. тех. наук, доц.
О.В. Мукан, канд. тех. наук, доц.

Схвалено Вченою радою Державної Академії статистики обліку та аудиту. (протокол № 7 від 26 лютого 2009 р.).

Ахрамович В.М.
С59
Навчальний посібник. ***Інформаційна безпека***-- К.: ДАСОА, 2008.-- 324 с.: іл. – Бібліограф.: 321с.

ISBN 5-89173-079-0

У навчальному посібнику викладено теоретичні та практичні аспекти захисту інформації, комп'ютерних мереж, інформаційних систем. Висвітлена можливість захисту вказаних компонентів за допомогою: криптографічних засобів захисту, мережевих екранів, операційних систем Windows, у програмах пакету Wicrosoft Office, систем видалення та відновлення даних, систем резервування даних, захист від впливу комп'ютерних вірусів. Показані можливі канали витоку інформації.

Для студентів різних спеціальностей, які вивчають курс «Інформаційна безпека», «Захист інформації», «Комп'ютерна безпека», «Технології захисту інформації», «Комп'ютерна вірусологія» і т.п.

ББК 32. 884

ISBN 5-89173-079-0

Зміст

По-справжньому захищеною можна вважати лише систему,
яка вимкнена, замурована в бетонний корпус, замкнута в приміщенні
зі свинцевими стінами і охороняється озброєним караулом,
- але і в цьому випадку сумніви не залишають мене".
Юджін Х. Спаффорд

Вступ

Народне прислів'я: «Хто володіє інформацією, той володіє світом» з'явилося в давні часи і відображає об'єктивний стан речей. Недаремно листування сильних світу цього відвіку була об'єктом пильної уваги їх недругів і друзів. Тоді-то і виникло завдання захисту цього листування від надмірно цікавих очей. Стародавні намагалися використовувати для вирішення цього завдання найрізноманітніші методи, і одним з них був тайнопис – уміння складати повідомлення так, щоб його сенс був недоступний нікому окрім присвячених у таємницю. Є свідоцтва тому, що мистецтво тайнопису зародилося ще в доантичні часи. Впродовж всієї своєї багатовікової історії, аж до зовсім недавнього часу, це мистецтво служило небагато ніж, в основному верхівці суспільства, не виходячи за межі резиденцій розділів держав, посольств і – звичайно, ж – розвідувальних місій. Дане питання особливо загострилося в роки світових воєн 20-століття, коли усе змінилося корінним чином – інформація придбала самостійну комерційну цінність і стала широко поширеною, майже звичайним товаром. Її проводять, зберігають, транспортують, продають і купують, а значить – крадуть і підроблюють – і, отже, її необхідно захищати.

Інформаційно-комунікаційні технології є одним з найважливіших факторів, котрі впливають на формування суспільства XXI століття. Їх революційний вплив стосується способу життя людей, освіти і роботи. Інформаційні технології стали життєво важливим стимулом розвитку світової економіки, вони дають можливість ефективно і творчо вирішувати економічні і соціальні проблеми. Людство вступило в нову епоху – епоху інформаційного суспільства. Підраховано, що для збільшення матеріального виробництва в два рази необхідне чотирикратне зростання обсягу інформації, що його забезпечує. Ще два десятиліття тому обсяг наукової інформації, необхідної для вирішення технологічних і соціальних проблем, подвою-

вався кожні сім років, а з 1995 року таке подвоєння відбувається кожні один-два роки.

У таких умовах інформація, яка забезпечує життєво й історично важливі напрямки діяльності людини, перетворюється в цінний продукт і основний товар, вартість якого поступово наближається до вартості продуктів матеріального виробництва, що робить її (інформацію) об'єктом інтересів самого різного характеру (комерційного, соціального, кримінального й ін.). Одним словом, виникнення індустрії обробки інформації із залізною необхідністю привело до виникнення індустрії засобів захисту інформації.

Об'єктами посягань можуть бути самі технічні засоби (комп'ютери і периферія) як матеріальні об'єкти, програмне забезпечення і бази даних, для яких технічні засоби є оточенням.

У цьому сенсі комп'ютер може виступати і як предмет посягань, і як інструмент. Можливе об'єднання вказаних понять, коли комп'ютер одночасно і інструмент і предмет. Зокрема, до цієї ситуації відноситься факт розкрадання машинної інформації, видалення її, порушення нормального процесу функціонування ЕОМ, мереж. Якщо це пов'язане з втратою матеріальних і фінансових цінностей, то цей факт можна кваліфікувати як злочин. Також якщо з даним фактом зв'язуються порушення інтересів національної безпеки, авторства, то кримінальна відповідальність прямо передбачена відповідно до законів України (див. додаток 1).

Особливу тривогу викликає те, що організовані злочинні формування активно використовують здобутки інформатики для досягнення злочинних цілей. Аналіз наявної емпіричної бази світового досвіду показує, що спостерігається тенденція, коли транснаціональна організована комп’ютерна злочинність становить загрозу не тільки національній безпеці окремої країни, але й загрожує всьому світовому порядку. Це стосується сфери економічної безпеки. Світовий “кіберпростір” у галузі економічних відносин активно освоюється криміналітетом. За експертними оцінками, обсяги операцій при електронній обробці та передачі за комп’ютерними мережами грошових ресурсів вказують на те, що потенційні втрати можуть бути вищі, ніж при тих самих операціях з використанням звичайних паперових технологій. Втрати ж

окремо взятої держави в таких випадках за лічені хвилини можуть досягати значних розмірів.

Розрізняють декілька видів атак на комп'ютерні системи.

Локальною атакою називається випадок, коли зловмисник опинився безпосередньо перед клавіатурою (дисководом, CD-ROM і т. п.) даного комп'ютера.

Віддалена атака — це варіант атаки, коли зловмисник не бачить (і можливо ніколи не побачить) ту робочу станцію (або сервер), яку він атакує. При цьому сам комп'ютер, що атакується, можливо, не проявляє ніякої мережевої активності.

Атака на потік даних — інцидент, коли комп'ютер (комп'ютери), що атакуються, активно відправляють, приймають або обмінюються даними з іншими комп'ютерами мережі, локальної або глобальної, а місцем атакуючої дії є сегмент мережі або мережевий вузол між цими системами.

Фахівці склали перелік дій, які потрібно провести у кожному конкретному випадку, щоб передбачати сценарії можливих нападів на комп'ютерну систему. Цей перелік включав:

визначення цінності інформації, що зберігається в комп'ютерній системі:

- оцінку тимчасових і фінансових витрат, які може дозволити собі зловмисник для подолання механізмів зашиті комп'ютерної системи;
- вірогідну модель поведінки зловмисника при атаці на комп'ютерну систему;
- оцінку тимчасових і фінансових витрат, необхідних для організації адекватного захисту комп'ютерної системи.

Таким чином, при проведенні аналізу потенційних погроз безпеці комп'ютерної системи експерт ставив себе на місце зловмисника, що намагається проникнути в цю систему. І насамперед потрібно було якомога точніше відповісти на наступні питання:

- наскільки високий рівень професійної підготовки зловмисника;
- якою інформацією про комп'ютерну систему, що атакується, він володіє;
- як зловмисник здійснює доступ до цієї системи;

- яким способом атаки він скористається з найбільшою вірогідністю.

Інформаційна безпека припускає відсутність погроз, направлених на:

- Цілісність;
- Конфіденційність;
- Доступність;
- Захист людини від інформації.

Цілісність інформації – припускає відсутність модифікації, зміни або знищення інформації.

Конфіденційність інформації – це захист інформації від несанкціонованого доступу.

Доступність (відсутність втрати інформації) – це доступність інформації з боку всіх зацікавлених осіб, які мають право на цю інформацію.

Загроза інформації – це потенційно можлива подія, яка приводить до наслідків порушення цілісності, доступності і конфіденційності інформації.

Порушення безпеки – називається реалізація даної загрози безпеці.

На сучасному етапі можна виділити три підходи до рішення проблем безпеки:

перший (приватний) підхід грунтується на вирішенні приватних завдань забезпечення інформаційної безпеки. Цей підхід є малоефективним, але достатньо часто використовується, оскільки не вимагає великих фінансових і інтелектуальних витрат;

другий (комплексний) підхід грунтується на вирішенні комплексу приватних завдань за єдиною програмою. Цей підхід в даний час є основним;

третій (інтегральний) підхід заснований на інтеграції різних підсистем зв'язку, підсистем забезпечення безпеки в єдину систему із загальними технічними засобами, каналами зв'язку, програмним забезпеченням і базами даних.

Розділ 1.

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Сучасний період ринкової економіки характеризується переходом до нової економічної моделі, головне місце в якій займають інформаційні технології, засновані на комунікаційних засобах та засобах обробки і збереження інформації.

Відповідно до Конституції України, інформація є предметом державної охорони, яка забезпечується Законами: "Про інформацію", "Про захист інформації в автоматизованих системах", "Про Державну службу спеціального зв'язку та захисту інформації України", "Про електронні документи та електронний документообіг" , "Про електронний цифровий підпис", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про основи національної безпеки України", "Про телекомунікації", "Про Національну систему конфіденційного зв'язку", "Про науково-технічну інформацію", "Кримінальний кодекс України".

Закон України "Про інформацію" закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності.

Закон України "Про захист інформації в автоматизованих системах" встановлює основи регулювання правових відносин щодо захисту інформації в автоматизованих системах (АС) за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

Дія Закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах. Цим Законом встановлюються об'єкти правового захисту - інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Зазначено, що захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.

Безпосередньо встановлюються загальні вимоги щодо захисту інформації та обов'язок винних осіб понести дисциплінарну, адміністративну, кримінальну або матеріальну відповідальність за порушення вимог закону про захист інформації.

Навмисні спроби діставання несанкціонованого доступу через зовнішні комунікації займають в даний час близько 10% всіх можливих порушень. Хоча ця величина здається не такою значною, досвід роботи в Internet показує, що майже кожен Internet- сервер по декілька разів на день піддається спробам проникнення. Крім того, необхідно мати на увазі динаміку розвитку ризику цього типу: за даними Групи вивчення комп'ютерних ризиків (CERT), що проводила дослідження різних систем, контрольованих урядом США, якщо в 1990 році зареєстровано 130 вдалих спроб несанкціоновано доступу до комп'ютерних ресурсів через Internet, то за 1994 рік ця цифра склала 2300. Втрати американських компаній, пов'язані з порушеннями безпеки, склали більш 5 млн. дол.

Етапи розвитку захисту інформації

Дана проблема захисту інформації розробляється у нас в країні і за кордоном уже більше 40 років. Природно, що за минулий час корінним чином змінилося як уявлення об її суть, так і методологічні підходи до рішення. Вказані зміни відбувалися поступово й безперервно, тому всяка періодизація цього процесу значною мірою носить штучний характер. Проте, щодо підходів до захисту інформації весь цей період досить чітко ділиться на три етапи, які умовно можна назвати початковим, розвиненим і комплексним.

Перші два етапи характеризуються екстенсивним підходом до рішення задач захисту інформації. Суть їх складає поступове розширення арсеналу використовуваних засобів захисту. На етапі розвиненого захисту починає набувати поширення комплексне застосування технічних програмних і організаційних засобів. В цілях регулювання правив захисту в провідних країнах стали прийматися спеціальні законодавчі акти.

Третій етап у даний час тільки починається. Його характерна особливість полягає в спробах аналітико-синтетичної обробки даних всього наявного досвіду теоретичних досліджень і практичного рішення задач захисту й формування на цій основі науково-методологічного базису захисту інформації. Іншими словами, основне

завдання третього етапу – переклад усієї справи захисту інформації на інтенсивні способи, що базуються на науковій основі.

Доречно буде також відзначити, що останнім часом все більш гостро ставиться проблема забезпечення так званої інформаційної безпеки, що є сукупністю двох паралельних процесів, – захисту інформації і захисту від інформації (від негативної дії інформації на сучасні технічні, технологічні і організаційні системи, а також на окремих людей, їх колективи й суспільство в цілому). Наслідки останньої дії можуть носити не просто важкий, а трагічний і навіть катастрофічний характер.

Основні погрози інформаційної безпеки

Сучасна інформаційна система є складною системою, що складається з великого числа компонентів різного ступеня автономності, які зв'язані між собою й обмінюються даними. Практично кожен компонент може піддатися зовнішній дії або вийти з ладу. Компоненти автоматизованої інформаційної системи можна розбити на наступні групи:

- апаратні засоби - комп'ютери і їх складова частини (процесори, монітори, термінали, периферійні пристрої - дисководи, принтери, контроллери, кабелі, лінії зв'язку і т.д.);
- програмне забезпечення - придбані програми, результатні, об'єктні, завантажувальні модулі; операційні системи і системні програми (компілятори, компонувальники й ін.), утиліти, діагностичні програми і т.д.;
- дані - що зберігаються тимчасово й постійно, на магнітних носіях, друкарські, архіви, системні журнали і т.д.

Небезпечні дії на комп'ютерну інформаційну систему можна підрозділити на випадкові і навмисні. Аналіз досвіду проектування, виготовлення й експлуатації інформаційних систем показує, що інформація піддається різним випадковим діям на всіх етапах циклу життя системи. Причинами випадкових дій при експлуатації можуть бути:

- аварійні ситуації із-за стихійних лих і відключень електроживлення;
- відмови й збої апаратури;

- помилки в програмному забезпеченні;
- помилки в роботі персоналу;
- перешкоди в лініях зв'язку із-за дій зовнішнього середовища.

Навмисні дії - це цілеспрямовані дії порушника. Порушниками можуть виступати: службовець, відвідувач, конкурент, найманець. Дії порушника можуть бути обумовлені різними мотивами:

- незадоволеністю службовця своєю кар'єрою;
- хабаром;
- цікавістю;
- конкурентною боротьбою;
- прагненням самоствердитися за всяку ціну.

Виходячи з цього визначення, нескладно виділити основні типи погроз інформації, здійснювані шляхом навмисної або ненавмисної дії на неї:

навмисні дії:

- перехоплення (у разі реалізації даного виду погроз стає можливим копіювання, читання, розголошування або використання відомостей закритого характеру);
- розкрадання (у цьому випадку зловмиснику трапляється щонайширша нагода здійснення своїх намірів);
- модифікація (погрози даного здійснюються шляхом несанкціонованого доступу і чреваті знищенням інформації або її фальсифікацією);
- руйнування (погрози даного типу мають, як правило, одноразовий характер прояву);

Можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника на рівні розробника даної системи;
- порушником може бути як стороння особа, так і законний користувач системи;
- порушнику відома інформація про принципи роботи системи;
- порушник вибирає найбільш слабку ланку в захисті.

Найбільш поширеним видом комп'ютерних порушень є несанкціонований доступ (НСД). НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректній установці й налагодженні.

Проведемо класифікацію каналів НСД, за якими можна здійснити розкрадання, зміну або знищення інформації:

Через людину:

- розкрадання носіїв інформації;
- читання інформації з екрана або клавіатури;
- читання інформації з роздруку.

Через програму:

- перехоплення паролів;
- розшифровка зашифрованої інформації;
- копіювання інформації з носія.

Через апаратуру:

- підключення спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
- перехоплення побічних електромагнітних випромінювань від апаратури, ліній зв'язку, мереж електроживлення і т.д.

Забезпечення інформаційної безпеки

Формування режиму інформаційної безпеки - проблема комплексна. Заходи з її рішення можна підрозділити на чотири рівні:

- законодавчий (закони, нормативні акти, стандарти і т.п.);
- морально-етичний (усілякі норми поведінки, недотримання яких веде до падіння престижу конкретної людини або цілої організації);
- адміністративний (дії загального характеру, організації, що робляться керівництвом);
- фізичний (механічні, электро- і електронно-механічні перешкоди на можливих шляхах проникнення потенційних порушників);

- апаратно-програмний (електронні пристрої і спеціальні програми захисту інформації).

Єдина сукупність всіх цих заходів, направлених на протидію погрозам безпеки з метою зведення до мінімуму можливості збитку, утворюють систему захисту.

Надійна система захисту повинна відповідати наступним принципам:

- Вартість засобів захисту повинна бути менше, ніж розміри можливого збитку;
- Кожен користувач повинен мати мінімальний набір привілеїв, необхідний для роботи;
- Захист тим більше ефективний, ніж простіше користувачу з ним працювати;
- Можливість відключення в екстрених випадках;
- Фахівці, що мають відношення до системи захисту повинні повністю уявляти собі принципи її функціонування й у разі виникнення скрутних ситуацій адекватно на них реагувати;
- Під захистом повинна знаходитися вся система обробки інформації;
- Розробники системи захисту, не повинні бути в числі тих, кого ця система контролюватиме;
- Система захисту повинна надавати докази коректності своєї роботи;
- Особи, що займаються забезпеченням інформаційної безпеки, повинні нести особисту відповідальність;
- Об'єкти захисту доцільно розділяти на групи так, щоб порушення захисту в одній з груп не впливало на безпеку інших;
- Надійна система захисту повинна бути повністю протестована й узгоджена;
- Захист стає ефективнішим і гнучким, якщо він допускає зміну своїх параметрів із боку адміністратора;
- Система захисту повинна розроблятися, виходячи з припущення, що користувачі здійснюватимуть серйозні помилки і, взагалі, мають якнайгірші наміри;

- Найбільш важливі й критичні рішення повинні ухвалюватися людиною;
- Існування механізмів захисту повинне бути по можливості приховано від користувачів, робота яких знаходиться під контролем.

Абстрактні моделі захисту даних

Розробки у області теорії захисту інформаційних об'єктів велися достатньо давно. Їх результатами є так звані абстрактні моделі захисту даних, в яких дослідники висловлюють загальні ідеї з цього питання і формують набори обмежень, що зв'язують суб'єкт, об'єкт і інші категорії.

Одна з перших моделей була опублікована в 1977 модель Біба (Biba). Згідно їй всі суб'єкти і об'єкти заздалегідь розділяються за декількома рівнями доступу, а потім на їх накладаються наступні обмеження: 1) суб'єкт не може викликати на виконання суб'єкти з вищим рівнем доступу; 2) суб'єкт не може модифікувати об'єкти з вищим рівнем доступу.

Модель Гогена-Мезігера (Goguen-Meseguer), представлена ними в 1982 році, заснована на теорії автоматів. Згідно їй система може при кожній дії переходити з одного дозволеного стану тільки в дещо інших. Суб'єкти і об'єкти в даній моделі захисту розбиваються на групи – домени, і перехід системи з одного стану в інший виконується тільки відповідно до так званої таблиці дозволів, в якій вказано які операції може виконувати суб'єкт, скажімо, із домена C над об'єктом із домена D. У даній моделі під час переходу системи з одного дозволеного стану в інший використовуються трансакції, що забезпечує загальну цілісність системи.

Сазерлендская (від англ. Sutherland) модель захисту, опублікована в 1986 році, робить акцент на взаємодії суб'єктів і потоків інформації. Так само як і в попередній моделі, тут використовується машина станів із безліччю дозволених комбінацій станів і деяким набором початкових позицій. У даній моделі досліджується поведінка множинних композицій функцій переходу з одного стану в інший.

Важливу роль у теорії захисту інформації грає модель захисту Кларка-Вільсона (Clark-Wilson), опублікована в 1987 році і модифікована в 1989. Заснована дана модель на використанні трансакцій і ретельному оформленні прав доступу су-

б'єктів до об'єктів. В даній моделі вперше досліджена захищеність третьої сторони в даній проблемі – сторони, що підтримує всю систему безпеки. Цю роль в інформаційних системах, звичайно, грає програма-супервізор. Крім того, в моделі Кларка-Вільсона трансакції вперше були побудовані за методом верифікації, тобто ідентифікація суб'єкта проводилася не тільки перед виконанням команди від нього, але і повторно після виконання. Це дозволило зняти проблему підміни автора в момент між його ідентифікацією і власне командою. Модель Кларка-Вільсона вважається однією з самих надійних відносно підтримки цілісності інформаційних систем.

КОНТРОЛЬНІ ПИТАННЯ

1. Інформація, як товар.
2. Відповідальність перед законом громадян з приводу захисту інформації
3. Етапи розвитку захисту інформації.
4. Групи автоматизованої інформаційної системи з точки зору захисту інформації.
5. Причинами випадкових дій при експлуатації, які приводять до втрати інформації.
6. Навмисні дії, які приводять до втрати інформації.
7. Гіпотетична модель потенційного порушника.
8. Поняття несанкціонованого доступу до даних.
9. Забезпечення інформаційної безпеки - проблема комплексна
10. Вимоги до коректності роботи системи захисту.
11. Абстрактні моделі захисту даних.
12. Особливості моделі Біба.
13. Особливості моделі Гогена-Мезігера.
14. Особливості Сазерлендської моделі.
15. Особливості моделі Кларка-Вільсона .

Розділ 2.

ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS.

ВСТУП.

Операційна система є найважливішим програмним компонентом будь-якої обчислювальної машини, тому від рівня реалізації політики безпеки в кожній конкретній ОС багато в чому залежить і загальна безпека інформаційної системи.

Парольний захист комп'ютера при його запуску.

При включенні комп'ютера в мережу для захисту від несанкціонованого доступу до програм та інформації необхідно встановити парольний захист на BIOS. Для цього, після початку запуску комп'ютера, натисніть клавішу Delete, або іншу за вказівкою комп'ютера та, вибравши відповідно в діалоговому вікні команди Set Supervisor Password та Set User Password, введіть відповідний пароль в діалогове віконце, яке з'явиться та зробіть підтвердження паролю. Для виходу з BIOS натисніть функціональну клавішу F10 і введіть Yes (Y). Пароль Set Supervisor Password надає можливість змінити пароль Set User Password. паролі можуть бути введеними однаковими.

Примітка:

В деяких сучасних BIOS може вказуватись тільки один тип паролю, наприклад, в BIOS American Megatremds – Change Password, та мається можливість перемикання паролю до входу до операційної системи Check Password, з вибором команд: Setup або Always.

Існує кілька способів обходу пароля в BIOS:

- Застосувати "пароль чорного ходу" виробника BIOS (див. Додаток 2);
- Використовувати програму злому пароля;
- Скинути CMOS за допомогою перемички або перемикання контактів;
- Скинути CMOS видаленням акумулятора не менш ніж на 10 хвилин;
- Заміна BIOS на аналогічну модель.

Для визначення типу BIOS на вашому комп'ютері необхідно, наприклад, ввести команду systeminfo із командного рядка (рис. 2.1).

Захист інформації при застосуванні операційної системи Windows XP

Парольний захист операційної системи

Для забезпечення безпеки комп'ютера необхідно організувати захист окремих файлів і каталогів (каталогів) та вжити заходів до фізичного захисту самого комп'ютера. Якщо на комп'ютері є конфіденційні відомості, вони повинні зберігатися в безпечному місці.

Іншим способом захисту комп'ютера є його блокування на час відсутності користувача на робочому місці й налагодження екранної заставки, захищеної паролем.

Щоб захистити паролем комп'ютер в режимі очікування (знаходячись в чекаючому режимі, комп'ютер перемикається в стан з низьким споживанням електроенергії, в якому відключаються такі пристрої, як жорсткі диски й монітор. При відновленні роботи комп'ютер швидко виходить із режиму і робочий стан повністю відновлюється. Режим чекання корисно застосовувати для збереження заряду батарей портативних комп'ютерів) і сплячому режимах (у сплячому режимі весь вміст пам'яті зберігається на жорсткому диску, відключаються монітор і жорсткі диски, і комп'ютер вимикається. При перезапуску комп'ютера стан робочого стану повністю відновлюється):

Натисніть кнопку **Пуск,** виберіть команди **Налагодження** й **Панель управління**, а потім двічі клацніть значок **Електроживлення**.

Виберіть вкладку **Додатково** (рис. 2.2) і встановіть прапорець **Запрошувати пароль при виході зі сплячого режиму**. При виході комп'ютера із сплячого режиму запрошуватиметься пароль облікового запису, із яким був здійснений вхід у систему.

Захист комп'ютера за допомогою паролів

Коли комп'ютер, захищений надійним паролем, інші користувачі, що не знають пароль, не зможуть дістати доступ до файлів або програм.

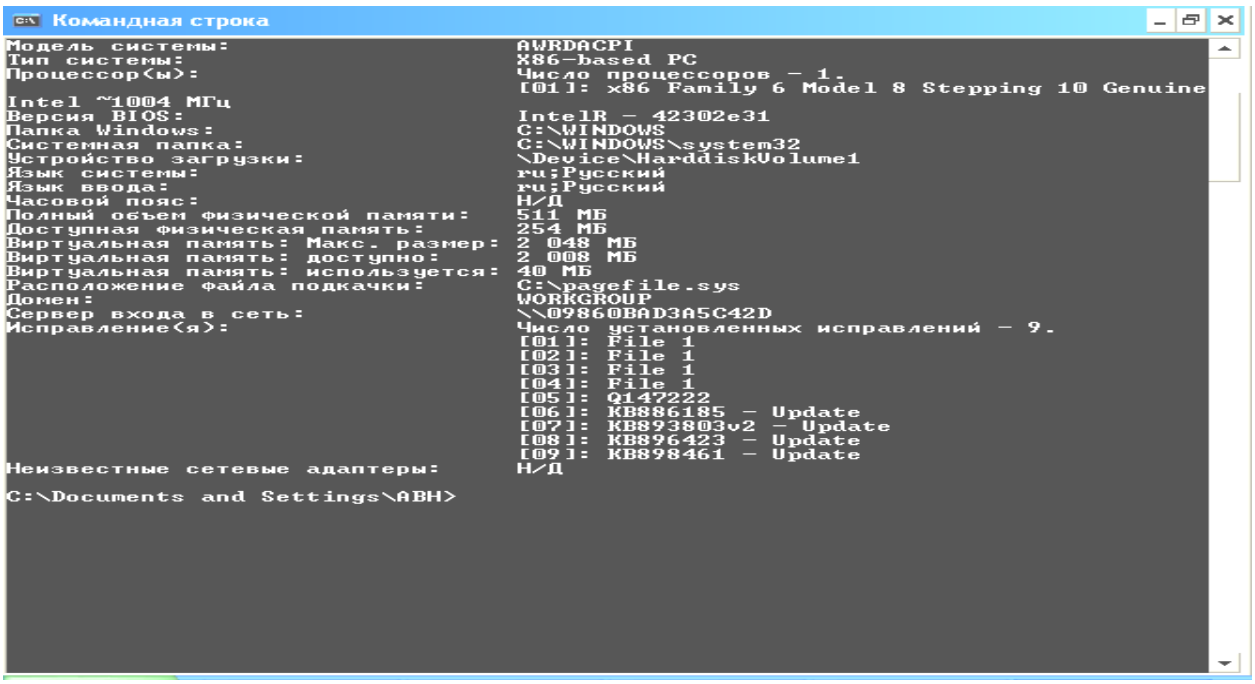


Рис. 2.1. Вікно командного рядка

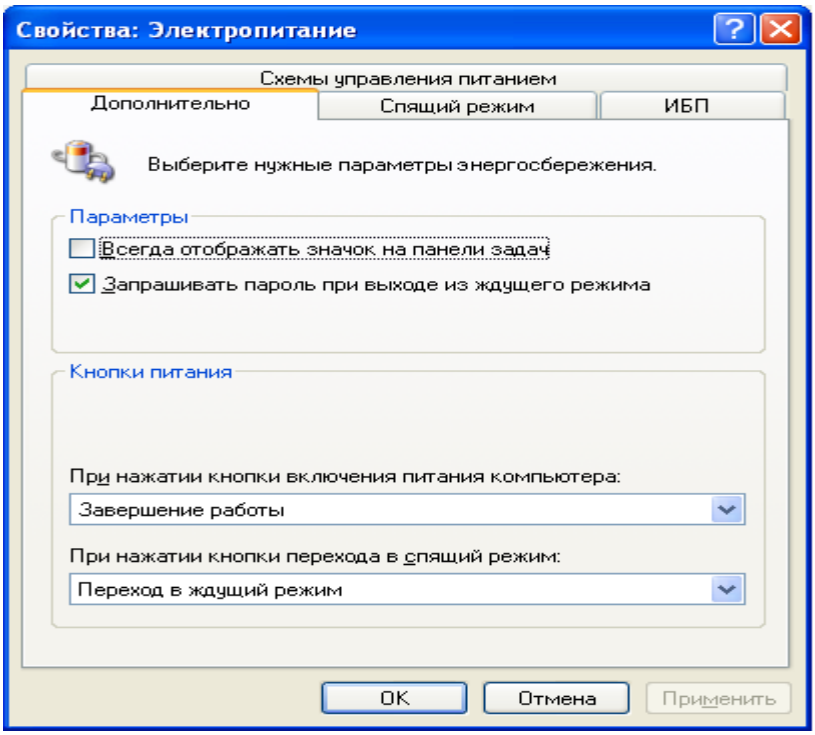


Рис. 2.2. Вікно електроживлення

Якщо при підключенні до веб-вузла, інтрамережі організації або мережевих каталогів потрібно указувати ім'я користувача й пароль, можна налагодити Microsoft Windows на запам'ятовування пароля.

При створенні пароля слід також створити дискету скидання паролів. Якщо пароль забутий, можна буде за допомогою цієї дискети скинути пароль і дістати доступ до своїх файлів і програм.

Примітка:

Майстер забутих паролів дозволяє створювати дискету скидання паролів, яку можна використовувати для відновлення облікового запису користувача й особистих параметрів комп'ютера, якщо користувач забув свій пароль.

Послідовність кроків для виконання цього завдання залежить від того, чи входить комп'ютер у мережевий домен або є частиною робочої групи (або є автономним комп'ютером).

Комп'ютер підключений до домена

Натисніть **CTRL+ALT+DEL**, щоб відкрити діалогове вікно **Безпека Windows**.

- Натисніть кнопку **Зміна пароля**;
- Натисніть кнопку **Архівація**, щоб запустити майстер забутих паролів;
- Натисніть кнопку **Далі** і слідуйте інструкціям на екрані.

Комп'ютер не підключений до домена

- Відкрийте на панелі управління компонент **Облікові записи користувачів**;
- Виберіть ім'я свого облікового запису.

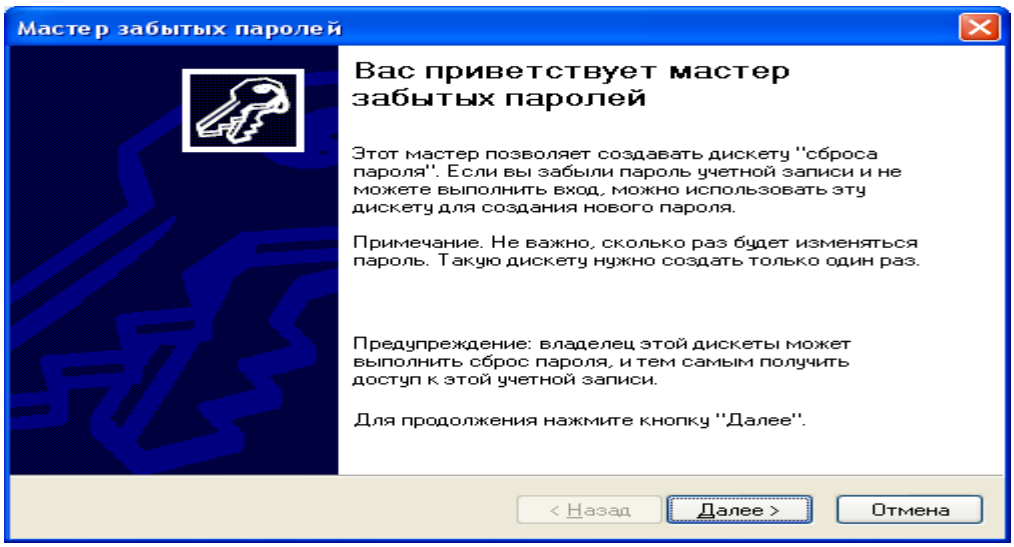


Рис. 2.3. Вікно майстра забутих паролів

- У групі **Підказка про пароль**, розташованій у вікні зліва, клацніть посилання. З'явиться майстер забутих паролів (рис.2.3);
- У майстрі забутих паролів слідуйте інструкціям на екрані.

Примітки:

Щоб відкрити компонент «**Облікові записи**», натисніть кнопку **Пуск**, виберіть команди **Налагодження** й **Панель управління**, потім двічі клацніть значок **Облікові записи користувачів**.

Дії з паролями залежать від того, чи приєднаний комп'ютер до мережевого домена. Щоб перевірити, чи приєднаний комп'ютер до мережевого домена, на робочому столі клацніть правою кнопкою миші значок **Мій комп'ютер** і виберіть команду **Властивості**. Якщо ім'я домена відображається на вкладці **Ім'я комп'ютера**, комп'ютер приєднаний до домена.

Облікові записи користувачів на локальному комп'ютері або на комп'ютері, який входить до робочої групи.

Існує два типи облікових записів користувачів, доступних на комп'ютері: обліковий запис адміністратора комп'ютера й обліковий запис з обмеженими правами. Обліковий запис гостя за умовчанням доступний для користувачів, що не мають власних облікових записів на комп'ютері.

Обліковий запис адміністратора комп'ютера .

Обліковий запис адміністратора комп'ютера призначений для тих, хто може вносити зміни на рівні системи, встановлювати програми і мати доступ до всіх файлів на комп'ютері. Користувач з обліковим записом адміністратора комп'ютера має повний доступ до інших облікових записів користувачів на комп'ютері. Користувач з обліковим записом адміністратора комп'ютера:

- може створювати й видаляти облікові записи користувачів на комп'ютері;
- може створювати паролі для інших користувачів на комп'ютері;
- може змінювати в обліковому записі імена користувачів, малюнки, паролі й типи облікових записів;
- не може змінити тип свого облікового запису у разі, коли на комп'ютері більше немає користувачів з обліковим записом адміністратора комп'ю-

тера. Як правило, забезпечується наявність на комп'ютері принаймні одного користувача з обліковим записом адміністратора.

Примітка:

Обліковий запис під назвою «Адміністратор» створюється в процесі установки системи. Цей обліковий запис із повноваженнями адміністратора комп'ютера використовує пароль адміністратора, який був уведений під час установки.

Обліковий запис з обмеженими правами.

Обліковий запис з обмеженими правами призначається для користувачів, яким повинно бути заборонено змінювати більшість налагоджень комп'ютера і видаляти важливі файли. Користувач з обліковим записом з обмеженими правами:

- не може встановлювати програми й устаткування, але має доступ до вже встановленим на комп'ютері програмам;
- може змінювати власний малюнок, призначений обліковому запису, а також створювати, змінювати або видаляти власний пароль;
- не може змінювати ім'я або тип власного облікового запису. Такі зміни повинні виконуватися користувачем з обліковим записом адміністратора комп'ютера.

Примітка:

Деякі програми можуть працювати неправильно для користувачів з обмеженими правами. У такому разі слід змінити тип облікового запису на адміністратора комп'ютера, тимчасово або назовсім.

Обліковий запис гостя

Обліковий запис гостя призначається для користувачів, що не мають власних облікових записів на комп'ютері. В облікового запису гість немає пароля. Це дозволяє швидко входити на комп'ютер для перевірки електронної пошти або проглядання Інтернету. Користувач, що увійшов з обліковим записом гостя:

- не може встановлювати програми й устаткування, але має доступ до вже встановленим на комп'ютері програмам;
- не може змінити тип облікового запису гостя;

- може змінити малюнок облікового запису гостя.

Примітка:

Компонент «Облікові записи користувачів» знаходиться на панелі управління. Щоб відкрити компонент «Облікові записи», натисніть кнопку **Пуск**, виберіть команди **Налагодження** й **Панель управління**, потім двічі клацніть значок **Облікові записи користувачів**.

Створення паролю користувача

Для виконання цієї процедури необхідно увійти до системи з обліковим записом «Адміністратор» або члена групи «Адміністратори». Якщо комп'ютер підключений до мережі, то параметри мережевої політики можуть заборонити виконання даної процедури.

Відкрийте на **Панелі управління** компонент **Облікові записи користувачів**.

На вкладці **Користувачі** виберіть ім'я користувача, для якого потрібно створити пароль, і введіть команду **Змінити обліковий запис**, а потім **Створення пароля** (рис. 2.4)

Уведіть новий пароль у поля **Новий пароль** і **Підтвердження пароля**, а потім натисніть кнопку **Создать пароль**.

Примітка:

Паролі можна створювати тільки для облікових записів локального комп'ютера, таких, як «Гість», «Адміністратор» або облікові записи, створені для цього комп'ютера.

Надійний пароль повинен відповідати наступним вимогам.

Пароль повинен складатися не менше ніж із семи знаків. Найбільш надійні паролі складаються з 7 або 14 знаків. Причиною надійності таких паролів є спосіб кодування.

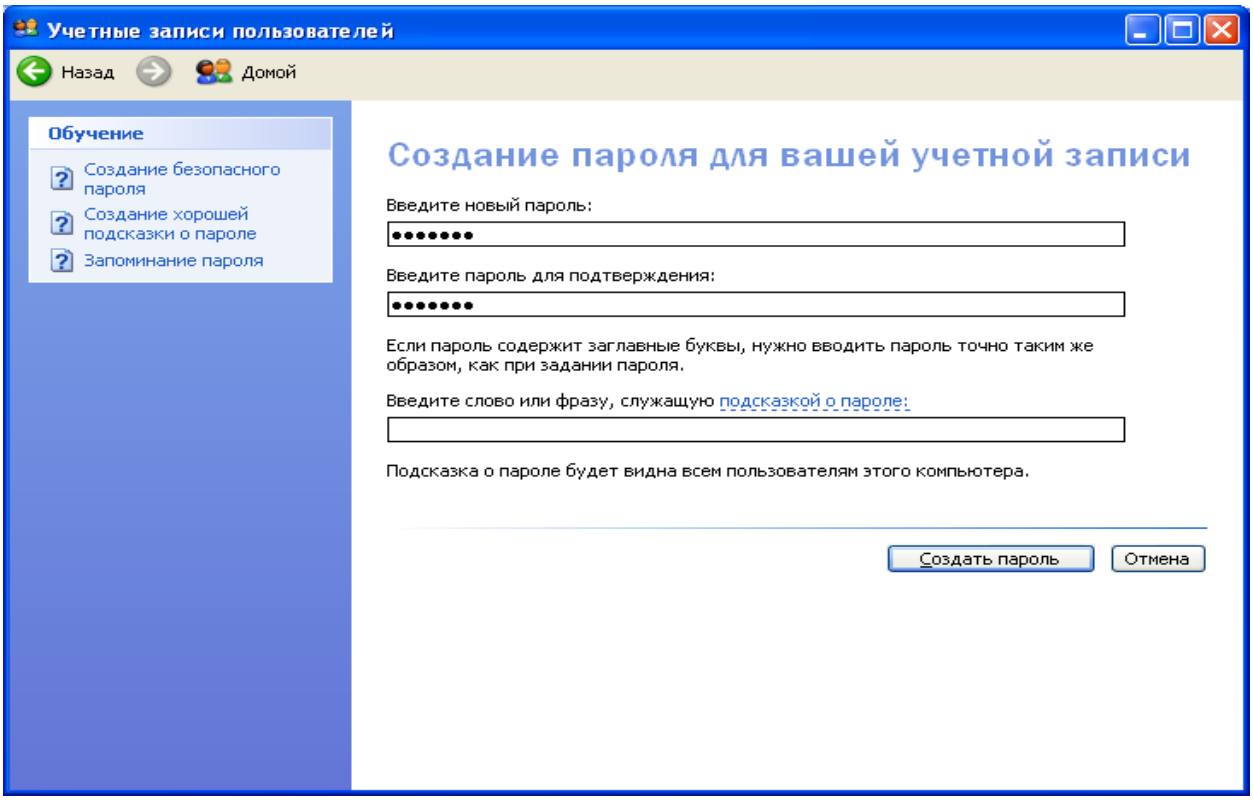


Рис. 2.4. Вікно введення пароля

Пароль повинен містити знаки, які наведені в таблиці 2.1.

Таблиця 2.1

Символи, які можна використовувати для паролів.

Група	Приклади
Букви (прописні і рядкові)	A, B, C... (або a, b, c...)
Цифри	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Символи (усі знаки, що не є буквами або цифрами)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ?, . /

Пароль повинен значно відрізнятися від паролів, що використалися раніше. Пароль не повинен містити прізвища або імені користувача. Як пароль не можна використовувати поширене слово або ім'я.

Паролі можуть бути найслабкішою ланкою в системі безпеки комп'ютера. Використання надійних паролів необхідне у зв'язку із застосуванням користувачами новітніх засобів і комп'ютерів для розшифровування паролів. Мережевий пароль, для злому якого раніше було б потрібно тижні, тепер може бути розкритий протягом декількох годин.

Паролі Windows можуть містити до 127 символів. Проте якщо Windows XP використовується в мережі, де є також комп'ютери з Windows 95 або Windows 98, не використовуйте паролі, довжина яких перевищує 14 символів. Windows 95 і Windows 98 підтримують паролі завдовжки до 14 знаків. Якщо пароль має велику довжину, увійти до мережі з цих комп'ютерів не вдасться.

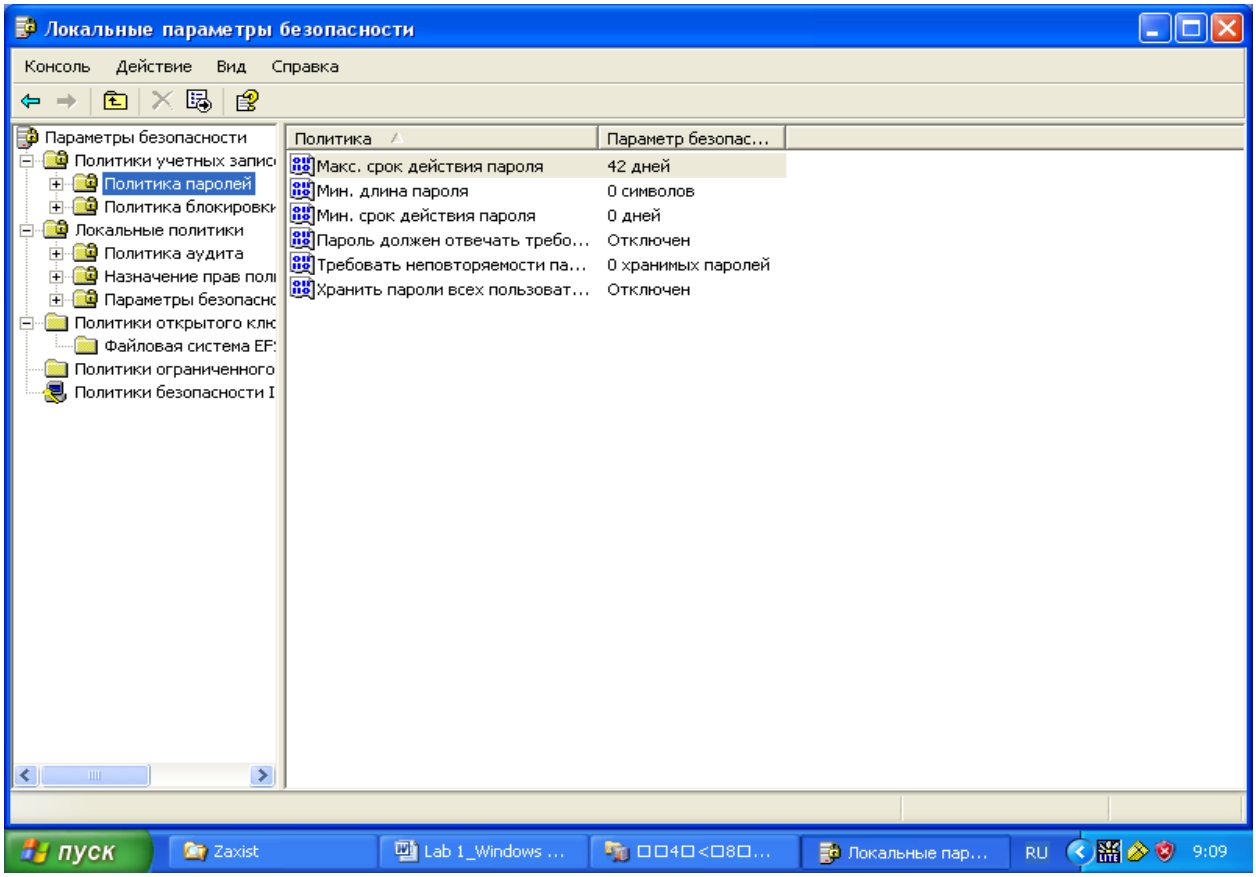


Рис. 2.5. Вікно встановлення параметрів паролю

Щоб зберегти пароль на комп'ютері:

Цю процедуру слід використовувати для отримання доступу до захищеного паролем ресурсу в мережі.

- У діалоговому вікні **Ім'я й пароль користувача**, що виводиться при спробі підключитися до захищеного ресурсу, в полі **Ім'я користувача** введіть ім'я користувача;
- У полі **Пароль** введіть пароль;
- Установіть прапорець **Зберегти пароль**;
- Установіть прапорець **Більше не питати цей пароль**.

У Windows при наступній спробі підключення до цього ресурсу не доведеться указувати ім'я користувача й пароль.

Для встановлення терміну дії пароля та інших його параметрів треба натиснути кнопку **Пуск**, виберіть команди **Налагодження** й **Панель управління**, а потім двічі клацніть значок **Администрирование**, двічі клацніть значок **Локальная политика безопасности** та виберіть **Политика учетных записей** та **Политика паролей** (рис. 2.5). Установіть необхідні параметри паролю, наприклад, термін дії (рис. 2.6) .

Запуск Windows у режимі захисту від збоїв

- Натисніть кнопку **Пуск** і виберіть команду **Завершення роботи;**
- Виберіть параметр перезавантажити комп'ютер, натисніть кнопку **OK**, а потім натисніть і утримуйте клавішу **CTRL** до появи меню завантаження Microsoft Windows;

На деяких комп'ютерах для виклику меню завантаження Microsoft Windows можна використовувати клавішу **F8** замість клавіші **CTRL**;

- Уведіть номер команди Safe mode (звід збоїв) і натисніть клавішу **ENTER**.

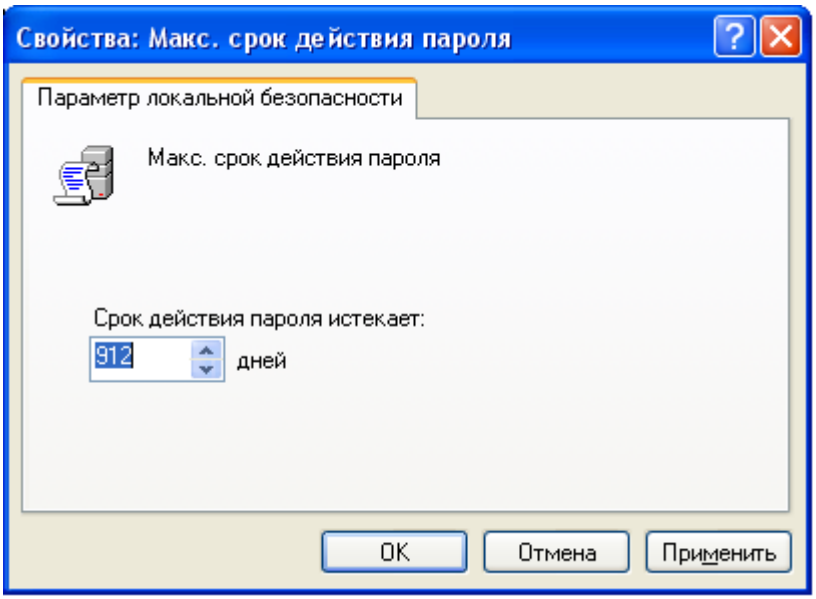


Рис. 2.6. Вікно встановлення терміну дії пароля

Примітки:

У режимі захисту від збоїв операційна система Windows використовує Налагодження за замовчуванням (монітор VGA, підтримка мережі відсутня, драйвер миші Microsoft і мінімальний набір драйверів пристроїв, необхідних для запуску Windows). Доступ до пристроїв читання компакт-дисків, принтерів і т.п. у цьому режимі відсутній.

- Для зміни Налагодження можна натиснути кнопку **Пуск**, вибрати команди **Налагодження** й **Панель керування**, а потім двічі клацнути значок **Мережа** або **Система**;
- Після завершення даної процедури для запуску Windows у звичайному режимі буде потрібно перезавантаження комп'ютера.

Керування доступом до каталогів і принтерів

1. У вікні **Мій комп'ютер** або у вікні **провідника** виберіть каталог чи принтер, доступ до яких потрібно обмежити.
2. У меню **Файл** виберіть команду **Властивості**.
3. Виберіть вкладку **Доступ**.
4. Якщо застосовується керування доступом на рівні користувачів, натисніть кнопку **Додати** для вказівки користувачів, разом із якими варто використовувати принтер або каталог.
5. Якщо застосовується керування доступом на рівні ресурсів, уведіть пароль для доступу до каталоги або принтеру.

Брандмауер Windows

Брандмауер допомагає підвищити безпеку комп'ютера. Він обмежує інформацію, що поступає на комп'ютер з інших комп'ютерів, дозволяючи краще контролювати дані на комп'ютері і забезпечуючи лінію оборони комп'ютера від людей або програм (включаючи віруси і хропаки), які несанкціоновано намагаються підключитися до комп'ютера.

Можна вважати брандмауер прикордонним постом, на якому перевіряється інформація (часто звана трафіком), що приходить з Інтернету або локальної мережі.

В ході цієї перевірки брандмауер відхиляє або пропускає інформацію на комп'ютер відповідно до встановлених параметрів.

Як працює брандмауер?

Коли до комп'ютера намагається підключитися хтось з Інтернету або локальної мережі, такі спроби називають «непередбаченими запитами». Коли на комп'ютер поступає непередбачений запит, брандмауер Windows блокує підключення. Якщо на комп'ютері використовуються такі програми, як програма передачі миттєвих повідомлень або мережеві ігри, яким потрібно приймати інформацію з Інтернету або локальної мережі, брандмауер запрошує користувача про блокування або дозвіл підключення. Якщо користувач дозволяє підключення, брандмауер Windows створює виключення, щоб у майбутньому не турбувати користувача запитами з приводу надходження інформації для цієї програми.

Якщо йде обмін миттєвими повідомленнями із співбесідником, який збирається прислати файл (наприклад, фотографію), брандмауер Windows запитає підтвердження про зняття блокування підключення й дозволі передачі фотографії на комп'ютер. А при бажанні брати участь у мережевій грі через Інтернет із друзями користувач може додати цю гру як виняток, щоб брандмауер пропускав ігрову інформацію на комп'ютер.

Хоча є можливість відключати брандмауер Windows для окремих підключень до Інтернету або локальної мережі, це підвищує вірогідність порушення безпеки комп'ютера.

Що може і чого не може брандмауер Windows (табл. 2.2)

Таблиця 2.2

Можливості брандмауера Windows

Він може:	Він не може:
Блокувати комп'ютерним вірусам і «хробакам» доступ на комп'ютер.	Виявити або знешкоджувати комп'ютерні віруси і «хропаки», якщо вони вже потрапили на комп'ютер. З цієї причини необхідно також установити антивірусне програмне забезпечення і своєчасно

	оновлювати його, щоб запобігти пошкодженню комп'ютера вірусами, «хропаками» і іншими небезпечними об'єктами, а також не допустити використання даного комп'ютера для розповсюдження вірусів на інші комп'ютери.
Запитати користувача про вибір блокування або дозвіл для певних запитів на підключення .	Заборонити користувачу відкривати повідомлення електронної пошти з небезпечними вкладеннями. Не відкривайте вкладення в повідомленнях електронної пошти від незнайомих відправників. Слід проявляти обережність, навіть якщо джерело повідомлення електронної пошти відоме і заслуговує довіри. При отриманні від знайомого користувача електронного листа з вкладенням уважно прочитайте тему повідомлення перед тим, як відкрити його. Якщо тема повідомлення є безладним набором знаків або не має сенсу, не відкривайте лист, поки не зв'яжетеся з відправником для отримання підтвердження.
Звістці облік (журнал безпеки) — за бажанням користувача — записуючи дозволені й заблоковані спроби підключення до комп'ютера. Цей журнал може виявитися корисним для діагностики неполадок..	Блокувати спам або несанкціоновані поштові розсилки, щоб вони не поступали в теку вхідних повідомлень. Проте деякі програми електронної пошти здатні робити це. Ознайомтеся з документацією своєї поштової програми, щоб з'ясувати її можливості.

Щоб уключити або вимкнути брандмауер Windows

Для виконання цієї процедури необхідно увійти до системи з обліковим записом «Адміністратор».

1. Відкрийте брандмауер Windows. В меню **Пуск** виберіть команду **Налагодження** та **Панель управління**. Двічі клацніть по піктограмі **Брандмауер Windows.**

2. На вкладці **Загальні** виберіть один із наступних параметрів:

- Включити (рис. 2.7) (рекомендується). Звичайно, використовується цей параметр.

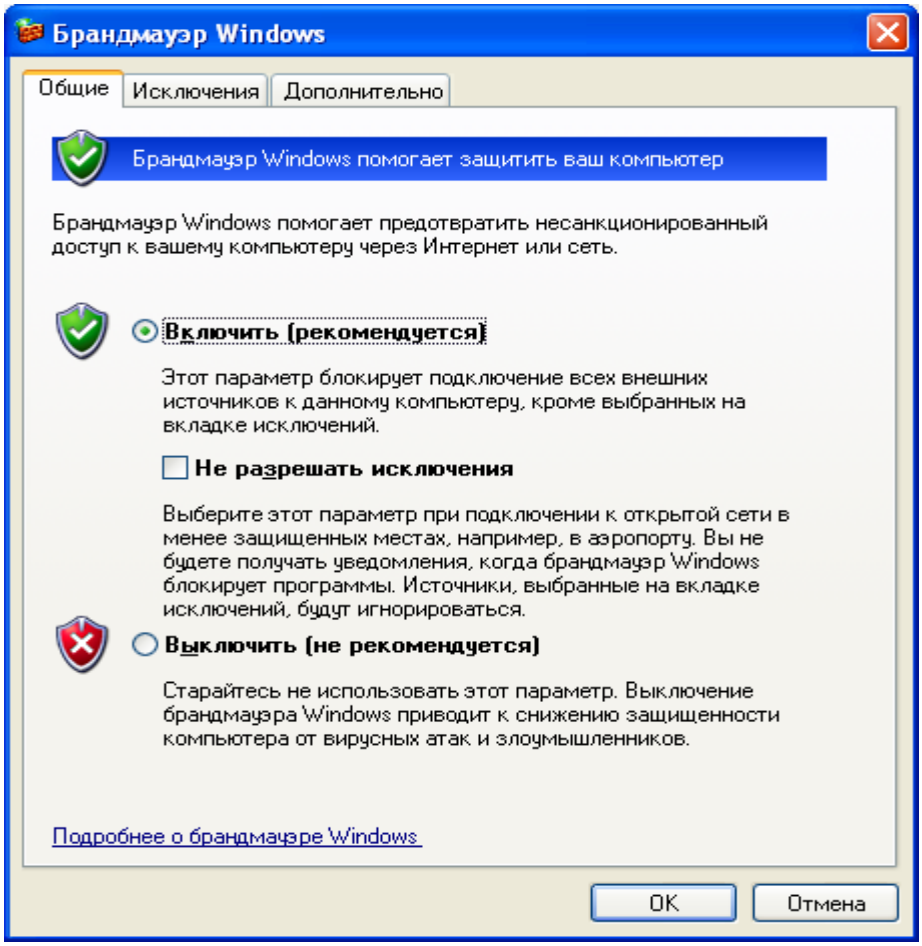


Рис. 2.7. Вікно брандмауера

Можна також установити прапорець **Не дозволяти виключення**. Коли встановлений цей прапорець, брандмауер блокує всі непередбачені запити на підключення до комп'ютера, зокрема, запити до програм або служб, вибраних на вкладці **Виключення**. Цей параметр служить для максимального захисту комп'ютера, на-

приклад, при підключенні до загальнодоступної мережі в готелі або аеропорту або в періоди розповсюдження через Інтернет особливо небезпечних вірусів або хропаків.

- Вимкнути (не рекомендується). Відключення брандмауера Windows може привести до того, що комп'ютер (і мережа, якщо вона є) може стати більш уразливим для атак із боку вірусів або невідомих зловмисників;
- Для всіх підключень до Інтернету і локальної мережі брандмауер Windows за умовчанням включений. Проте деякі виробники комп'ютерів або мережеві адміністратори можуть вимкнути його;

Ризик при створенні виключень

Кожне виключення, що дає програмі можливість зв'язуватися через брандмауер Windows, робить комп'ютер більш уразливим. Створення виключення рівносильне пробиттю пролому в брандмауері. Якщо таких проломів опиниться дуже багато, брандмауер уже не буде міцною перешкодою. Звичайно, зломщики використовують спеціальні програми для пошуку в Інтернеті комп'ютерів із незахищеними підключеннями. Якщо створити багато виключень і відкрити багато портів, комп'ютер може виявитися жертвою таких зломщиків.

- Щоб зменшити потенційний ризик при створенні виключень:
- Створюйте виключення, тільки коли воно дійсно необхідне;
- Ніколи не створюйте виключень для програми, яку погано знаєте;
- Видаляйте виключення, коли необхідність у них відпадає.

Створення виключень, не дивлячись на ризик

Іноді потрібно відкрити комусь можливість зв'язку з вашим комп'ютером, не дивлячись на риск, наприклад, коли очікується отримання файлу, посланого через програму передачі миттєвих повідомлень, або коли хочеться взяти участь у мережевій грі через Інтернет.

Якщо йде обмін миттєвими повідомленнями із співбесідником, який збирається прислати файл (наприклад, фотографію), брандмауер Windows запитає підтвердження про зняття блокування підключення й дозволі передачі фотографії на ваш комп'ютер. А при бажанні брати участь у мережевій грі через Інтернет із друзями

можна додати цю гру як виняток, щоб брандмауер пропускав ігрову інформацію на ваш комп'ютер.

Щоб додати програму в список виключень

Для виконання цієї процедури необхідно увійти до системи з обліковим записом «Адміністратор».

Відкрийте брандмауер Windows. На вкладці **Виключення** в групі **Програми й служби** встановіть прапорець для програми або служби, яку потрібно вимкнути, а потім натисніть кнопку **OK**.

Якщо програма або служба, яку потрібно вимкнути, відсутня в списку, виконайте наступні дії.

Натисніть кнопку **Додати програму** (рис. 2.8).

У діалоговому вікні **Додавання програми** виберіть **програму**, яку потрібно додати, і натисніть кнопку **OK**. Ця програма з'явиться (із установленим прапорцем) на вкладці **Виключення** в групі **Програми й служби**. Натисніть кнопку **OK**.

Якщо програма або служба, яку потрібно встановити, не перерахована в діалоговому вікні Додавання програми, виконайте наступні дії.

У діалоговому вікні **Додавання програми** натисніть кнопку **Огляд**, знайдіть **програму**, яку потрібно додати, і **двічі клацніть по ній мишкою**. (Програми, звичайно, зберігаються на комп'ютері в каталозі «Program Files».) Програма з'явиться в групі **Програми** в діалоговому вікні **Додавання програми**.

Натисніть кнопку **OK**. Ця програма з'явиться (із установленим прапорцем) на вкладці **Виключення** в групі **Програми й служби**.

Натисніть кнопку **OK**.

Якщо програму як і раніше не вдалося знайти, можна відкрити порт (див. додаток 3). Порт подібний маленьким дверцям у брандмауері, через які дозволяється взаємодіяти. Щоб визначити, який порт потрібно відкрити, на вкладці **Виключення** натисніть кнопку **Додати порт**. (Відкривши порт, не забудьте знову закрити його, коли перестанете використовувати.)

Додавання виключення переважніше, ніж відкриття порту, із наступної причини:

- Простіше зробити;
- Немає необхідності з'ясовувати номер використовуваного порту;
- Додавання виключення допомагає підтримувати безпеку, оскільки брандмауер відкритий тільки в той час, коли програма чекає підключення до неї.

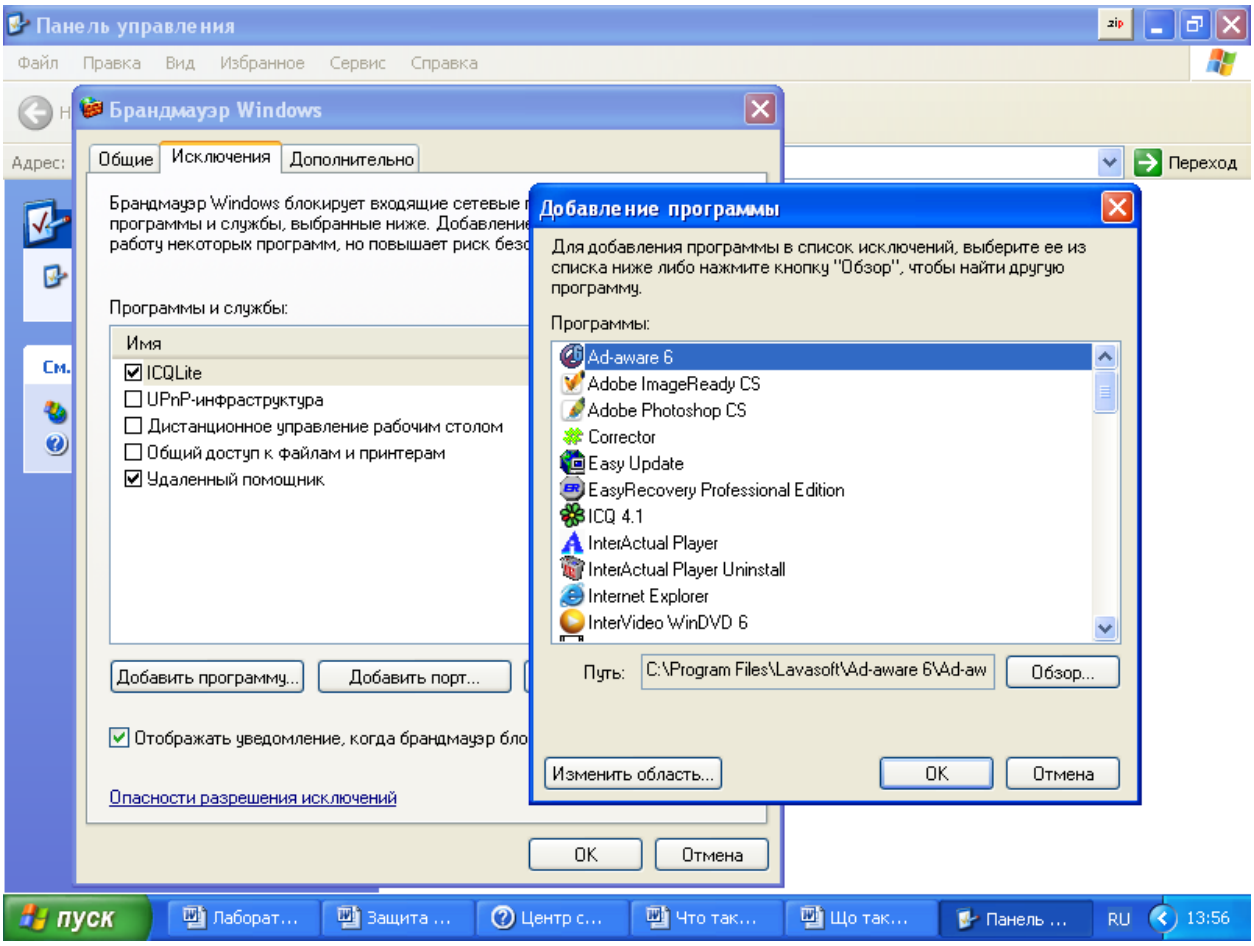


Рис. 2.8. Вікно додавання програми до списку виключень

Щоб змінити порт або параметри програми:

Для виконання цієї процедури необхідно увійти до системи з обліковим записом «Адміністратор» . Для проглядання списку активних портів комп'ютера введіть

команду Netstat –a з командного рядка (рис. 2.9).

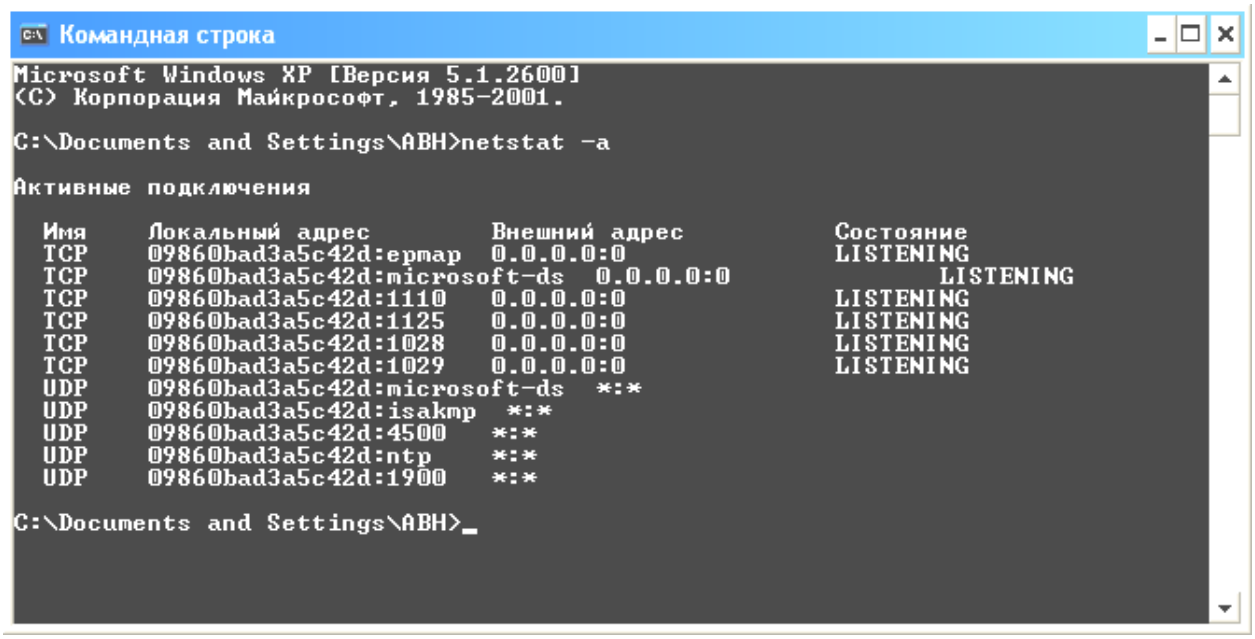


Рис. 2.9. Список активних портів комп'ютера

1. Відкрийте брандмауер Windows.

На вкладці **Виключення** виберіть програму або службу, для якої потрібно змінити параметри порту, і натисніть кнопку **Змінити**.

У діалоговому вікні **Зміна** порту або **Зміна програми** виберіть параметри, які потрібно змінити.

Визначення активних параметрів брандмауера Windows.

Поєднання параметрів на вкладці **Виключення** і будь-які додаткові параметри в розділі **Параметри** мережевого підключення на вкладці **Додатково** називаються «Результуючим набором» параметрів брандмауера Windows.

Для кожного підключення результуючий набір параметрів може бути різним. Параметри, що відкривають порт для певного підключення, мають вищий пріоритет у порівнянні з глобальними параметрами, які можуть забороняти відкриття цього порту. У табл. 2.3. приведені декілька прикладів.

Таблиця 2.3

Поєднання параметрів брандмауера Windows

Глобальний параметр	Параметр для підключення	Результуючий набір

Відключено	Відключено	Відключено
Включено (підмережа)	Відключено	Включено (підмережа)
Включено (глобально)	Відключено	Включено (глобально)
Відключено	Включено	Включено
Включено (підмережа)	Включено	Включено (глобально)
Включено (глобально)	Включено	Включено (глобально)

Якщо брандмауер Windows включений, можна вести журнал (або запис) безпеки, в який записуються успішні підключення, що здійснюються через брандмауер, і підключення, які блокуються (утрачені пакети).

Якщо журнал налаштований на запис утрачених пакетів, збираються відомості про кожну спробу подолання брандмауера, яка виявляється й блокується брандмауером Windows. Наприклад, якщо параметри протокола ICMP (Internet Control Message Protocol) не вирішують вхідні ехо-запити, наприклад, такі, які посилаються командами Ping і Tracert, і подібний луна-запит одержаний із зовнішньої мережі, цей запит відхиляється і відомості про це записуються в журнал.

Якщо журнал налаштований на запис успішних підключень, збираються відомості про кожне успішне підключення, яке здійснюється через брандмауер. Наприклад, коли комп'ютер успішно підключається до веб-вузла за допомогою веб-оглядача, це підключення записується в журнал.

Журнал безпеки

Складається з двох розділів.

- У заголовку відображаються відомості про версії журналу безпеки і про поля, які доступні для введення даних, куди можна додавати зведення;

- У журналі міститься повний звіт із усією зібраною й записаною інформацією про трафік або спроби підключення через брандмауер. Журнал безпеки є динамічним списком, а нові записи даних відображаються в нижній частині журналу.

Примітки:

Ведення журналу безпеки брандмауера Windows за умовчанням відключено.

Щоб включити параметри ведення журналу безпеки

Для виконання цієї процедури необхідно увійти до системи з обліковим записом «Адміністратор».

Відкрийте брандмауер Windows. На вкладці **Додатково** в групі **Ведення журналу безпеки** натисніть кнопку **Параметри**.

Виберіть один із наступних параметрів:

- Щоб включити реєстрацію невдалих спроб установлення вхідного підключення, встановіть прапорець Записувати пропущені пакети;
- Щоб уключити реєстрацію успішних витікаючих підключень, встановіть прапорець Записувати успішні підключення.

Щоб змінити розмір файлу журналу безпеки

Для виконання цієї процедури необхідно увійти до системи з обліковим записом «Адміністратор». Також необхідно включити брандмауер Windows.

На вкладці Додатково в групі Ведення журналу безпеки натисніть кнопку Параметри.

У полі Граничний розмір файлу журналу: уведіть новий розмір файлу або використовуйте клавіші із стрілками для його завдання.

За умовчанням граничний розмір журналу безпеки рівний 4096 КБ. Максимальний розмір файлу журналу складає 32 767 КБ.

При перевищенні допустимого розміру файлу pfirewall.log відомості, що зберігалися в цьому файлі, зберігаються у файл з ім'ям pfirewall.log.old. Нові відомості зберігаються у файлі з ім'ям pfirewall.log.

Шифрування даних за допомогою операційної системи Windows XP.

Файлова система (EFS) забезпечує ядро технології шифрування файлів, використовуваної для збереження шифрованих файлів на томах файлової системи NTFS. Після того як файл або каталог зашифровані, із ними працюють так само, як і з іншими файлами чи каталогами.

Шифрування є прозорим для користувача, що зашифрував файл. Це означає, що перед використанням файл не потрібно розшифровувати. Можна, як, звичайно, відкрити файл і змінити його.

Використання EFS подібне з використанням дозволів для файлів і каталогів. Обидва методи використовуються для обмеження доступу до даних. Але зловмисник, що одержав несанкціонований фізичний доступ до зашифрованих файлів і каталогів, не зможе їх прочитати. При його спробі відкрити або скопіювати зашифрований файл або каталог з'явитися повідомлення, що доступу немає. Файли й каталоги не захищені від несанкціонованих фізичних атак.

Шифрування і розшифровування файлів виконується установкою властивостей шифрування для каталогів і файлів, як встановлюються й інші атрибути, наприклад, «тільки читання», «стиснутий» або «схований». Якщо шифрується каталог, усі файли і підкаталоги, створені в зашифрованій каталогові, автоматично шифруються. Рекомендується використовувати шифрування на рівні каталоги.

Файли й каталоги можуть також бути зашифровані або розшифровані за допомогою команди cipher. При роботі з зашифрованими файлами і каталогами варто враховувати наступні повідомлення й рекомендації. Можуть бути зашифровані тільки файли і каталоги, що знаходяться на файлрвій системі NTFS. Оскільки протокол WebDAV працює з файловою системою NTFS, для шифрування файлів за допомогою протоколу WebDAV потрібно система NTFS.

Стиснуті файли й каталоги не можуть бути зашифровані. Якщо шифрування виконується для стиснутого файлу чи каталогу, файл або каталог перетворяться до стану без стиску. Зашифровані файли можуть стати розшифрованими, якщо файл копіюється або переміщається на файлову систему, яка не є файловою системою NTFS.

При переміщенні незашифрованих файлів у зашифровану каталог вони автоматично шифруються в новій каталогові. Однак зворотна операція не приведе до автоматичної розшифровування файлів. Файли необхідно явно розшифрувати.

Не можуть бути зашифровані файли з атрибутом «Системний» і файли в структурі каталогів системний кореневий каталог.

Шифрування каталогу або файлу не захищає їх від видалення. Будь-який користувач, що має права на видалення, може видалити зашифровані каталоги або файли. З цієї причини рекомендується використання EFS у комбінації з можливостями системи NTFS.

Можуть бути зашифровані або розшифровані файли й каталоги на віддаленому комп'ютері, для якого дозволене віддалене шифрування. Однак якщо зашифрований файл відкривається за мережею, передані при цьому за мережею дані не будуть зашифровані. Інші протоколи, наприклад, SSL/TLS або IPSec, повинні використовуватися для шифрування даних, переданих за мережею. Протокол WebDAV дозволяє локально зашифрувати файл і передати його в зашифрованому виді.

Шифрування файлу або каталогу

Відкрийте провідник Windows. Клацніть правою кнопкою миші на файлі чи каталозі, що потрібно зашифрувати, і виберіть із контекстного меню команду **Властивості**. На вкладці **Загальні** натисніть кнопку **Інші** (рис. 2.10). Установіть прапорець **Шифрувати вміст для захисту даних** (рис. 2.11).

Коли шифрується окремий файл, система запросить підтвердження необхідності зашифрувати також і каталог, що містить цей файл. Якщо підтвердження отримане, усі файли і підкаталоги, що додаються в каталог в майбутньому, будуть зашифровані при додаванні.

Коли шифрується каталог, система запросить підтвердження необхідності зашифрувати також файли і підкаталоги в даній каталогові. Якщо підтвердження отримане, усі файли і підкаталоги, розташовані в каталогові, шифруються, так само як і усі файли і

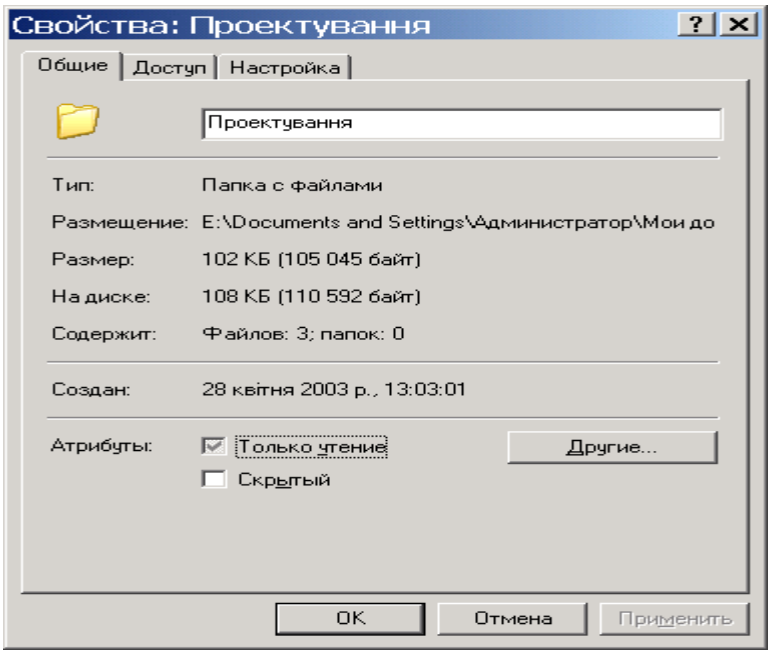


Рис. 2.10. Вікно властивостей каталогу.

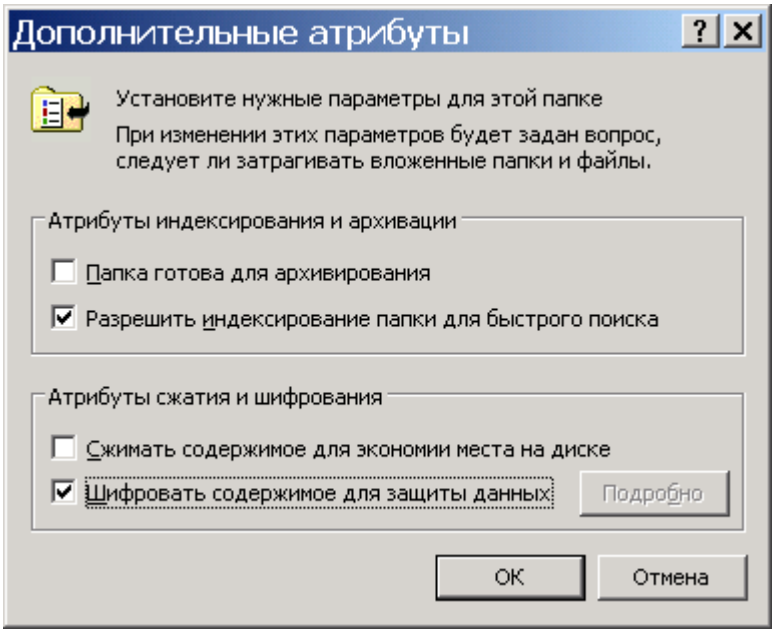


Рис. 2.11. Вікно вибору процесу шифрування.

підкаталоги, що будуть додані в каталог в майбутньому. Якщо обране шифрування тільки каталоги, усі файли і підкаталоги в даній каталогові залишаються незашифрованими. Однак будь-які файли і підкаталоги, що додаються в каталог в майбутньому, будуть зашифровані при додаванні.

Розшифровування файлу або каталогу

Відкрийте **провідник** Windows. Правою кнопкою миші клацніть зашифрований каталог або диск, потім виберіть команду **Властивості**. На вкладці **Загальні** на-

тисніть кнопку **Додатково**. Зніміть прапорець **Шифрувати вміст для захисту даних**. Коли розшифровується каталог, система запросить підтвердження необхідності розшифровувати також файли і підкаталоги в даній каталогові. Якщо обране розшифровування тільки каталоги, зашифровані файли й каталоги в розшифрованій каталогові залишаються зашифрованими. Однак нові файли й каталоги, створювані в розшифрованій каталогові, не будуть зашифровуватися автоматично.

Шифрування та дешифрування файлів та каталогів на віддаленому комп'ютері.

Щоб зашифрувати файл або каталог на віддаленому комп'ютері необхідно відкрити **провідник** Windows. У меню **Сервіс** виберіть команду **Підключити мережний диск** і потім виконуйте інструкції у діалоговому вікні Підключення мережного диска. Клацніть правою кнопкою миші файл або каталог, що потрібно зашифрувати, і виберіть із контекстного меню команду **Властивості**. На вкладці Загальні натисніть кнопку **Додатково**.

Установіть прапорець **Шифрувати вміст для захисту даних**.

Примітки:

Файли і каталоги можуть бути зашифровані тільки на томах із файловою системою NTFS.

Стиснуті файли й каталоги не можуть бути зашифровані. Якщо шифрування виконується для стиснутого файлу чи каталогу, файл або каталог перетворяться до стану без стиску. Не можуть бути зашифровані файли з атрибутом «Системний» і файли в структурі каталогів системний кореневий каталог.

У середовищі домена віддалене шифрування виключене за замовчуванням. Щоб дозволити шифрування для конкретного комп'ютера, адміністратор домена може зробити цей комп'ютер доступним для делегування. Коли шифрується каталог, система запросить підтвердження необхідності зашифрувати також файли і підкаталоги в даній каталогові. Якщо підтвердження отримане, усі майбутні файли і підкаталоги, що додаються до каталоги, будуть зашифровані автоматично.

Програми, що створюють тимчасові робочі файли, можуть поставити під загрозу безпеку шифрування файлу. При роботі з такими програмами використовуйте шифрування на рівні каталоги, а не окремих файлів.

Використання програми перевірки підпису файлу

Інколи при установці на комп'ютері нових програм системні файли й файли драйверів пристроїв заміняються несумісними версіями чи версіями, що не мають цифрового підпису, що приводить до нестабільної роботи системи. Системні файли і файли драйверів пристроїв, включені до складу Windows XP, постачені цифровим підписом Microsoft, що означає, що це оригінальні, незмінені файли, що вони схвалені корпорацією Microsoft для використання в системі Windows. За допомогою програми перевірки підпису файлу можна знаходити на комп'ютері непідписані файли (рис. 2.12) й одержувати наступні відомості про їх:

- ім'я файлу;
- місце розташування файлу;
- дата зміни файлу;
- тип файлу;
- номер версії файлу.

Відкрийте вікно **Перевірка підпису файлу**. Якщо використати в діалоговому вікні (рис. 2.13) кнопку **Дополнительно**, то це дасть можливість пошуку різноманітних файлів та можливість вибору журналу і параметрів його ведення.

Щоб запустити програму перевірки підпису файлу, виберіть у меню **Пуск** команду **Виконати**, уведіть **sigverif** і натисніть кнопку **ОК** (рис. 2.14).

Захист інформації при застосуванні операційної системи Windows NT

Як правило, відразу при запуску системи машина автоматично запитує Login name (те ж саме, що і user ID) і пароль.

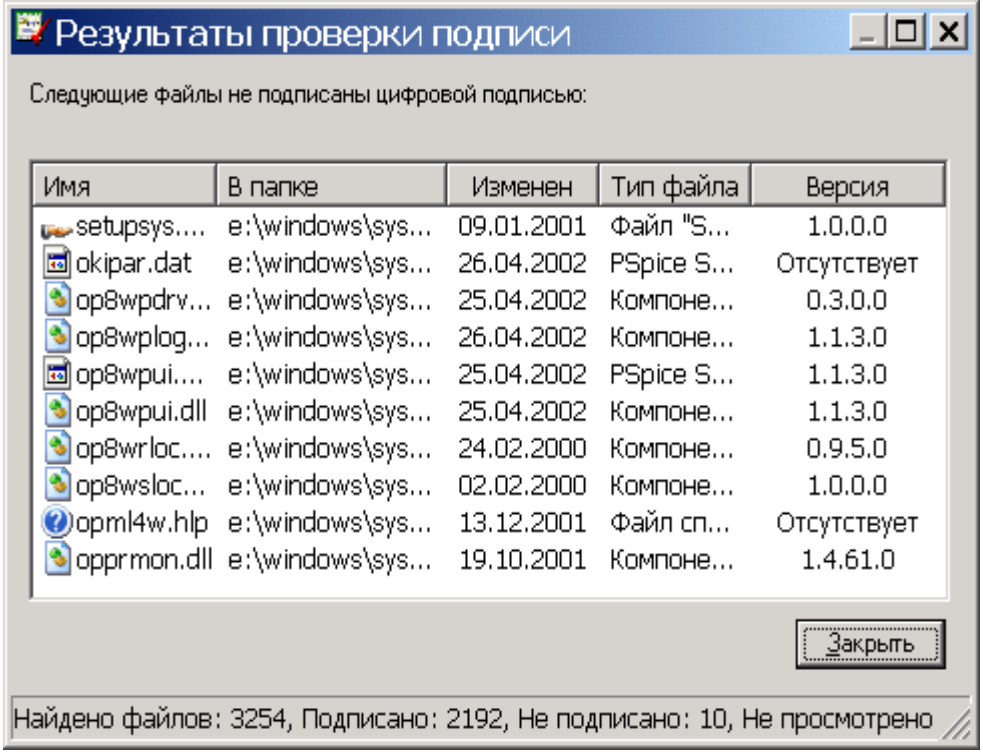


Рис. 2.12. Вікно зі списком системних файлів без цифрового підпису фірми Microsoft.

Налагодження мережі Windows for Workgroups проводиться через **панель керування**, піктограму "**мережа**". У діалогове віконце, на робочій станції, вводиться ім'я машини і номер робочої групи; провадиться Налагодження відповідних служб і

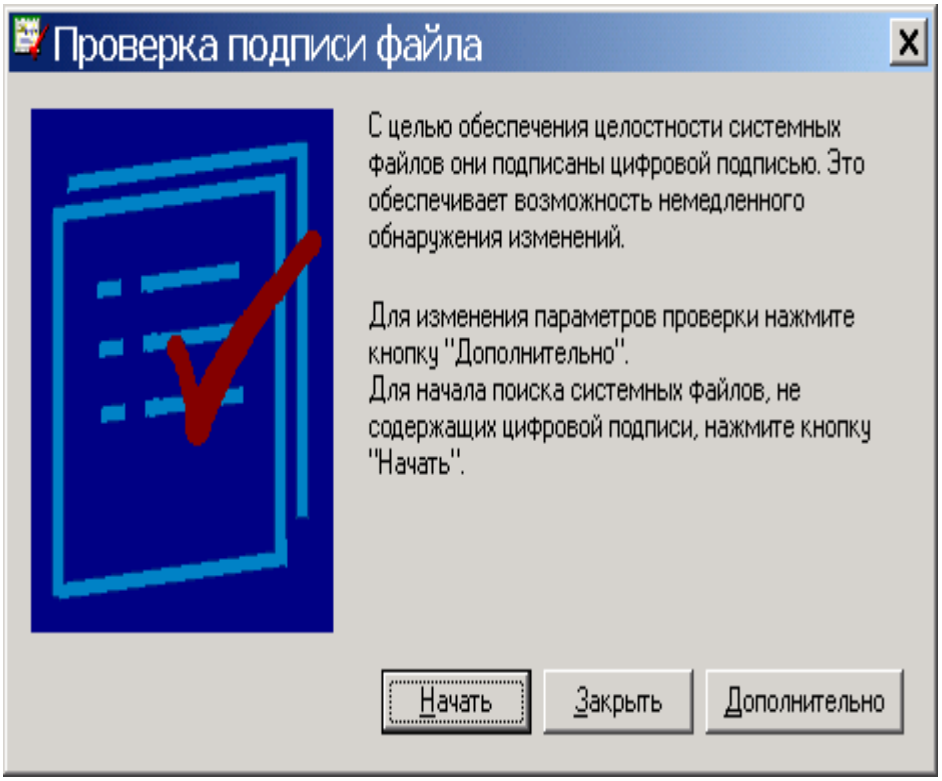


Рис. 2.13. Вікно перевірки підпису файлу.

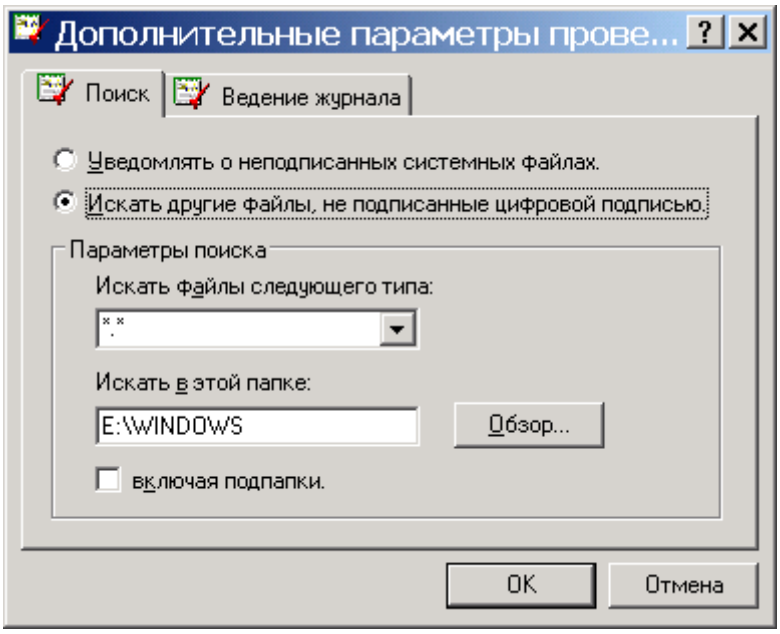


Рис. 2.14. Вибір параметрів

протоколів; настроюються мережні адаптери, прив'язки; у протоколі TCP/IP для кожного мережного адаптеру вказують IP адресу робочої станції, маску підмережі, основний шлюз, настроюють службу DNS, вказуючи ім'я вузла, домен, порядок пошуку служби DNS, адреса WINS, параметри маршрутизації.

Розглянемо роботу комп'ютера на якому встановлена операційна система Windows NT. Для одержання доступу до мережі двічі клацніть піктограму "**Мережеве оточення**" на **робочому столі** , а потім **двічі клацніть значок комп'ютера**. Якщо потрібного комп'ютера немає в списку, двічі клацніть піктограму "**Вся мережа**".

Пошук комп'ютера в мережі

Натисніть кнопку **Пуск**, виберіть команду **Знайти**, а потім виберіть **Комп'ютер**. Якщо відомо ім'я комп'ютера, запишіть його в поле **Ім'я**. Наприклад,: **marketing.**

Використання мережного принтера

Двічі клацніть піктограму "**Мережне оточення**" і знайдіть комп'ютер, на якому знаходиться принтер. **Двічі клацніть піктограму комп'ютера**, а потім **двічі клацніть піктограму принтера**.

Призначення загального каталогу

У вікні **Мій комп'ютер** або в **провіднику** Windows виберіть каталог, що потрібно зробити загальним. У меню **Файл** виберіть команду **Властивості**. Виберіть вкладку **Доступ**, а потім виберіть параметр **Открыть доступ к этой папке** (рис. 2.15). Виберіть тип доступу в групі Тип доступу і, при необхідності, уведіть пароль, а також установіть максимальне число користувачів при необхідності. встановіть для них дозвіл (натисніть кнопку Разрешение) та виберіть тип доступу й групи користувачів, які будуть мати доступ до каталогу.

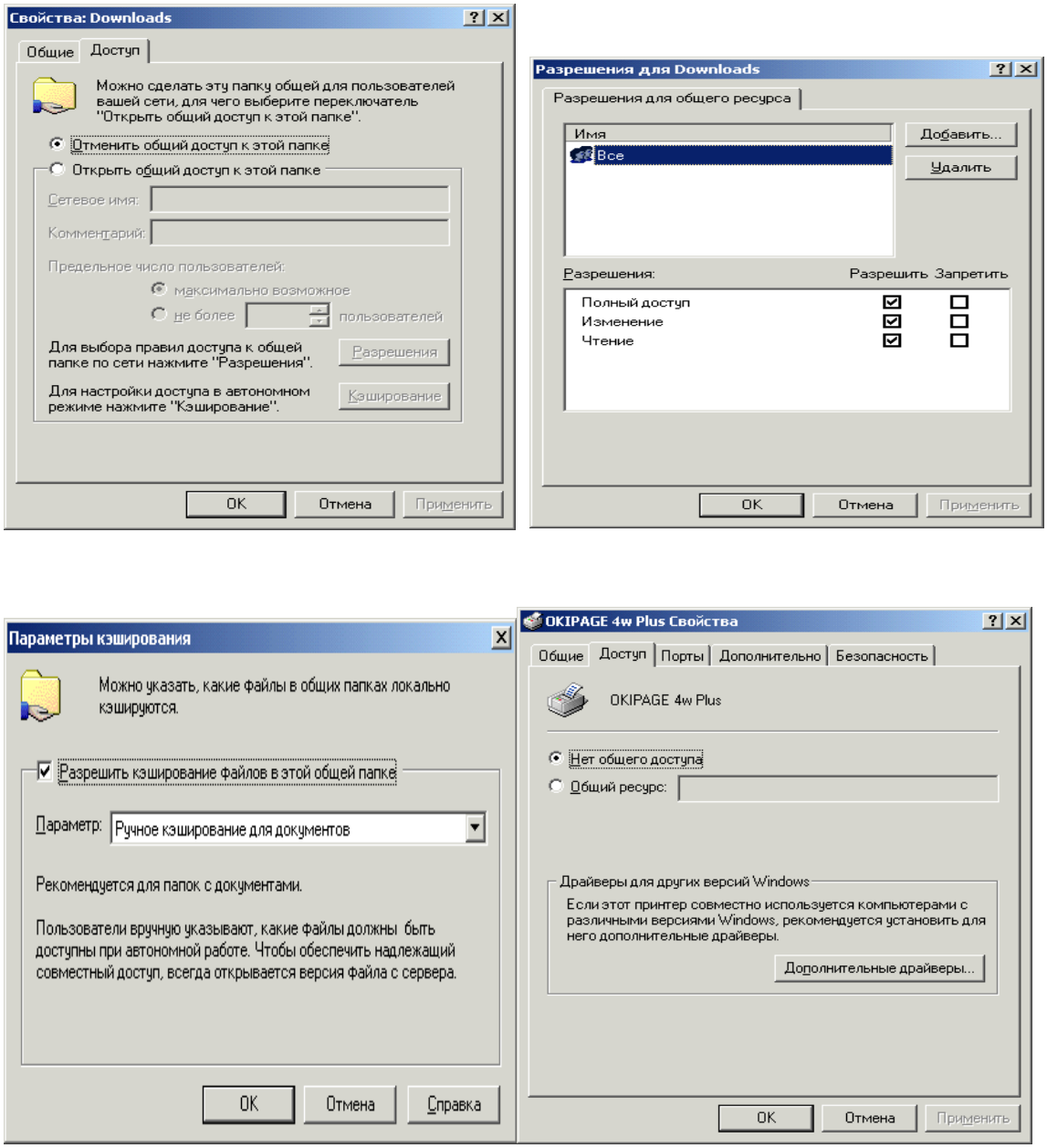


Рис. 2.15. Вибір типу доступу до каталога.

При налагоджені доступу в автономному режимі натисніть кнопку **Кеширование**.

Призначення загального принтера

Натисніть кнопку **Пуск**, виберіть команду **Налагодження**, а потім виберіть **Принтери**. Клацніть значок принтера, який потрібно зробити загальним. У меню **Файл** виберіть команду **Властивості**. Виберіть вкладку **Доступ**, а потім виберіть параметр **Загальний ресурс**.

Керування доступом до каталогів і принтерів

У вікні **Мій комп'ютер** або у вікні **провідника** виберіть загальну каталог або принтер, доступ до яких потрібно обмежити. У меню **Файл** виберіть команду **Властивості**. Виберіть вкладку **Доступ**. Якщо застосовується керування доступом на рівні користувачів, натисніть кнопку **Додати** для вказівки користувачів, разом із якими варто використовувати принтер або каталог. Якщо застосовується керування доступом на рівні ресурсів, уведіть пароль для доступу до каталогу або принтера.

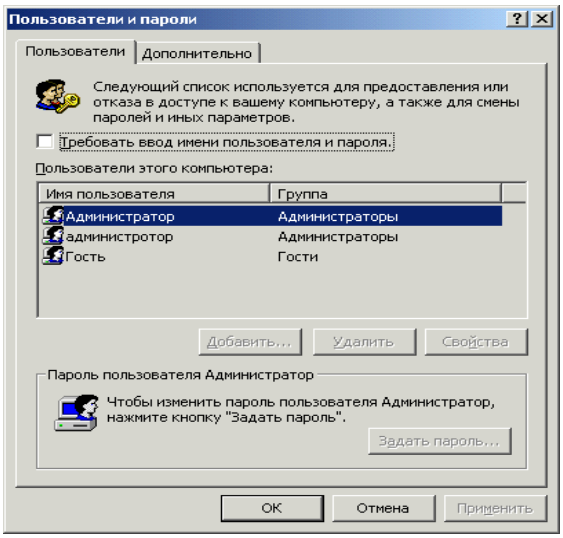


Рис. 2.16. Вікно користувачів.

Зміна мережевого пароля

Для відкриття діалогового вікна **Властивості**: Паролі треба натиснути кнопку **Пуск**, вибрати команди **Налагодження** і **Панель керування**, а потім **двічі клацнути значок Користувачі** (рис. 2.16).

Натисніть кнопку Задати паролі.

Виберіть пароль, що потрібно перемінити, і натисніть кнопку **Змінити**. Уведіть старий пароль. Уведіть новий пароль, а потім знову введіть його в поле **Підтвердження пароля**.

Щоб дозволити іншому користувачу входити в мережу з цього комп'ютера, у вікні Запровадження мережного пароля введіть нові значення в поля користувач і **Пароль**, а потім натисніть кнопку **OK**.

Указівка імені комп'ютера і робочої групи

Для відкриття діалогового вікна **Мережа** можна натиснути кнопку **Пуск**, вибрати команди **Налагодження** й **Панель керування**, а потім двічі клацнути значок **Мережа**. Виберіть вкладку **Ідентифікація**. Уведіть ім'я комп'ютера. Ім'я комп'ютера повинно бути унікальним. Неможливо використовувати ім'я, що уже використовується в мережі. Можна також увести опис комп'ютера. Ці дані будуть доступні для інших користувачів при перегляді списку мережних комп'ютерів.

Призначення прав адміністратора, користувача, гостя.

На комп'ютері з операційною системою Windows NT натисніть кнопку **Пуск** і виберіть команди **Програми** й **Адміністрування**, **Локальна політика безпеки** , а потім Політика враховуючих записів, виберіть **Політика паролів** (рис. 2.17), аналогічно вибираються права користувача (рис. 2.18). Виконуйте інструкції, які виводяться на екран. На комп'ютері з операційною системою Windows 95 або більш пізньої натисніть кнопку **Пуск**, виберіть команди **Програми**, **Стандартні й Службові**, а потім виберіть **Призначені завдання**.

На комп'ютері з операційною системою Windows NT натисніть кнопку **Пуск** і виберіть команди **Програми** й **Адміністрування**, **Призначення прав користувача**. Виконуйте інструкції, які виводяться на екран під час роботи майстра. Аналогічно перегляньте локальну політику , політику відкритого ключа, політику безпеки IP. Натисніть кнопку **Пуск** і виберіть команди **Програми й Адміністрування**, Управління комп'ютером та перегляньте відповідні можливості діалогових вікон (рис 2.19).

Використання інспектора для контролю за використанням загальних ресурсів

Інспектор мережі дозволяє з'ясувати, хто саме використовує загальні ресурси вашого комп'ютера. Він також дає можливість відкривати спільний доступ до ресурсів і відключати інших користувачів від комп'ютера або окремих файлів.

Установка інспектора постановки клієнта для мереж Microsoft, а також запуску служби доступу до файлів і принтерів комп'ютера.

Для запуску інспектора натиснути кнопку **Пуск**, вибрати команди **Програми, Стандартні й Службові**, а потім вибрати команду **Інспектор**.

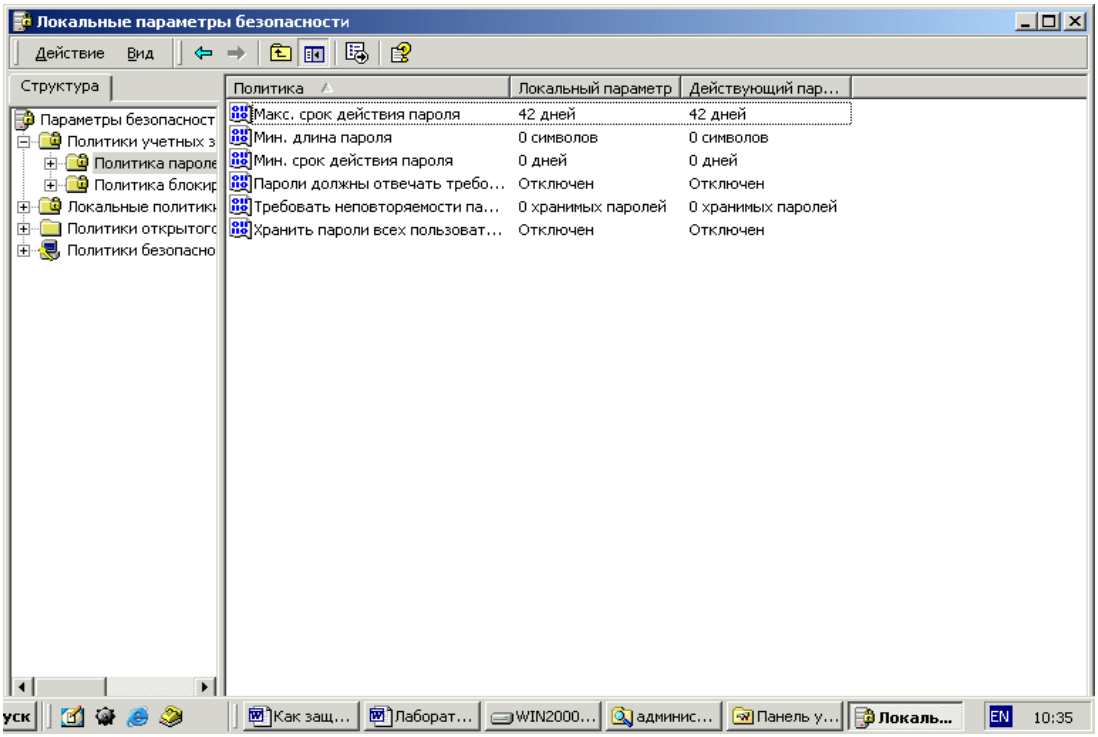


Рис. 2.17. Призначення параметрів паролів адміністратора, користувача, гостя.

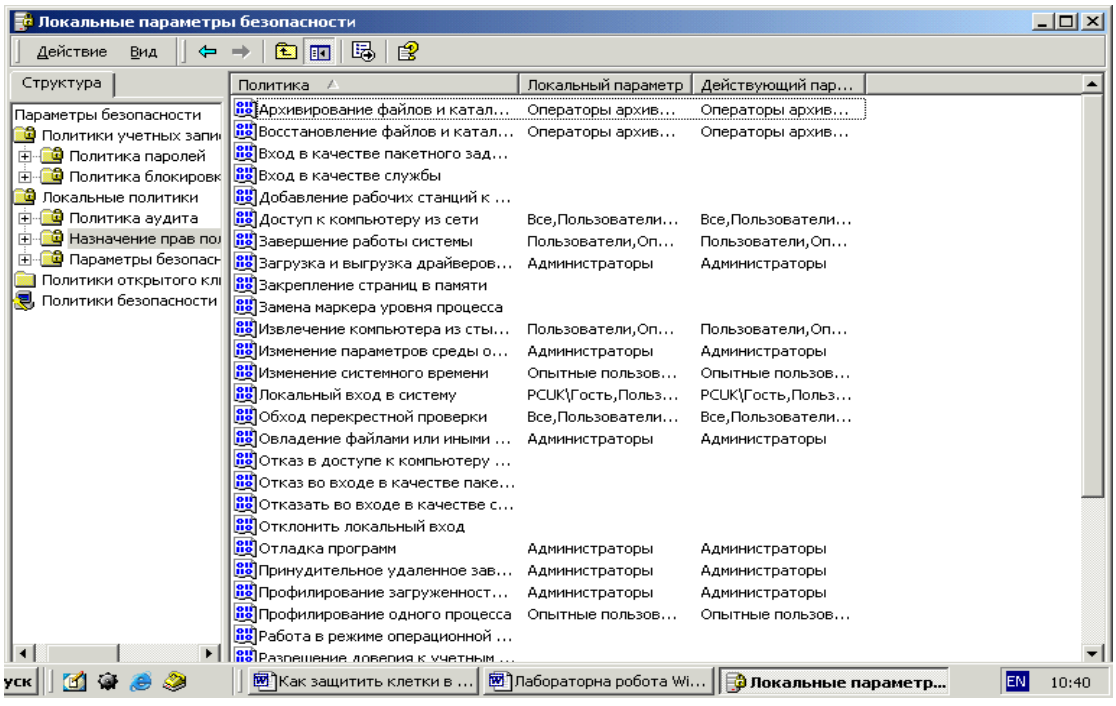


Рис. 2.18. Підбір прав користувачів.

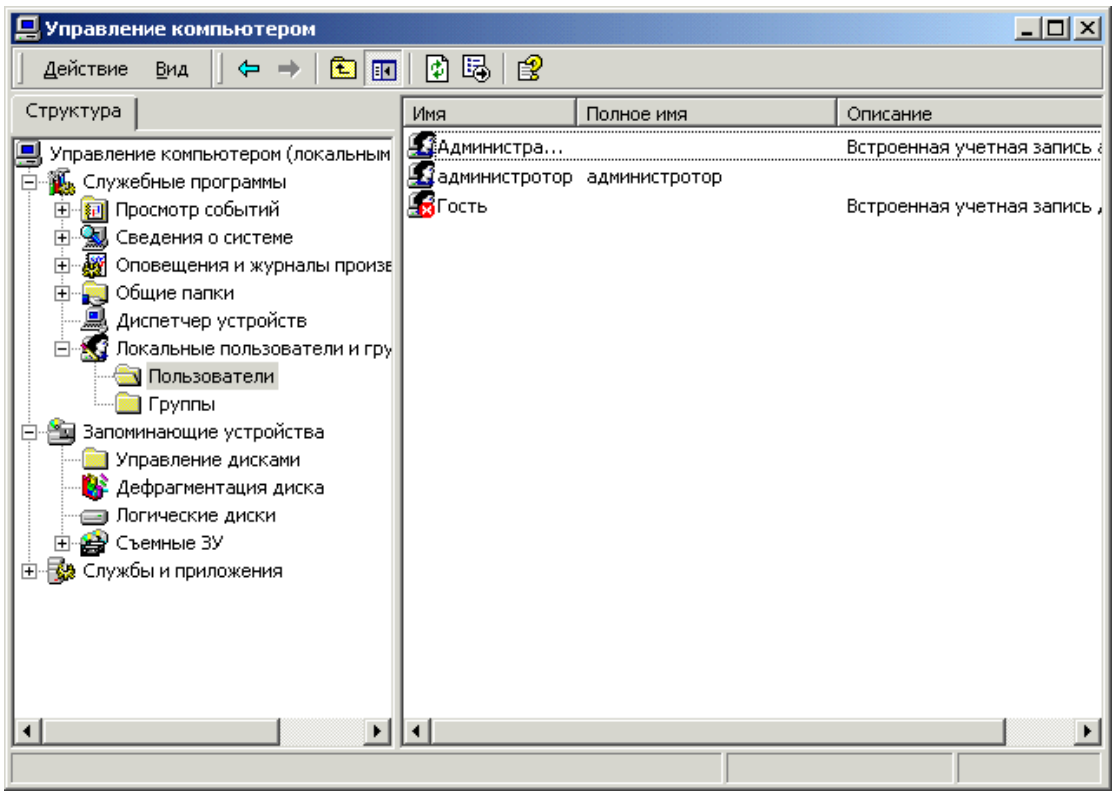


Рис. 2.19. Підбір параметрів безпеки.

КОНТРОЛЬНІ ПИТАННЯ

1. Як установлюється парольний захист для BIOS?
2. Які можливості є для зняття паролю з BIOS?
3. Як установлюється парольний захист для Windows?
4. Як установлюється парольний захист комп'ютера в режимі чекання?
5. Як установлюється парольний захист комп'ютера в режимі сплячки?
6. Як запускається Windows у режимі захисту від збоїв?
7. Для чого і коли використовується режим запуску комп'ютера в режимі захисту від збоїв?
8. Як проводиться керування доступом до каталогів та файлів на рівні користувачів?
9. Як проводиться керування доступом до каталогів та файлів на рівні ресурсів?
10. Як проводиться налагодження параметрів брандмауера Windows?
11. Як проводиться налагодження параметрів журналу безпеки?

12. Як відкрити (закрити) доступ до порта комп'ютера?
13. Як дозволити (заборонити) повний доступ програми до Інтернету.
14. В якій файловій системі можливий процес шифрування?
15. Чому рекомендується разом із процесом шифрування використовувати атрибути для захисту файлової системи?
16. Вимоги до файлів, які підлягають шифруванню.
17. Порядок шифрування файлів та каталогів на комп'ютері.
18. Порядок дешифрування файлів та каталогів на комп'ютері.
19. Порядок шифрування файлів та каталогів на віддаленому комп'ютері.
20. Використання програми перевірки підпису файлу.
21. Для чого потрібна перевірка підпису файлу?
22. Призначення прав групі користувачів.
23. Створення груп користувачів.

Розділ 3.

ЗАХИСТ ІНФОРМАЦІЇ В ПРОГРАМАХ MICROSOFT OFFICE.

Не секрет, що програмний пакет Microsoft Office є найпопулярнішим і найбільш використовуваним для підготовки документів. При роботі з додатками MS Office виникає проблема забезпечення конфіденційності інформації, що зберігається в документах. На жаль не всі способи захисту, реалізовані в цьому пакеті, дозволяють надійно захистити інформацію.

Захист від фішингових схем в Microsoft Office

Фішинг (від англійського слова «fishing») - це вид мережевого шахрайства, націлений на те, щоб користувач надав свої особисті дані зловмисникам.

Існує безліч способів обману користувачів, у тому числі створення адреса електронної пошти й веб-вузлів, що імітують популярні й надійні торговельні марки. Звичайно, при фішинг-атаці використовуються підроблені повідомлення електронної пошти, замасковані під повідомлення від широко відомої компанії або Інтернет-ресурсу, наприклад, від банку, компанії, що випускає кредитні карти, благодійної організації, або Інтернет-магазина. Ціль цих облудних дій — змусити користувача представити дані особистої ідентифікації (Інформація особистого порядка (PII). Будь яка інформація, яка містить детальні відомості про людину, в тому числі його ім'я, країна проживання, домашня адреса, адреса електронної пошти, номер кредитної карти, номер посвідчення особи, IP-адреса або номер іншого документа, який посвідчує особистість.), наприклад:

Ім'я користувача

Адреса й номер телефону

Пароль або PIN-Код

Номер банківського рахунку

Номер пластикової карти (платіжної або кредитної)

Код дійсності (Код перевірки карти. Код, який використовується компаніями, що випускають кредитні карти, для авторизації розходів закредитною картою.

Наприклад, American Express використовує в якості цього кода чотиризначне ое число на титульній стороні кредитної карти, а Visa, MasterCard і Discover трьохначне число на їїі оберненій стороні.) кредитної карти (CVC) або її контрольний параметр (CVV)

Номер соціального страхування

Ці відомості можуть використовуватися для різноманітних фінансових махінацій. Найпоширеніший спосіб - крадіжка ідентифікаторів дійсності, за допомогою яких зловмисники, маючи у своєму розпорядженні особисті дані користувача, можуть підтвердити його дійсність, і діяти від його ім'я, наприклад:

Подати заявку й одержати кредит.

Зняти всі гроші з банківського рахунку, і витратити ліміт на кредитних картах користувача.

Переказати гроші з накопичувального або кредитного рахунків на чековий, а потім, використовуючи копію платіжної карти користувача, знімати готівку із чекового рахунку через банкомати з усьому світі.

Приклади й характеристики фішингових схем

Підроблені повідомлення електронної пошти — користувач одержує повідомлення, подібне за зовнішніми ознаками з офіційним повідомленням від компанії, з якою він веде справи. Лист попереджає про необхідність звірити реквізити банківського рахунку й про припинення банківських операцій доти, поки відповідні дані не будуть надані.

Сполучення обману при торгах і підроблених веб-вузлів умовно депонованих платежів Предмети виставляються для продажу на легальних мережевих аукціонах після чого покупців шляхом обману змушують оформити оплату на підробленому веб-вузлі умовно депонованих платежів.

Підробка оплати торговельних операцій у мережі. Зловмисник пропонує угоду: він купує товар, але ціна в рахунку на оплату буде трохи вище заявленої, а отриману різницю продавець поверне покупцеві, виписавши й відіславши чек. Товар так і не оплачується, а із чеку, відправленому зловмисникові, він одержує суму

різниці. Крім того, у чеку міститься номер банківського рахунку користувача, банківський код, адреса й номер телефону, а значить зловмисник може використовувати ці відомості для подальших махінацій.

Фіктивні благодійні організації — у цій схемі фішингу до користувача звертаються від імені благодійної організації й просять надати матеріальну підтримку. На жаль, на почутті жалю намагаються заробити багато хто.

Підроблені веб-вузли — зовні вони схожі на справжні. При відвідуванні цих веб-вузлів на комп'ютер може автоматично завантажитися потенційно небезпечне програмне забезпечення, наприклад комп'ютерний вірус (Вірус. Компьютерна програма або макрос, «які заражують» файли, вставляючі в них особисту копію. При завантаженні зараженного файла в пам’ять може бути зараження інших файлів. Віруси часто викликають небезпечні побічні ефекти.). Шпигунське програмне забезпечення може записати натискання клавіш при доступі користувача до особистих мережевих облікових записів. Ці відомості передаються шахраю-фішеру. Від такого виду атак можна захиститися, якщо завантажити й установити антишпигунське програмне забезпечення..

Фішингових схем існує набагато більше. Останні відомості про розкритий фішингових схемах див. на веб-вузлі Anti-Phishing Working Group.

Стандартні ознаки фішингової схеми

На жаль, фішинг-атаки стають усі більш хитрими, і звичайному користувачеві не просто визначити підроблені повідомлення електронної пошти або веб-вузли. Тому фішинг-схеми так часто й успішно використовуються зловмисниками. Наприклад, багато підроблених повідомлень електронної пошти й веб-вузли містять емблеми компаній, торговельні марки яких добре відомі й заслуговують довіри. Для захисту від фішингу слідуйте наступним елементарним правилам:

Запит особистої інформації в повідомленні електронної пошти Законослухняні підприємці як правило не використовують електронну пошту для передачі особистих даних. Ставтеся з особливою обережністю до повідомлень, у

яких запитується особиста інформація, навіть якщо вони виглядають цілком правдоподібною.

Терміновий характер стилю викладу. Фішингові повідомлення електронної пошти, звичайно, відрізняються ввічливою й люб'язною формою. Як правило, це спонукує користувача відповісти на повідомлення, або клацнути включене в повідомлення посилання. Щоб збільшити ймовірність відповідей, у листі створюється видимість терміновості, щоб користувач відповідав негайно, не роздумуючи. Звичайно, підроблені повідомлення електронної пошти не адресовані користувачеві особисто, у той час як справжні повідомлення від банку або компанії електронної комерції, клієнтом якої може бути користувач, звичайно, містять особистий обіг. Далі наведений приклад реальної фішингової схеми.

Дорогий клієнт! Наш банк цінує Вашу довіру, і повідомляє про необхідність провести звірення даних про Ваш банківський рахунок через велику кількість неактивних користувачів. У випадку відмови, Ваш обліковий запис буде вилучений. Для звірення даних клацніть наведене нижче посилання.

Вкладення В багатьох схемах фішингу користувача просять відкрити вкладення в повідомленні електронної пошти, що може заразити комп'ютер вірусом (Вірус. Компьютерная програма або макрос, «які заражують» файли, вставляючі в них особисту копію. При завантаженні зараженого файлу в пам’ять може відбутися зараження інших файлів. Віруси часто викликають небезпечні побічні ефекти.) або встановити шпигунське ПЗ. Шпигунське ПЗ на комп'ютері користувача може записати натискання клавіш при доступі користувача до особистих мережевих облікових записів. Будь-які вкладення перед переглядом варто спочатку зберегти, потім перевірити антивірусною програмою з останніми антивірусними базами, а тільки потім відкривати. Щоб захистити комп'ютер користувача, у додатку Outlook автоматично блокуються вкладення з файлами визначених типів, через які можливе поширення вірусів. Якщо в додатку Outlook виявлене підозріле повідомлення, то вкладення, що містять будь-які файли, блокуються.

Підроблені посилання. Творці фішингових повідомлень досить мистецьки вміють уводити в оману так, що звичайний користувач практично не може

відрізнити підроблене посилання від справжнього. Краще у вікні веб-оглядача набирати веб-адресу або URL-URL-адреса (URL-адреса. Адреса, яка вказує протокол (такой як HTTP або FTP) і розташування объекта, документа, веб-сторінки або другого ресурса в Інтернеті або Інтрамережі, наприклад: http://www.microsoft.com/.), який, не викликає сумнівів. Також можна помістити правильний URL-Адреса в папку «Вибране» веб-оглядача. Не слід копіювати URL з повідомлень у вікно веб-оглядача через буфер обміну. Зловмисники можуть використовувати для підробки посилань наступні методи.

Маскування посилань Навіть якщо пропоноване посилання містить повністю або частково назву існуючої компанії, вона може бути «маскованою». Це означає, що відображуване посилання здійснює перехід з невідомої адреси, найчастіше на підроблений веб-вузол. Зверніть увагу, що в цьому прикладі при наведенні покажчика миші на посилання в повідомленні додатка Outlook у полі на жовтому тлі відображається інша числова адреса Інтернету. Це повинно насторожити користувача. Пам’ятайте, що посилання навіть у поле з жовтим тлом може бути підробленої й виглядати як надійна веб-адреса.

Варто також знати про URL, що містять знак «@». Наприклад, адреса URL https://www.woodgrovebank.com@nl.tv/secure_verification.aspx містить перехід на мережний ресурс, що зазначений після знака «@», а не на Wood Grove Bank. Це відбувається тому, що веб-оглядачі ігнорують в URL всі, що йде до знака «@».

У дійсності місця, на яке вказує посилання nl.tv/secure_verification.aspx, цілком може бути небезпечним веб-вузлом

Омограми — це слова з однаковим правописом, але з різними значеннями. У комп'ютерному середовищі атака із застосуванням омограми має на увазі використання веб-адреси, що дуже схожа на відому, але в дійсності такою на являється. Підроблені веб-посилання використовуються у фішингових схемах, щоб шляхом обману змусити користувача клацнути посилання. Наприклад, замість адреси www.microsoft.com можна підставити

- www.micosoft.com або
- www.mircosoft.com.

У більш витончених видах атак із застосуванням омограми веб-адреса виглядає точно також, як адреса справжнього веб-вузла. Це відбувається, коли ім’я домена (Доменне ім’я. Адреса мережевого оточення, яка визначає власника в наступному форматі: сервер.організація.тип. Наприклад, ім’я www.government.ru визначає веб-сервер уряду Росії) створюється за допомогою знаків алфавіту інших мов, не англійського. Наприклад, веб-адреса виглядає як справжня, тому що візуально не можна визначити, що «с» є символом кирилиці російського алфавіту:

www.microsoft.com

Фішери підробляють доменні імена банків і інших компаній, щоб користувач думав,що відвідує знайомий веб-вузол. Для виявлення подібних підробок доменних імен у веб-адресах потрібно спеціальне програмне забезпечення. В 2007 Office здійснюється захист від посилань на підозрілі веб-вузли.

Захист від фішингу й атак із застосуваннями омограм в Microsoft Office

Підозрілі посилання в документах

За замовчуванням у 2007 Office відображаються оповіщення служби безпеки в наступних випадках:

- якщо користувач клацнув у відкритому документі посилання на веб-вузол, адреса якого є підробленим доменним ім'ям;
- якщо користувач відкрив файл із веб-вузла, адреса якого містить підроблене доменне ім'я.

Якщо клацнути посилання на веб-вузол, що використовує, можливо, підроблене доменне ім'я, відображається наступне оповіщення (рис. 3.1).

Потім пропонується вибрати, чи продовжити відвідування підробленого веб-вузла. У даній ситуації рекомендується нажати кнопку НІ. Ця функція допомагає захиститися від атак із застосуванням омограм.

Підозрілі посилання в повідомленнях електронної пошти

За замовчуванням в Microsoft Office Outlook 2007 із підозрілими повідомленнями виконуються наступні дії:

Якщо фільтр небажаної пошти вважає, що повідомлення не є небажаним, але може бути пов'язане з фішингом, повідомлення залишається в папці «Вхідні», але

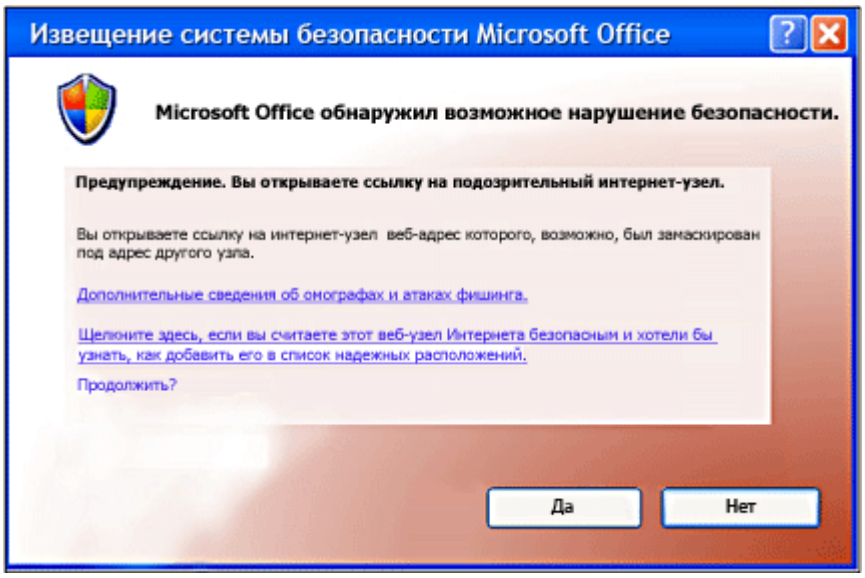


Рис. 3.1 Вікно повідомлення про підроблене посилання

всі посилання в повідомленні відключаються, і скористатися функціями «Відповісти» і «Відповісти всім» неможливо.

Якщо фільтр небажаної пошти вважає, що повідомлення є й небажаним, і пов'язане з фішингом, то повідомлення автоматично направляється в папку Небажана пошта. Усі повідомлення, переміщувані в папку Небажана пошта, перетворяться в звичайний текст, а всі посилання в повідомленні відключаються. Крім того, відключаються функції «Відповісти» і «Відповісти всім». Зміна дій цих функцій відобразиться на інформаційній панелі (рис. 3.2).

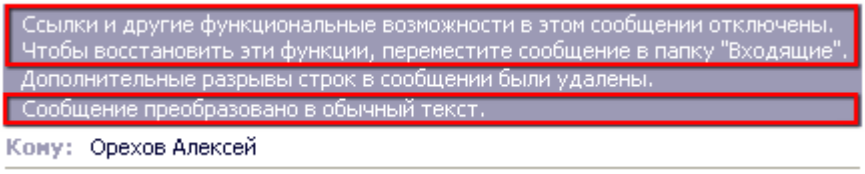


Рис. 3.2 Вікно інформаційної панелі

Якщо клацнути посилання, що було відключено в повідомленні фішингу, відобразиться діалогове вікно Безпека Outlook (рис. 3.3).

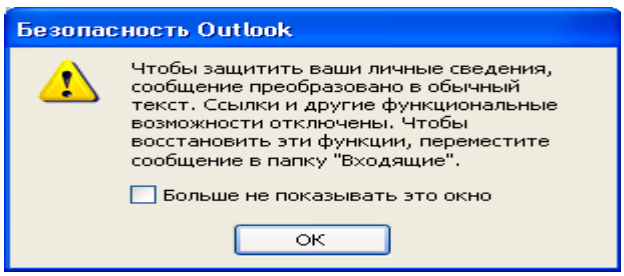


Рис. 3.3 Вікно безпека Outlook.

Щоб і далі одержувати оповіщення про потенційні погрози безпеки, натисніть кнопку ОК. Щоб попередження більше не відображалися, установіть прапорець Більше не показувати це вікно.

Рекомендації із захисту від мережевих шахраїв

Ніколи не відповідайте на повідомлення електронної пошти, у яких запитуються ваші особисті відомості Ставтеся з підозрою до всіх повідомлень електронної пошти від компаній або осіб, у яких запитуються ваші особисті відомості, а також до тих, у яких вам надсилають ваші особисті відомості із проханням їх звірити, або підтвердити. Краще зателефонуєте в цю компанію за номером, що ви одержали від цієї компанії особисто. Не дзвоніть за номером, зазначеним у повідомленні електронної пошти. Не передавайте особисті відомості особам, які подзвонили вам самі.

Не клацайте посилання в підозрілих повідомленнях електронної пошти Не переходите з посиланнях у підозрілому повідомленні. Посилання може бути небезпечним. Замість цього для відвідування веб-вузла введіть у веб-оглядачі URL, або використовуйте посилання в меню «Вибране». Не копіюйте посилання з повідомлень у поле адреси оглядача через буфер обміну.

Не відсилайте особисті відомості в звичайних повідомленнях електронної пошти Звичайні повідомлення електронної пошти не піддаються шифруванню. Якщо повідомлення електронної пошти необхідно використовувати для особистих фінансових операцій, використовуйте додаток Outlook для цифрового підпису і шифрування повідомлень за допомогою захисту S/MIME. В MSN, Microsoft Hotmail, Microsoft Outlook Express, Microsoft Office Outlook Web Access, Lotus Notes, Netscape і Eudora є підтримка захисту S/MIME.

Взаємодійте тільки з відомими й надійними компаніями Користуйтеся послугами добре відомих компаній, що поставляють якісні послуги. На комерційному веб-вузлі повинна бути опубліковане заява про конфіденційність, яка означає, що компанія зобов'язується не передавати відомості про вас третім особам.

Переконайтеся, що на веб-вузлі використовується шифрування. У поле Адреса оглядача перед адресою веб-вузла повинне стояти https:// замість звичайного

http://. Щоб відобразити цифровий сертифікат веб-вузла, у рядку стану оглядача двічі клацніть значок блокування . Ім'я, що стоїть після Кому виданий у сертифікаті, повинне збігатися з ім'ям відвідуваного веб-вузла. У випадку сумнівів негайно покиньте веб-вузол і повідомите про нього. Не виконуйте представлених на цьому веб-вузлі інструкцій.

Поліпшуйте захист комп'ютера Дуже важливо використовувати брандмауер, обновляти програмне забезпечення комп'ютера й використовувати антивірусні програми, особливо при підключенні до Інтернету через телефонний модем або із цифровій абонентській лінії через DSL-Модем. Також доцільно використовувати анти-шпигунську програму. Можна завантажити анти-шпигунське програмне забезпечення Майкрософт або використовувати програми інших виробників.

Стежте за своїми фінансовими операціями Відслідковуйте підтвердження про зроблені замовлення, вивчайте звіти з операціями із кредитною картою й із банківськими операціями відразу після одержання — чи дійсно оплачені тільки проведені вами фінансові операції. Негайно повідомляйте про всі невідповідності в банківському рахунку, подзвонивши на номер, зазначений в інструкції з роботи з банківським рахунком. Використовуйте для покупок у мережі тільки одну кредитну карту, це полегшить контроль за фінансовими операціями.

Для фінансових операцій в Інтернеті використовуйте кредитну карту В більшості регіонів особиста відповідальність користувача при підробці його кредитної карти буде істотно обмежена. Однак при проведенні платежів прямо з банківського рахунку або із платіжної карти користувач відповідає вже за весь баланс засобів на банківському рахунку. Крім того, для використання в Інтернеті більш краща кредитна карта з невеликою граничною сумою кредиту, оскільки сума коштів, що зможе викрасти зловмисник, буде обмежена. Найкраще використовувати «віртуальні», призначені для однократного використання й діючі один або два місяці номера кредитні карти, які великі компанії з випуску кредитних карт стали надавати своїм клієнтам для покупок у мережі.

Повідомлення про мережеве шахрайство й крадіжку ідентифікатора.

У випадку одержання облудного повідомлення електронної пошти можна повідомити про дану проблему, і прикласти підозріле повідомлення. Інформування повноважних органів про підозрілі повідомлення сприяє боротьбі з фішинговими схемами.

У додатку Outlook виберіть, але не відкривайте повідомлення, про яке потрібно повідомити.

У меню Дії виберіть команду Переслати як вкладення, або натисніть сполучення клавіш CTRL+ALT+F.

У поле Кому введіть адресу електронної пошти компанії, яку необхідно інформувати про повідомлення з фішингом. Для повідомлення про підозрілі листи можна використовувати наступні адреси:

reportphishing@antiphishing.org — для відправлення в професійну асоціацію Anti-Anti-Phishing Working Group,

spam@uce.gov — для відправлення в FTC (Federal Trade Commission),

abuse@msn.com — для відправлення в MSN,

abuse@microsoft.com — для відправлення в корпорацію Майкрософт.

Натисніть кнопку Відправити.

Дії із системою безпеки Microsoft Office

Виявлення підроблених доменних імен за замовчуванням включено. Його можна відключити, щоб не відображалися попередження системи безпеки, однак це робити не рекомендується. У перерахованих додатках (Word, Excel, PowerPoint і Access)

Випуск 2007 системи Microsoft Office виконайте наступні дії.

Натисніть кнопку Microsoft Office  , а потім кнопку Параметри, наприклад, в Word (рис. 3.4).

Виберіть категорію Центр керування безпекою, натисніть кнопку Параметри центра керування безпекою, і перейдіть у категорію Параметри конфіденційності (рис. 3.5).

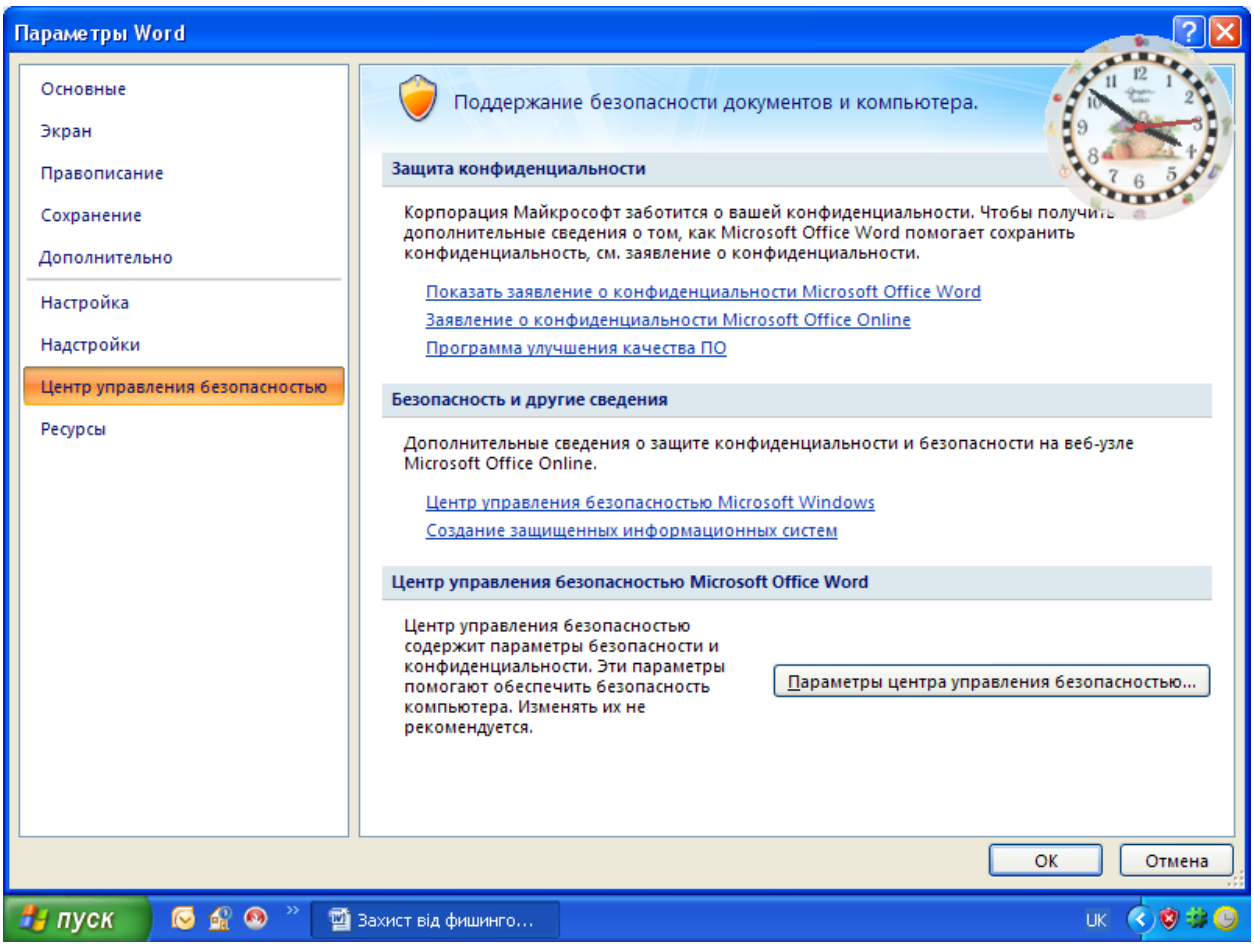


Рис. 3.4 Вікно параметрів Word

Зніміть прапорець Перевірка документів Microsoft Office, узятих із підозрілих веб-вузлів або утримуючих посилань на такі веб-вузли. Visio і InfoPath

У меню Сервіс виберіть команду Центр забезпечення безпеки, і клацніть Параметри конфіденційності.

Зніміть прапорець Перевірка документів Microsoft Office, узятих із підозрілих веб-вузлів або утримуючих посилань на такі веб-вузли.

Відключення оповіщень системи безпеки для веб-вузлів шляхом їхньої позначки як надійних вузлів в Internet Explorer

Якщо відомо, що певний веб-вузол заслуговує довіри, оповіщення можна відключити, додавши цей веб-вузол у зону надійних вузлів оглядача Internet Explorer. У зоні надійних вузлів перебувають веб-вузли, які визначені як безпечні, наприклад, вузли в локальній мережі користувача або вузли з надійних джерел. Додавання веб-вузла в зону надійних вузлів указує, що всі файли, що завантажуються або запускаються із цього веб-вузла, не заподіють шкоди

комп'ютеру, або інформації, що зберігається на ньому. За замовчуванням у зоні надійних вузлів ніяких вузлів немає, а рівень безпеки для зони надійних вузлів установлений «Низький».

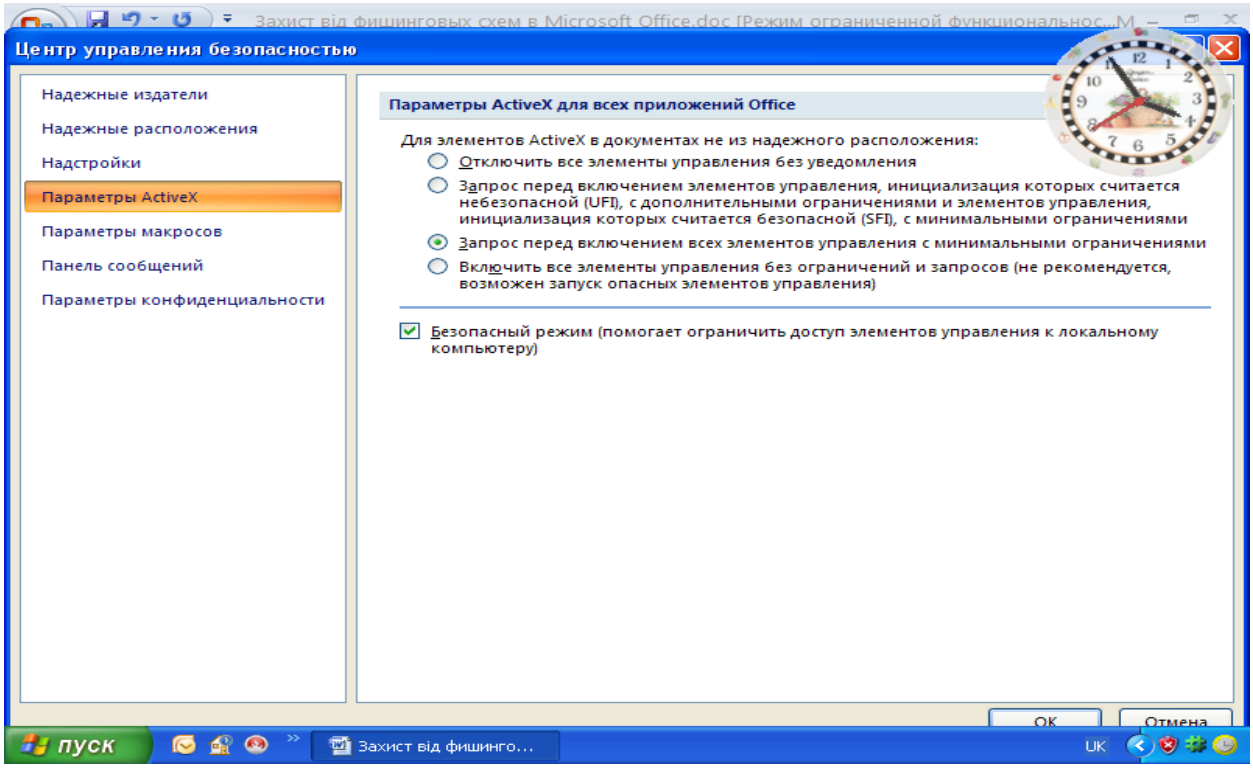


Рис. 3.5 Вікно відключення повідомлень на підозрілі адреси

Додавання веб-вузла в зону надійних вузлів

В оглядачі Internet Explorer версій 5, 6 або 7 виберіть у меню Сервіс команду Властивості оглядача.

На вкладці Безпека клацніть значок Надійні вузли, а потім натисніть кнопку Вузли.

У поле Додати вузол у зону введіть або виберіть адресу конкретного веб-вузла, а потім натисніть кнопку Додати.

Якщо потрібно, щоб в оглядачі Internet Explorer перед підключенням до будь-якого веб-вузла цієї зони перевірялася надійність сервера кожного веб-вузла в цій зоні, установіть прапорець Для всіх вузлів цієї зони потрібна перевірка серверів (https:).

Двічі натисніть кнопку ОК.

Захист інформації у Microsoft Word 2003.

Для захисту змісту файлу в Microsoft Word необхідно з підменю **Сервіс** подати команду **Установити захист**. У діалоговому віконці, яку з'явиться вибрати відповідний тип захисту (рис. 3.6) та ввести пароль. Далі натиснути кнопку **ОК.** Підтвердити пароль. Для зняття захисту з файлу подається команда **Зняти захист** із підменю **Сервіс**.

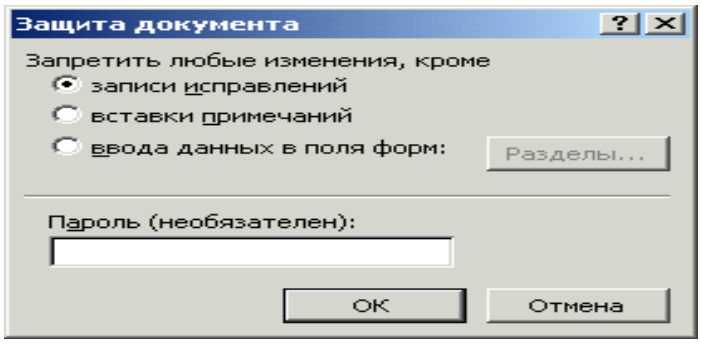


Рис. 3.6. Вікно відбору типу захисту.

У відповідне діалогове вікно вводиться пароль та натиснути кнопку **ОК**.

Захист документа за допомогою цифрового підпису.

В цьому випадку необхідно виконати наступні дії:

У меню **Сервіс** виберіть команду **Параметри**, а потім відкрийте вкладку **Безопасность** (рис. 3.7)

- Натисніть кнопку **Цифровые подписи**;
- Натисніть кнопку **Додати**;
- Виберіть сертифікат, який слід додати, і натисніть кнопку **ОК**.

Примітка:

За відсутності цифрового сертифіката його необхідно одержати. Цифровий сертифікат можна одержати в комерційному центрі сертифікації, такому як, наприклад, VeriSign, Inc., в адміністратора внутрішньої безпеки або у фахівця з інформаційних технологій. Цифровий підпис можна також створити самостійно за допомогою програм, наприклад, Selfcert.exe. Докладніші відомості про сертифікації продуктів фірми Microsoft див. на веб-вузлі Microsoft Security Advisor.

Якщо самостійно створений сертифікат не був виданий офіційним центром сертифікації, підписи з використанням такого сертифіката, називають макросами з автопідписом.

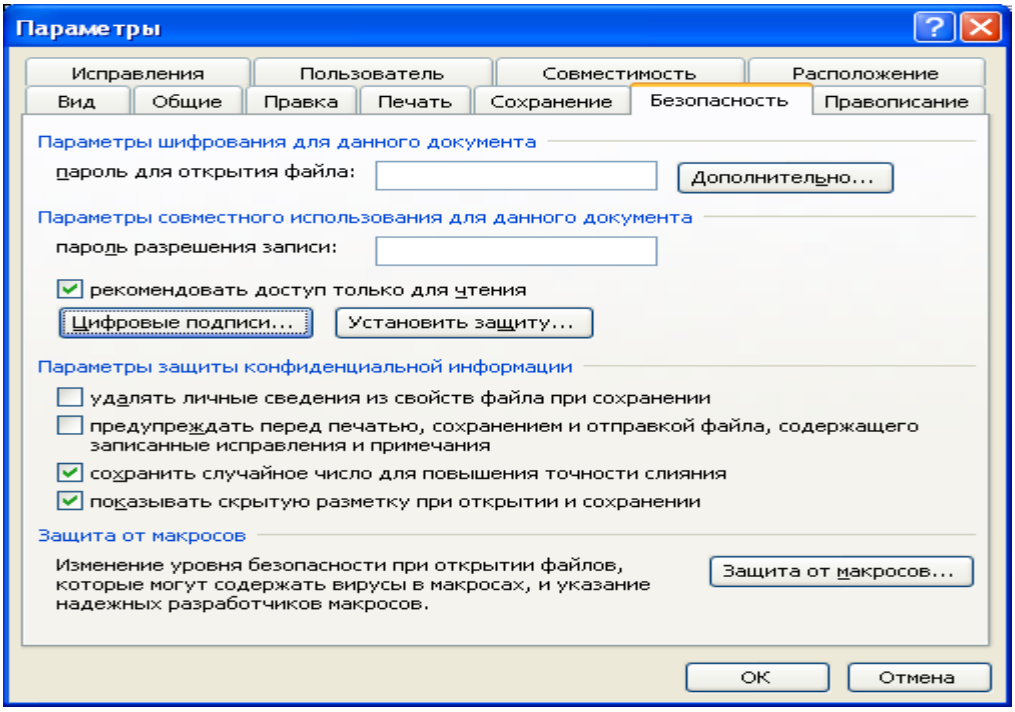


Рис. 3.7. Вікно Безпеки.

Установлення паролю на дозвіл відкриття документа.

- Відкрийте файл;
- У меню **Сервіс** виберіть команду **Параметри**, а потім відкрийте вкладку **Безпека;**
- У полі **Пароль** для відкриття файлу введіть пароль (рис.3.7), а потім натисніть кнопку **OK;**
- Уведіть пароль ще раз повторно, а потім натисніть кнопку **OK**.

Примітка.

Використовуйте надійні паролі, що представляють комбінацію прописних і рядкових букв, цифр і символів. Паролі, що не містять набір таких елементів, є ненадійними. Приклад надійного паролю: Y6dh!et5. Ненадійний пароль: House27. Використовуйте надійний пароль, який можливо запам'ятати, щоб не записувати його.

Щоб задати пароль, що містить до 255 знаків, натисніть кнопку **Додатково**, а потім виберіть тип шифрування RC4.

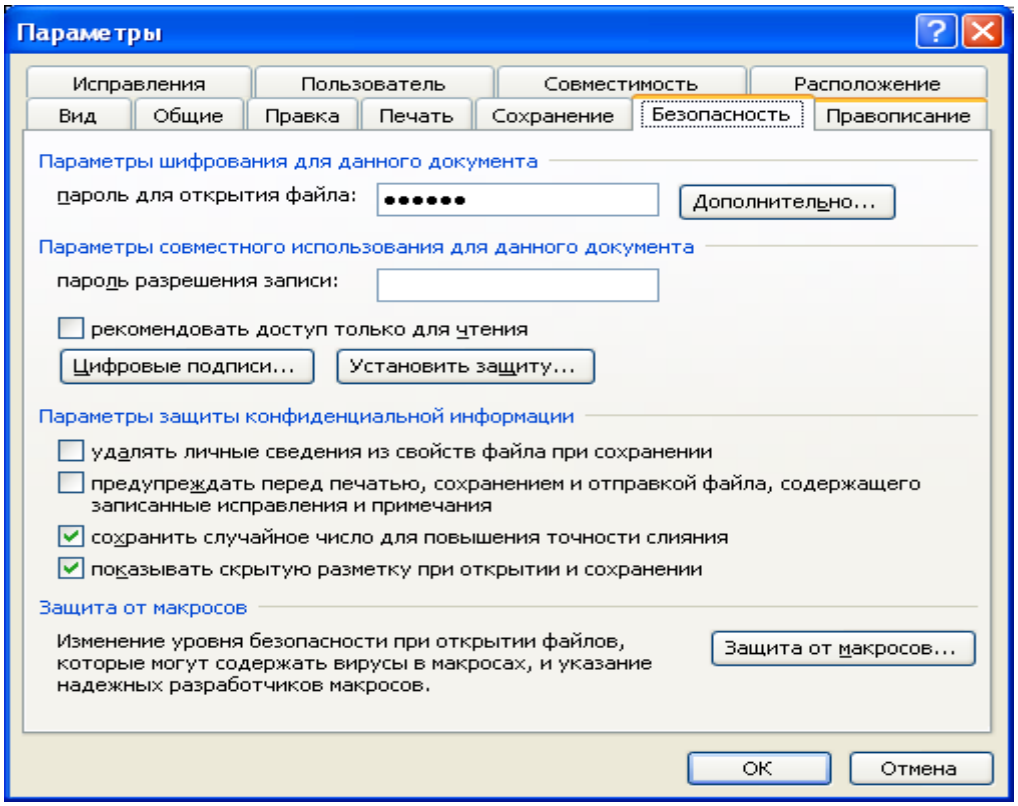


Рис. 3.8. Вікно введення паролю

Захист інформації у Microsoft Excel.

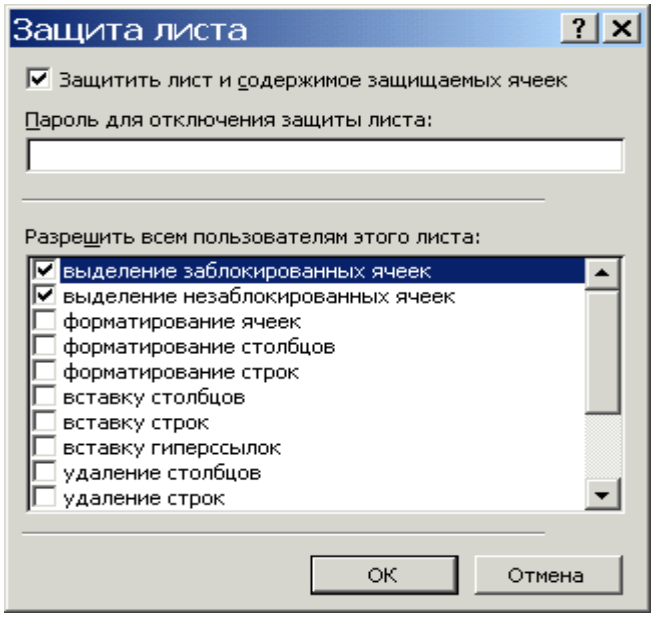
Захист документа за допомогою цифрового підпису та на відкриття документа здійснюється аналогічно, як у Microsoft Word

Як захистити комірки від ненавмисних змін? Навіщо це потрібно?

Одна з найбільших переваг комп'ютера - гнучка робота з інформацією. Захотів - записав, захотів - стер, додав, зменшив, змінив. Однак у цьому ж і небезпека: результати багатоденної роботи можна запросто втратити за кілька секунд, натиснувши не ту клавішу. Але куди простіше подбати про те, щоб деякі комірки просто не можна було змінити.

Наприклад, у стовпці F у нас формули обчислення суми, їх змінювати не треба. Рамочки, заголовок теж не повинні мінятися. Якби ми могли як-небудь позначити їх, щоб Excel не дозволяв їх змінювати.

Як це зробити? Давайте для початку захистимо весь лист.



Виконайте **Сервіс Захист Захистити лист** . З'явиться діалогове вікно (рис. 3.9):

Паролі можна вводити або не вводити. Є можливість підбору параметрів захисту встановленням, або видаленням прапорців біля відповідних параметрів. Після підбору параметрів захисту введіть команду **ОК**. Але тепер із таблицею взагалі нічого не можна зробити. Треба розблокувати хоча б деякі

Рис. 3.9 Вікно вибору параметрів захисту листа

комірки. Для зняття захисту з листа виконайте **Сервіс Захист Зняти захист листа**. Тепер потрібно визначити комірки, які не можна змінювати. Для цього необхідно виділити потрібні комірки та ввести команду **Формат комірок Захист**. З'явиться діалогове вікно (рис.3.10):

Треба встановити прапорець зліва від віконця “**Защищаемая ячейка**”.

Тепер комірка буде заблокована, якщо захистити лист, то цю комірку не можна буде змінювати.

Щоб розблокувати комірки, які можна змінювати, потрібно:

1. Зняти захист листа, якщо він є.

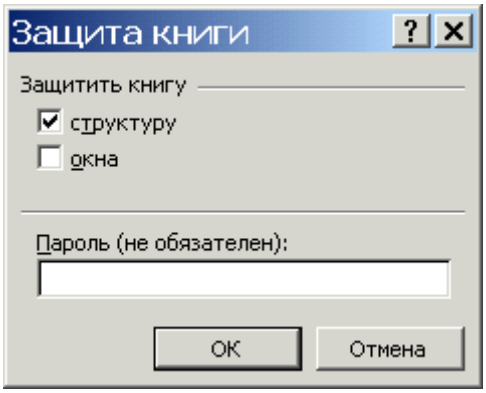
2. Виділити інтервал комірок, який потрібно розблокувати й виконати **Формат ячеек Захист** і забрати прапорець у вікні "**Захищені комірки**".

Аналогічно встановлюється захист на книгу (рис. 3.11).

Захист інформації в Microsoft Word 2007.

Захист документа від небажаних змін і приміток

Установка захисту документа дозволяє ввести обмеження на різні види змін, внесені в нього рецензентами.



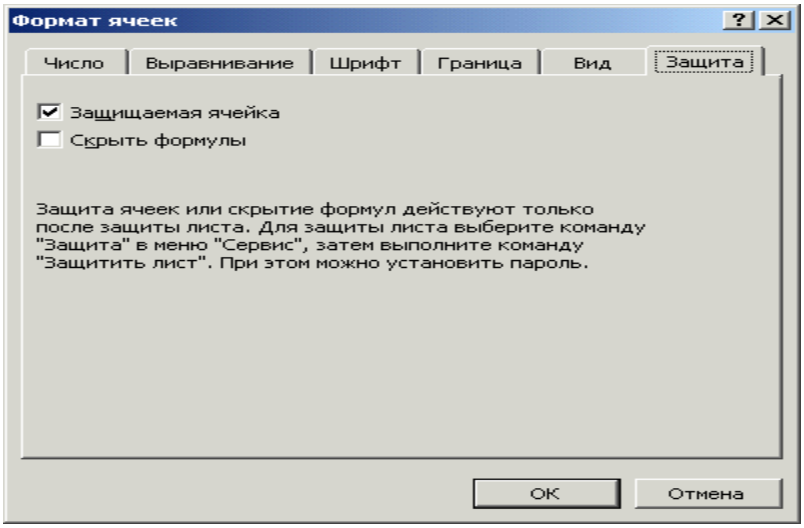


Рис. 3.11. Вікно захисту книги. Рис. 3.10. Вікно формату комірок.

Дозвіл на внесення приміток і записаних виправлень

1. На вкладці Рецензування в групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити форматування й редагування (рис. 3.12).

2. Для вказівки стилів, які рецензент зможе застосовувати або змінювати, в області завдань Захист документа в групі Обмеження на форматування встановіть прапорець Обмежити набір дозволених стилів (рис. 3.13), а потім клацніть Настроювання.

3. У групі Обмеження на редагування встановіть прапорець Дозволити тільки зазначений спосіб редагування документа.

4. У списку обмежень на редагування виберіть пункт Запис виправлень. (Сюди входять примітки, а також вставлений, вилучений і переміщений текст.)

ПРИМІТКА. Для додаткових можливостей захисту використовуйте службу Active Directory, клацніть Обмежити дозвіл, щоб скористатися керуванням правами на доступ до даних. У групі Включити захист натисніть кнопку Так, включити захист.

Для установки пароля на документ і надання паролю користувачам можливості зняти захист уведіть пароль у поле Новий пароль (необов'язково), а потім підтвердіть його.

ВАЖЛИВО. Якщо пароль не заданий, дані обмеження можуть бути змінені будь-яким рецензентом.

Дозвіл тільки на додавання приміток

1. На вкладці Рецензування в групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити редагування.

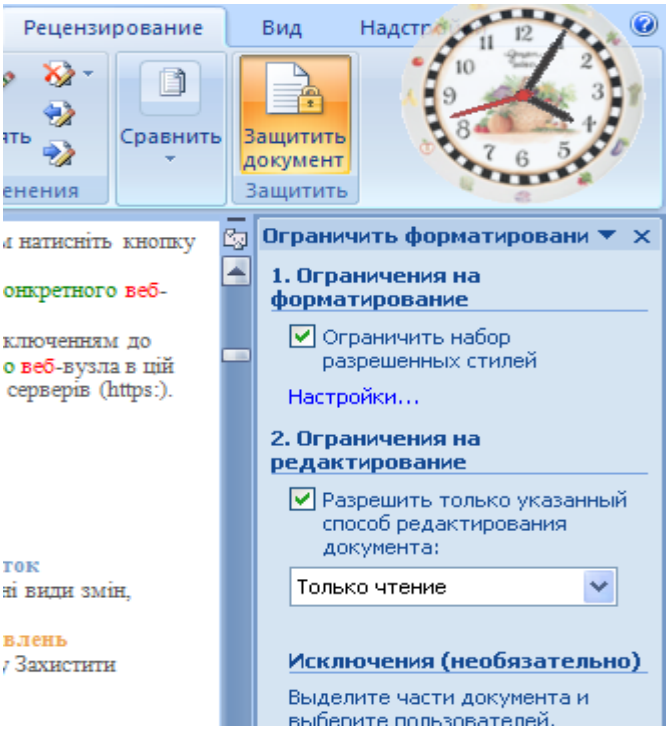


Рис. 3.12 Вікно налагодження обмежень

2. В області завдань Захист документа в групі Обмеження на редагування встановіть прапорець Дозволити тільки зазначений спосіб редагування документа.

3. У списку обмежень на редагування виберіть пункт Примітки.

Якщо деяким користувачам необхідно надати дозвіл на редагування окремих областей документа, виділіть ці області, а потім укажіть, які користувачі або групи користувачів можуть їх змінювати. Клацніть по списку, що розкривається, поруч з ім'ям користувача або групи користувачів для перегляду області, або всіх областей, доступних даному користувачеві, або групі користувачів для внесення

4. змін, або зняття дозволу для певного користувача, або групи.

ПРИМІТКА. Для додаткових можливостей захисту використовуйте службу Active Directory, клацніть Обмежити дозвіл, щоб скористатися правами на доступ до даних.

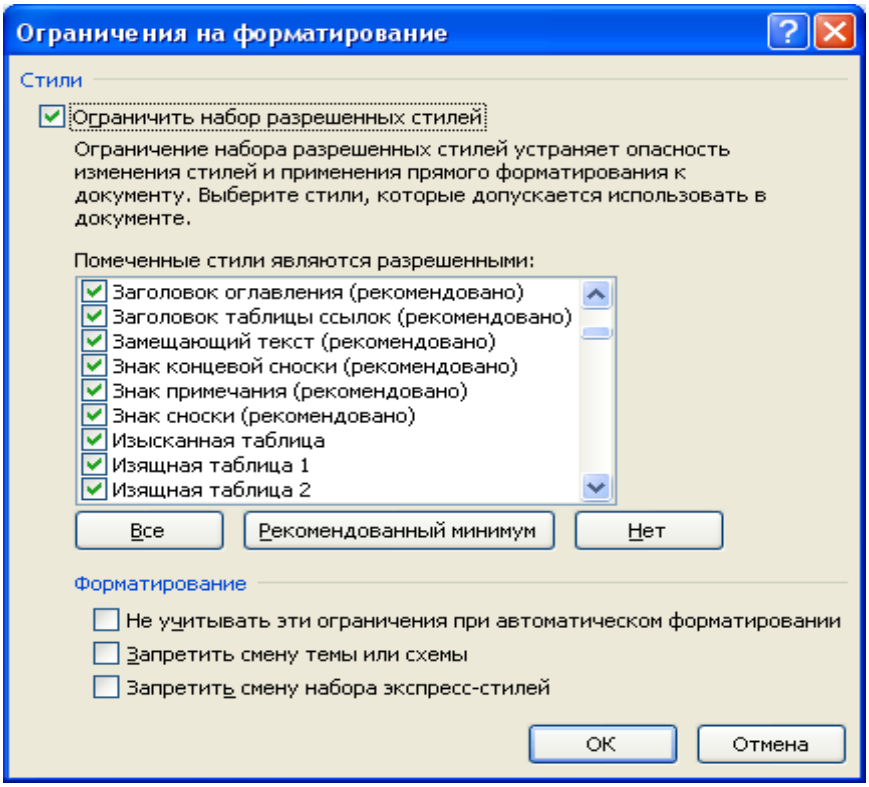


Рис. 3.13 Вікно відбору дозволених стилів

1. У групі Включити захист натисніть кнопку Так, включити захист.

2. Для установки пароля на документ і надання паролю користувачам можливості зняти захист уведіть пароль у поле Новий пароль (необов'язково), а потім підтвердіть його (рис. 3.14)

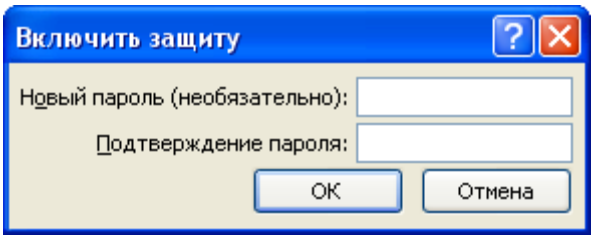


Рис. 3.14 Вікно введення паролю

ВАЖЛИВО. Якщо пароль не заданий, установлені обмеження можуть бути змінені будь-яким рецензентом.

Зняття захисту від додавання приміток і виправлень

1. На вкладці Рецензування в групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити форматування й редагування.

2. В області завдань Захист документа натисніть кнопку Відключити захист.

ПРИМІТКА. Якщо для захисту документа використовується пароль, його необхідно ввести для зняття захисту.

Установка пароля для відкриття й зміну документа

У Випуск 2007 системи Microsoft Office для доступу до документів Microsoft Office Word 2007, книгам Microsoft Office Excel 2007 і презентаціям Microsoft Office PowerPoint 2007, і для захисту їх від змін іншими користувачами можна використовувати пароль.

Видалення пароля для документа

Щоб забезпечити можливість перегляду або зміни вмісту тільки авторизованими рецензентами, можна захистити весь документ паролем.

1. Натисніть кнопку Кнопка «Office»  , а потім виберіть команду Зберегти як.

2. Клацніть пункт Сервіс (рис. 3.15), а потім виберіть Загальні параметри (рис. 3.16).

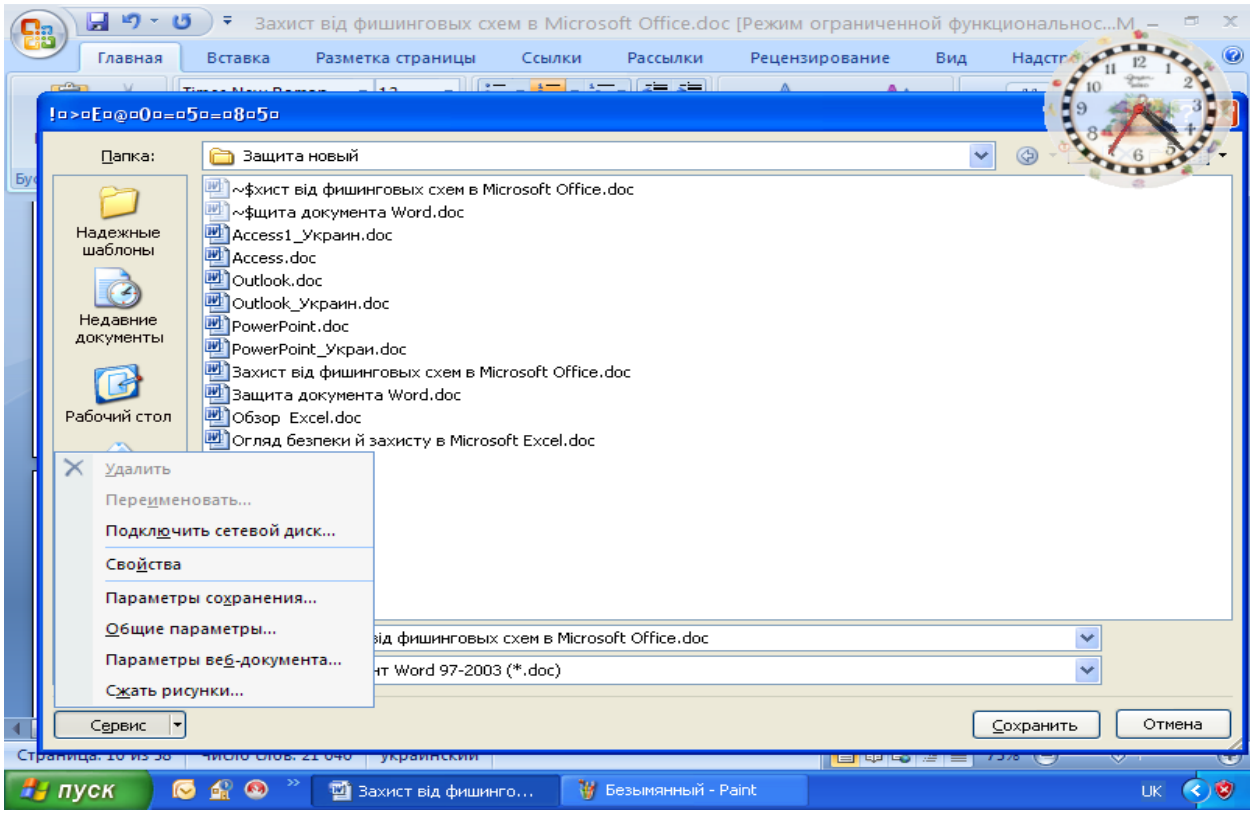


Рис. 3.15 Вікно збереження документа

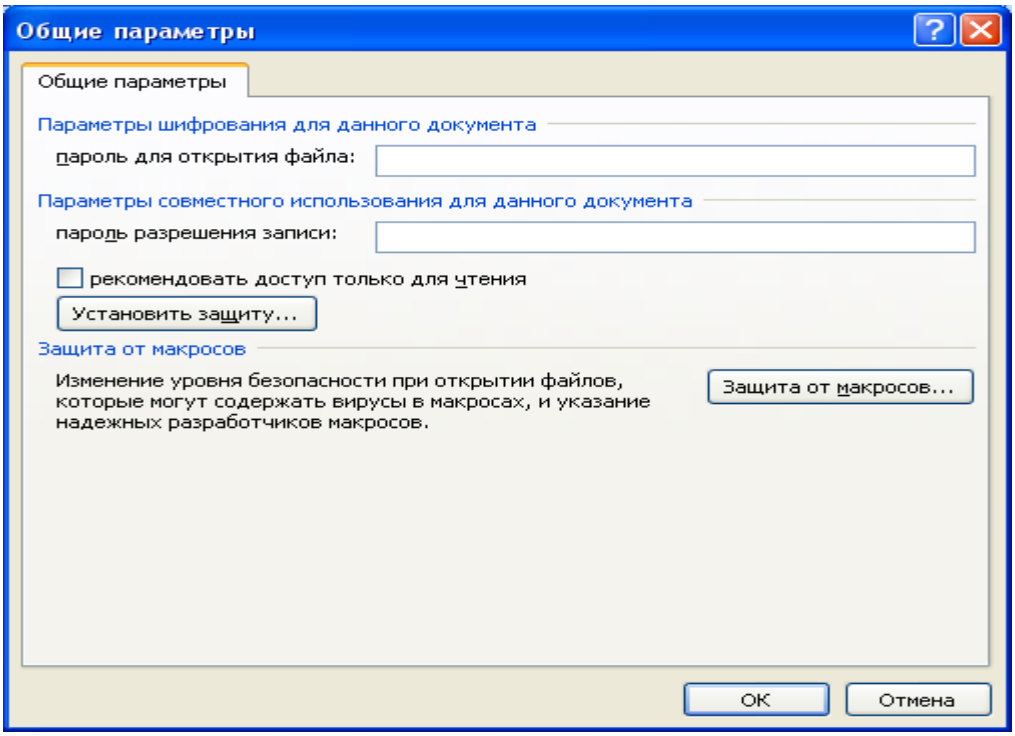


Рис. 3.16 Вікно введення паролів

3. Виконайте наступні дії:

- Якщо потрібно, щоб рецензенти вводили пароль перед переглядом документа, уведіть пароль у поле Пароль для відкриття.
- Якщо потрібно, щоб рецензенти вводили пароль перед збереженням внесених у документ змін, уведіть пароль у поле Пароль для зміни.

ПРИМІТКИ.

- Пароль для відкриття. За замовчуванням у цій функції застосовується шифрування. Шифрування - це стандартний метод, використовуваний для захисту файлів.
- Пароль для зміни В цій функції не використовуються методи шифрування. Вона розроблена для того, щоб користувач міг співробітничати з рецензентами, яким він довіряє. Вона не призначена для захисту файлів.
- Обидва паролі. Можна призначити обидва паролі — один для доступу до файлу, а іншої — для дозволу певним рецензентам змінювати його вміст. Переконайтеся, що ці паролі різні.

ВАЖЛИВО.

Використовуйте надійні паролі, що представляють собою сполучення прописних і малих літер, цифр і символів. Паролі, що не містять набір таких елементів, є ненадійними. Надійний пароль: Y6dh!et5. Ненадійний пароль: House27. Паролі повинні складатися не менш чим з 8 символів. Рекомендується використовувати фразу-пароль, що складається з 14 або більше символів.

1. Щоб запобігти випадковій зміні файлу рецензентами, установіть прапорець рекомендувати тільки для читання. При відкритті файлу рецензентам буде запропоновано відкрити його в режимі «тільки для читання».
2. Натисніть кнопку ОК.
3. При запиті підтвердити пароль уведіть його ще раз, а потім натисніть кнопку ОК.
4. Натисніть кнопку Зберегти.
5. Якщо піде запрошення, натисніть кнопку Так, щоб замінити існуючий документ.

Установка пароля для файлу

Щоб дозволити перегляд або зміну даних тільки авторизованими рецензентами, можна захистити файл паролем.

Натисніть кнопку Microsoft Office  , а потім виберіть команду Зберегти як.

Клацніть пункт Сервіс, а потім виберіть Загальні параметри (рис. 3.17).

Виконайте наступні дії:

1. Якщо потрібно, щоб рецензенти вводили пароль перед переглядом книги, уведіть пароль у поле Пароль для відкриття.
2. Якщо потрібно, щоб рецензенти вводили пароль перед збереженням внесених у книгу змін, уведіть пароль у поле Пароль для зміни.

ПРИМІТКИ

- Пароль для відкриття. За замовчуванням у цій функції застосовується шифрування. Шифрування - це стандартний метод, використовуваний для захисту файлів.

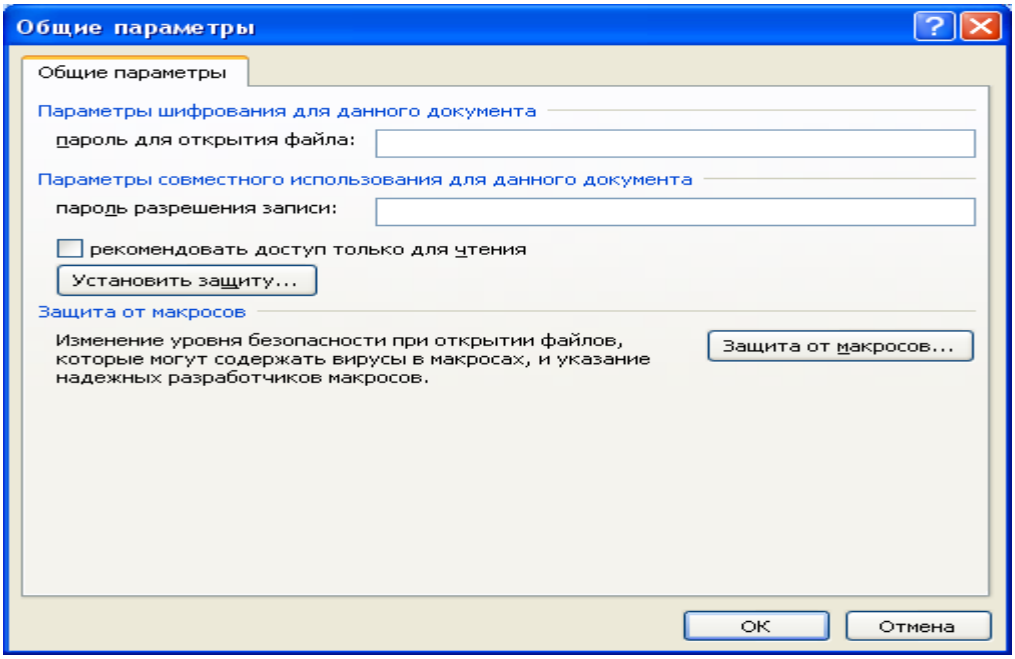


Рис. 3.17 Вікно введення паролів для книги.

- Пароль для зміни В цій функції не використовуються методи шифрування. Він розроблений для того, щоб користувач міг співробітничати з рецензентами, яким він довіряє. Він не призначений для захисту файлів.
- Обидва паролі. Можна призначити обидва паролі — один для доступу до файлу, а інший — для дозволу певним рецензентам змінювати його вміст. Переконайтеся, що ці паролі різні.

3. Щоб запобігти випадковій зміні файлу рецензентами, установіть прапорець Рекомендувати тільки для читання. При відкритті файлу рецензентам буде запропоновано відкрити його в режимі «тільки для читання».
4. Натисніть кнопку ОК.
5. При запиті підтвердити пароль уведіть його ще раз, а потім натисніть кнопку ОК.
6. Натисніть кнопку Зберегти.
7. Якщо піде запрошення, натисніть кнопку Так, щоб замінити існуючий файл.

Зміна пароля

Виконайте наступні дії:

1. Відкрийте файл із використанням пароля на відкриття в режимі читання й запису.

2. Натисніть кнопку «Office»  , а потім виберіть команду Зберегти як.

3. Клацніть пункт Сервіс, а потім виберіть Загальні параметри.

4. Виберіть існуючий пароль, а потім уведіть новий пароль.

5. Натисніть кнопку ОК.

6. При запиті підтвердити пароль уведіть його ще раз, а потім натисніть кнопку ОК.

7. Натисніть кнопку Зберегти.

8. Якщо піде запрошення, натисніть кнопку Так, щоб замінити існуючий файл.

Видалення пароля

Виконайте наступні дії:

1. Відкрийте файл із використанням пароля на відкриття в режимі читання й запису.

2. Натисніть кнопку Кнопка «Office»  , а потім виберіть команду Зберегти як.

3. Клацніть пункт Сервіс, а потім виберіть Загальні параметри.

4. Виберіть пароль, а потім натисніть клавішу DEL.

5. Натисніть кнопку ОК.

6. Натисніть кнопку Зберегти.

7. Якщо піде запрошення, натисніть кнопку Так, щоб замінити існуючий файл.

Додавання захисту в оперативну форму

Щоб запобігти видаленню або зміні окремих елементів керування вмістом, або групи елементів керування в оперативній формі, можна встановити для них індивідуальний захист. Також можна захистити весь уміст форми паролем.

Додавання захисту частинам форми

1. Відкрийте форму, яку необхідно захистити.

2. Виділіть елемент керування вмістом або групу елементів керування, зміни якої необхідно обмежити.

3. На вкладці Розробник у групі Елементи керування виберіть пункт Властивості рис. 3.18.

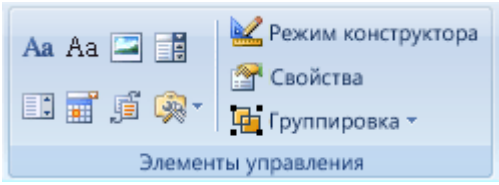


Рис. 3.18 Вікно відбору властивостей

4. У діалоговому вікні Властивості елемента керування вмістом у групі Блокування виконайте наступні дії.

- Установіть прапорець Елемент керування вмістом не можна видалити, що дозволяє редагування елемента керування вмістом, але забороняє видалення елемента керування вмістом із форми.
- Установіть прапорець Уміст не можна редагувати, що дозволяє видалення елемента керування, але забороняє редагування вмісту в елементі керування.

ПРИМІТКА. Цей варіант недоступний для всіх елементів керування.

Якщо вкладка Розроблювач недоступна, натисніть кнопку Microsoft Office  і клацніть Основні й потім установіть прапорець Показувати на стрічці вкладку розроблювача (рис. 3.19). Visio, Outlook або Publisher.

Додавання захисту всього вмісту форми

1. Відкрийте форму, яку необхідно захистити.

2. Нажавши кнопку Режим конструктора в групі Елементи керування, переконайтеся, що не використовується режим конструктора.

3. На вкладці Розробка в групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити форматування й редагування.

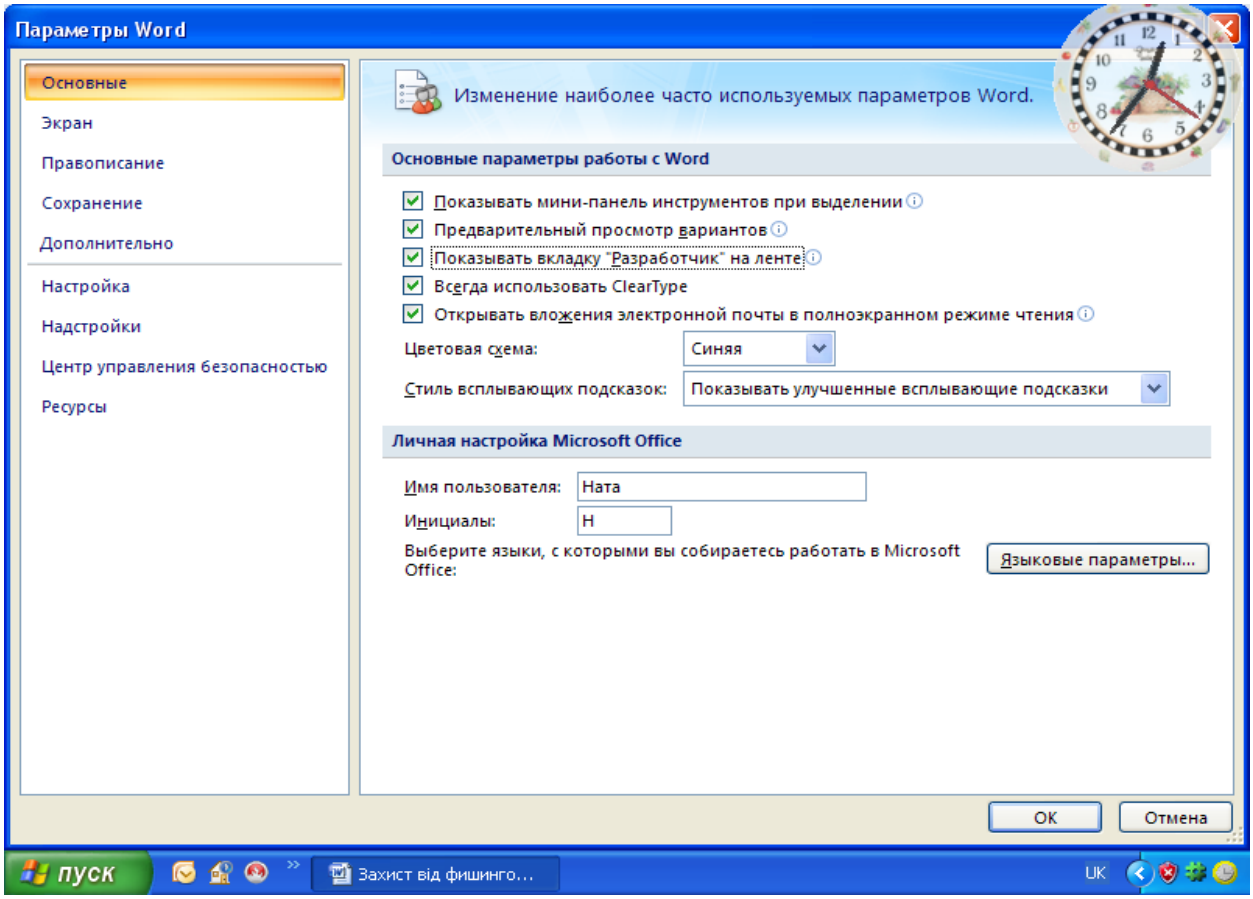


Рис. 3.19 Вікно встановлення вкладки Розроблювач

4. В області завдань Захист документа в групі Обмеження на редагування встановіть прапорець Дозволити тільки зазначений спосіб редагування документа.

5. У списку обмежень редагування виберіть пункт Уведення даних у поля форм.

6. У групі Включити захист натисніть кнопку Так, включити захист.

7. Для призначення пароля для документа, щоб тільки знаючі його користувачі могли видалити захист, уведіть пароль у вікні Новий пароль (необов'язково), а потім підтвердіть його.

Блокування форми

1. Переконайтеся в тім, що не використовується режим конструктора, шляхом натискання кнопки Режим конструктора в групі Елементи керування на вкладці Розроблювач.

2. На вкладці Розроблювач у групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити форматування й редагування.

3. В області завдань Захистити документ у групі Обмеження на редагування встановіть прапорець Дозволити тільки зазначений спосіб редагування документа.

4. У списку обмежень редагування виберіть пункт Уведення даних у поля форм.

5. У групі Включити захист натисніть кнопку Так, включити захист.

6. Для призначення пароля для документа, щоб тільки користувачі, що знають його, могли видалити захист, уведіть пароль у вікні Новий пароль (необов'язково), а потім підтвердіть пароль.

ВАЖЛИВО. Якщо пароль не використовується, змінити обмеження редагування може будь-який користувач.

Розблокування форми

1. На вкладці Розробник у групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити форматування й редагування.

2. В області завдань Захистити документ натисніть кнопку Відключити захист.

ПРИМІТКА. Якщо для захисту документа використовується пароль, його варто ввести до зняття захисту.

Дозвіл вибіркового виправлення захищеного документа

Після установки захисту документа шляхом вибору параметрів Тільки читання або Примітки в області завдань Захист документа можна вказати певні частини документа, на які обмеження поширюватися не буде. Можна також надати дозвіл окремим користувачам на зміну цих частин документа.

1. На вкладці Рецензування групі Захист виберіть команду Захистити документ, і потім клацніть Обмежити форматування й редагування.

2. В області завдань Захист документа виберіть команду Відключити захист.

3. Якщо документ уже був захищений паролем, у діалоговому вікні Зняти захист уведіть пароль.

4. Укажіть частини документа, на які обмеження поширюватися не буде.

5. Наприклад, виберіть групу абзаців, заголовок або слово.

6. Виконайте одну з наступних дій.

7. Щоб дозволити всім відкриваючий документ редагування обраних фрагментів, у списку Зняти захист установіть прапорець Групи.

8. Щоб дозволити тільки персональне редагування обраних фрагментів, виберіть пункт Інші користувачі, а потім уведіть імена користувачів. Розділяйте імена крапкою з коми. Натисніть кнопку ОК, а потім установіть прапорці напроти імен користувачів, яким дозволяється редагування обраних фрагментів.

ПРИМІТКА. При виборі декількох користувачів вони будуть додані в поле Група як елементи; наступного разу, таким чином, можна буде легко вибрати групу, не вводячи імена кожного користувача.

1. Продовжуйте вибирати частини документа, і призначати дозвіл користувачам їх редагувати.

2. У розділі Включити захист натисніть кнопку Так, включити захист.

3. Виконайте одну з наступних дій.

- Щоб призначити пароль документу, і щоб знаючі пароль користувачі могли зняти захист, уведіть пароль у поле Новий пароль (необов'язково), а потім підтвердіть його.
- Щоб зашифрувати документ, для того щоб тільки авторизовані власники могли зняти захист, клацніть Перевірка дійсності користувача.

Перегляд параметрів конфіденційності

Щоб переглянути параметри конфіденційності, у додатках (Word, Excel, PowerPoint і Access) 2007 Microsoft Office виконайте наступні дії.

1. Натисніть кнопку Microsoft Office  , і потім клацніть, наприклад, Параметри Word.

2. Відкрийте сторінку Центр керування безпекою, натисніть кнопку Параметри центра керування безпекою, і потім натисніть кнопку Параметри конфіденційності (рис. 3.20).

Приєднання сертифіката

Для офіційного підтвердження приналежності штампа або підпису можна приєднати штамп, або підпис до сертифіката. Рішення групового твердження підтримують сертифікати, які були випущені відповідно до стандартів сертифікації, включаючи відкриті й закриті сертифікати, випущені компаніями. Приєднання сертифіката означає шифрування з використанням сертифіката, а не його вкладення.

1. Підготуйте сертифікат до використання. Якщо необхідно скористатися одним із декількох відкритих сертифікатів, збережіть його з веб-вузла, на якому він був випущений. Закритий ключ також повинен бути збережений. Для одержання додаткової інформації зверніться в центр сертифікації.

2. На панелі завдань натисніть кнопку «Пуск», а потім виберіть команду Виконати.

3. Щоб запустити консоль керування MMC, у вікні Відкрити введіть mmc.exe (рис. 3.21).

4. Щоб відкрити діалогове вікно Додати, або видалити оснащення, у меню Консоль (рис. 3.22) консолі керування клацніть Додати, або видалити оснащення.

5. Щоб відкрити діалогове вікно Додати ізольоване оснащення, натисніть кнопку Додати.

6. У списку Додати ізольоване оснащення виберіть пункт Сертифікати, а потім натисніть кнопку Додати.

7. У діалоговому вікні Оснащення диспетчера сертифікатів виберіть пункт Мого облікового запису користувача й клацніть Готово.

8. У діалоговому вікні Додати ізольоване оснащення клацніть Закрити, а потім натисніть кнопку ОК у діалоговому вікні Додати або видалити оснащення.

9. Перейдіть на рівень кореневої папки дерева консолі й клацніть +, зображений поруч із пунктом «Сертифікати - поточний користувач», щоб розгорнути вузол.

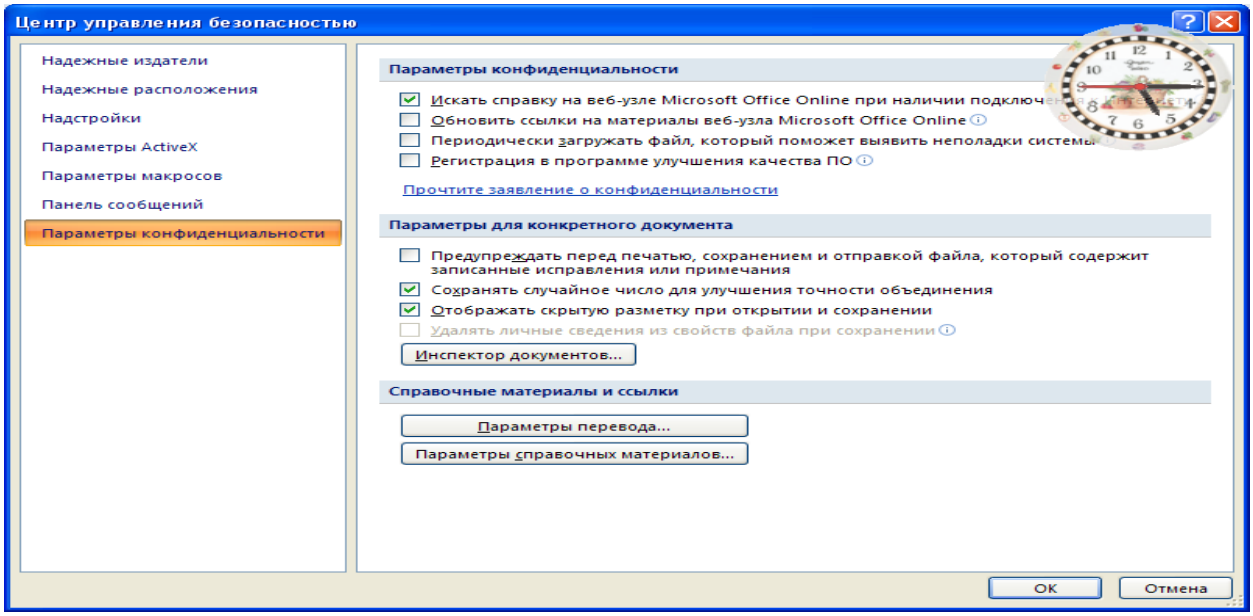


Рис. 3.20 Вікно параметрів конфіденційності

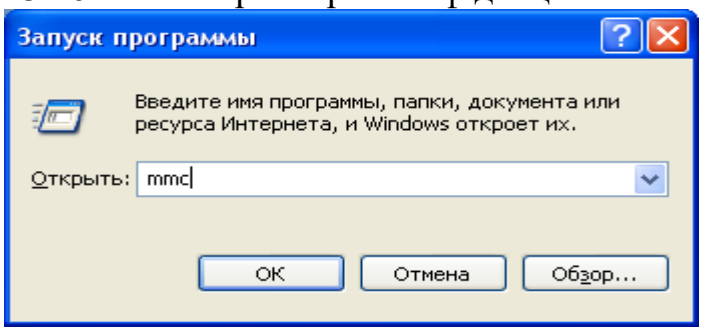


Рис. 3.21 Вікно запуску консолі

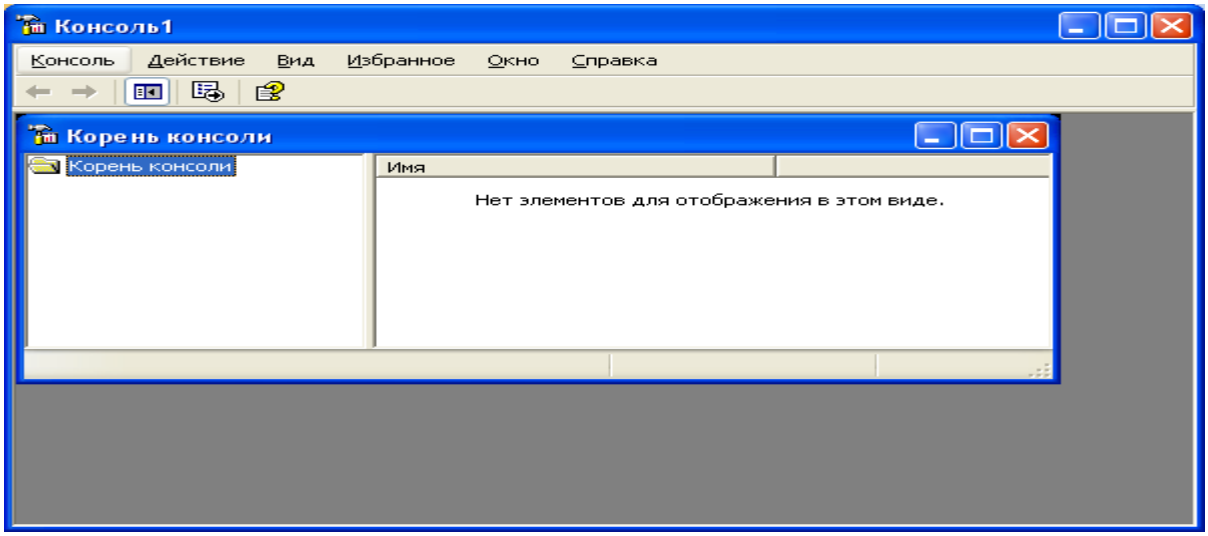


Рис. 3.22 Вікно консолі

10. У розгорнутому вузлі виділіть пункт Особисті.

11. У меню Дія виберіть пункт Усі завдання, потім - пункт Імпорт.

12. Щоб вибрати місце розташування сертифіката, підготовленого на першому кроці, на другому екрані майстра натисніть кнопку Огляд, а потім натисніть кнопку Далі.

13. Уведіть пароль у вікні Пароль, і зніміть обидва прапорці Включити посилений захист закритого ключа, і Позначити цей ключ як експортований. Щоб перейти на наступну сторінку, натисніть кнопку Далі.

14. Установіть прапорець Помістити всі сертифікати в наступне сховище, і виберіть Сховище сертифікатів як Особисті. Щоб перейти на наступну сторінку, натисніть кнопку Далі.

15. Щоб вийти з майстра імпорту сертифікатів натисніть кнопку Готово.

16. Підтвердіть повідомлення, що імпорт був завершений.

17. З вузла в групі Сертифікати - поточний користувач клацніть вузол Довірені кореневі центри сертифікації або вузол Проміжні центри сертифікації.

18. Щоб імпортувати сертифікат, повторіть кроки з 11 з 16.

19. Тепер, коли документ підписаний в Microsoft Office Word 2007 або Microsoft Office Excel 2007, відобразиться сертифікат, що був доданий у діалоговому вікні Вибір сертифіката.

Захист інформації у Microsoft Excel 2007

В MICROSOFT OFFICE EXCEL передбачено кілька рівнів захисту для керування доступом до даних EXCEL і їхньої зміни. щоб захистити дані книги, можна виконати наступні дії:

- Для підвищення безпеки варто захистити весь файл книги за допомогою пароля (Пароль. Спосіб обмеження доступу до книги, листу або частини листа. В Microsoft Excel довжина пароля не повинна перевищувати 255 букв, цифр, пробілів і інших символов. При введенні пароля враховується регистр букв.), який дозволить переглядати або змінювати дані тільки вповноваженим користувачам.

- Як додатковий захист певних даних можна захистити окремі елементи книги з паролем або без нього. Захист листа й елементів книги може запобігти випадковій або зловмисній зміні, переміщення, або видалення важливих даних.

Використання паролів для захисту книги

Коло користувачів, що мають можливість відкривати книгу, і використовувати дані, що втримуються в ній, можна обмежити, установивши пароль на перегляд книги або збереження внесених у неї змін.

Захист за допомогою пароля на рівні книги використовує поліпшені методи шифрування, щоб захистити книгу від неавторизованого доступу. Пароль можна задати при збереженні книги. Можна визначити два різних паролі, які будуть використовуватися в наступних випадках:

- Відкриття й перегляд книги. Цей пароль шифрується, щоб захистити дані від неавторизованого доступу.
- Зміна книги. Цей пароль не шифрується й призначений тільки для того, щоб дати певним користувачам можливість змінювати дані в книзі, і зберігати зміни у файлі.

Ці паролі використовуються для всієї книги. Для підвищення безпеки варто завжди встановлювати паролі на відкриття й перегляд файлу. Щоб надати право змінювати дані тільки деяким користувачам, може знадобитися призначити обидва паролі.

ВАЖЛИВО. Варто завжди використовувати надійні паролі, утворені сполученням прописних і малих літер, цифр і символів. Паролі, що не сполучать у собі цих елементів, не є надійними. Надійний пароль: Y6dh!et5. Ненадійний пароль: House27. Використовуйте надійний пароль, якому можна запам'ятати, щоб не довелося його записувати.

При необхідності нагадати користувачам про те, що дані в книзі дуже важливі й не повинні змінюватися, можна використовувати в додатку Excel рекомендацію

відкривати книгу тільки для читання. Цей параметр можна визначити при збереженні книги з використанням пароля на відкриття файлу або без нього. Відкриваючи книгу, користувачі будуть одержувати рекомендацію відкрити її в режимі тільки для читання, однак це не запобіжить внесенню змін у книгу.

Захист окремих елементів книги й листа

При роботі із книгою разом з іншими користувачами, включаючи спільне використання даних, може виникнути необхідність захистити дані в окремих елементах листа або книги від можливих змін. Можна задати пароль, що користувачі повинні будуть уводити для окремих захищених елементів книги й листа.

ВАЖЛИВО. Захист елементів книги або таблиці не слід плутати із захистом паролем на рівні книги. Захист елементів не захищає книгу від зловмисників.

Захист елементів листа

При захисті листа всі комірки цього листа блокуються за замовчуванням, і користувачі не можуть вносити зміни в ці комірки. Наприклад, вони не можуть вставити, змінити, видалити або відформатувати дані в блокованих комірках. Однак при захисті листа можна вказати, які елементи користувачам буде дозволено змінювати.

Розблокування обраних областей захищеного листа

Перед тим як захистити лист, можна розблокувати діапазони комірок, у яких *користувачам буде дозволено змінювати або вводити дані. Можна розблокувати комірки для всіх або для окремих користувачів.*

Використання пароля для керування доступом до захищених елементів

При захисті книги або листа для блокування їхніх елементів використовувати пароль не обов'язково. У цьому контексті пароль використовується тільки для того, щоб дозволити окремим користувачам доступ до елементів, допомагаючи заборонити доступ усім іншим користувачам. Цей рівень захисту за допомогою пароля не гарантує, що всі важливі дані книги будуть захищені. Для підвищення безпеки варто захищати за допомогою пароля всю книгу, що дозволить охоронити неї від несанкціонованого доступу.

При захисті за допомогою пароля елементів книги або листа дуже важливо запам'ятати цей пароль. У противному випадку зняти захист із книги або листа буде неможливо.

Захист структури й вікон книги

Можна заблокувати структуру книги, що запобіжить додаванню й видаленню аркушів, або відображенню схованих аркушів. Крім того, можна заборонити зміну розмірів або положення вікон. Дія такого захисту поширюється на всю книгу.

Захист конфіденційності даної книги

Приховання, блокування й захист елементів книги й листа не призначені для захисту даних або важливих відомостей, що зберігаються в книзі. Вони можуть допомогти ускладнити дані або формули, здатні спантеличити інших користувачів, і запобігають їхньому перегляду, і внесення в них змін.

Сховані або захищені паролем дані в книгах Excel не шифруються. Щоб забезпечити безпеку важливих відомостей, обмежте доступ до всіх файлів Excel, що містять подібні відомості, зберігши їх там, де вони будуть доступні тільки авторизованим користувачам.

Захист елементів листа

1. Виберіть лист, який потрібно захистити.
2. Щоб розблокувати всі комірки або діапазони, які повинні бути доступні іншим користувачам для зміни, виконайте наступні дії:
3. Виберіть послідовно всі комірки або діапазони, які потрібно розблокувати.
4. На вкладці Головна в групі Комірки клацніть Формат, а потім виберіть команду Формат комірок (рис. 3.23).

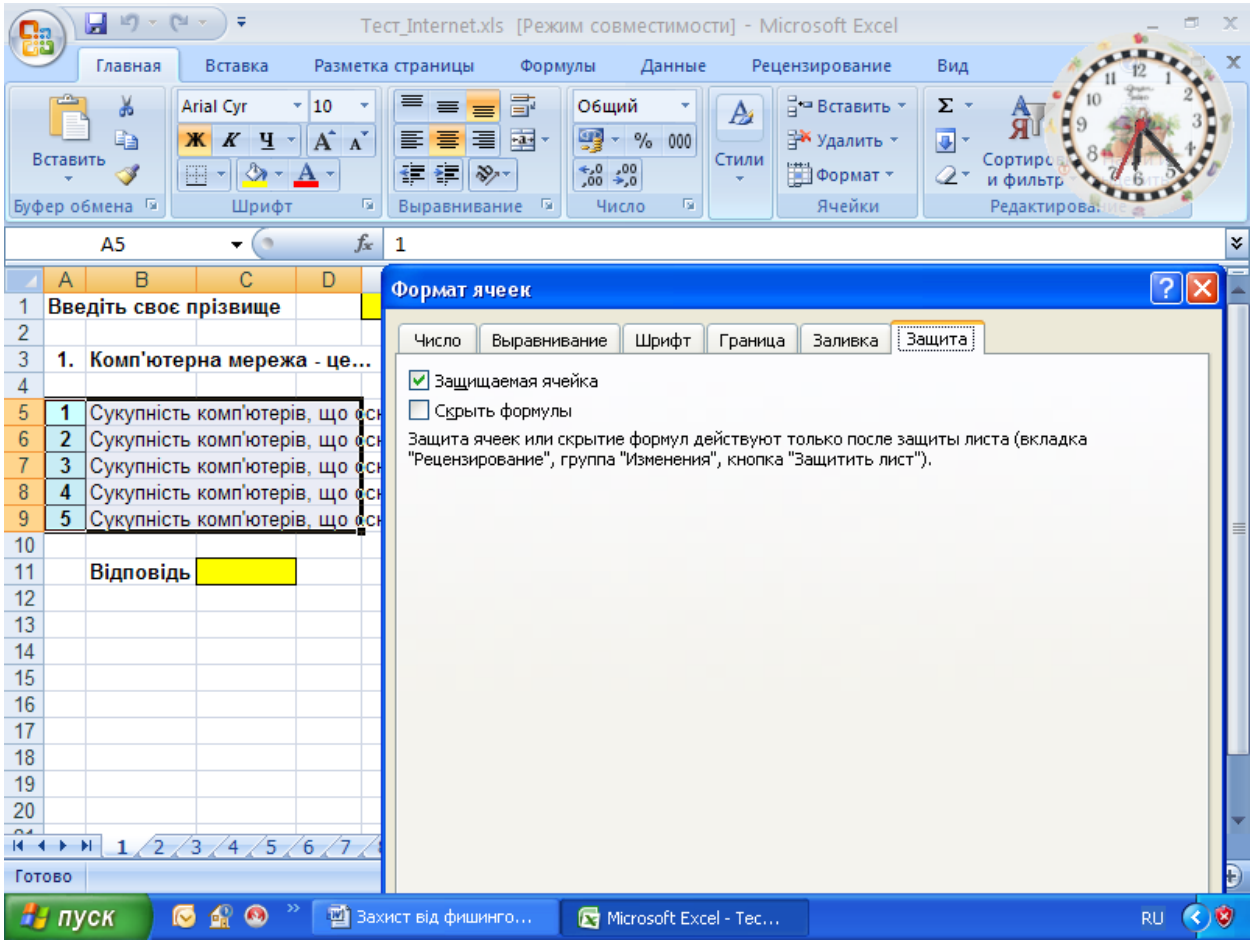


Рис. 3.23 Вікно захисту комірок

5. На вкладці Захист зніміть прапорець Не обновляти зв'язок і натисніть кнопку OK.
6. Щоб сховати всі формули, які не повинні відображатися, виконайте наступні дії:

- Виберіть на листі комірки, що містять формули, які необхідно сховати.
- На вкладці Головна в групі Комірки клацніть Формат, а потім виберіть команду Формат комірок.
- На вкладці Захист установіть прапорець Схований і потім натисніть кнопку OK.

7. Щоб розблокувати всі графічні проекти (наприклад, картинки, проекти Clip art, фігури або графіку Smart Art) які повинні бути доступні користувачам для зміни, виконайте наступні дії:.

- Утримуючи натиснутої клавішу CTRL, послідовно клацніть усі графічні проекти, які потрібно розблокувати (рис. 3.24).
- На стрічці з'явиться вкладка Робота з малюнками або Засоби малювання, що містить вкладку Формат.

Примітка. Можна також використовувати команду Перейти для швидкого вибору всіх графічних проектів на листі (рис. 3.25). На вкладці Головна в групі Редагування натисніть кнопку Знайти й виділити, а потім виберіть команду Перейти. Натисніть кнопку Виділити, а потім виберіть пункт Об'єкти.

1. На вкладці Формат у групі Розмір натисніть кнопку виклику діалогового вікна Розмір та Властивості поруч із кнопкою Розмір (рис. 3.26).

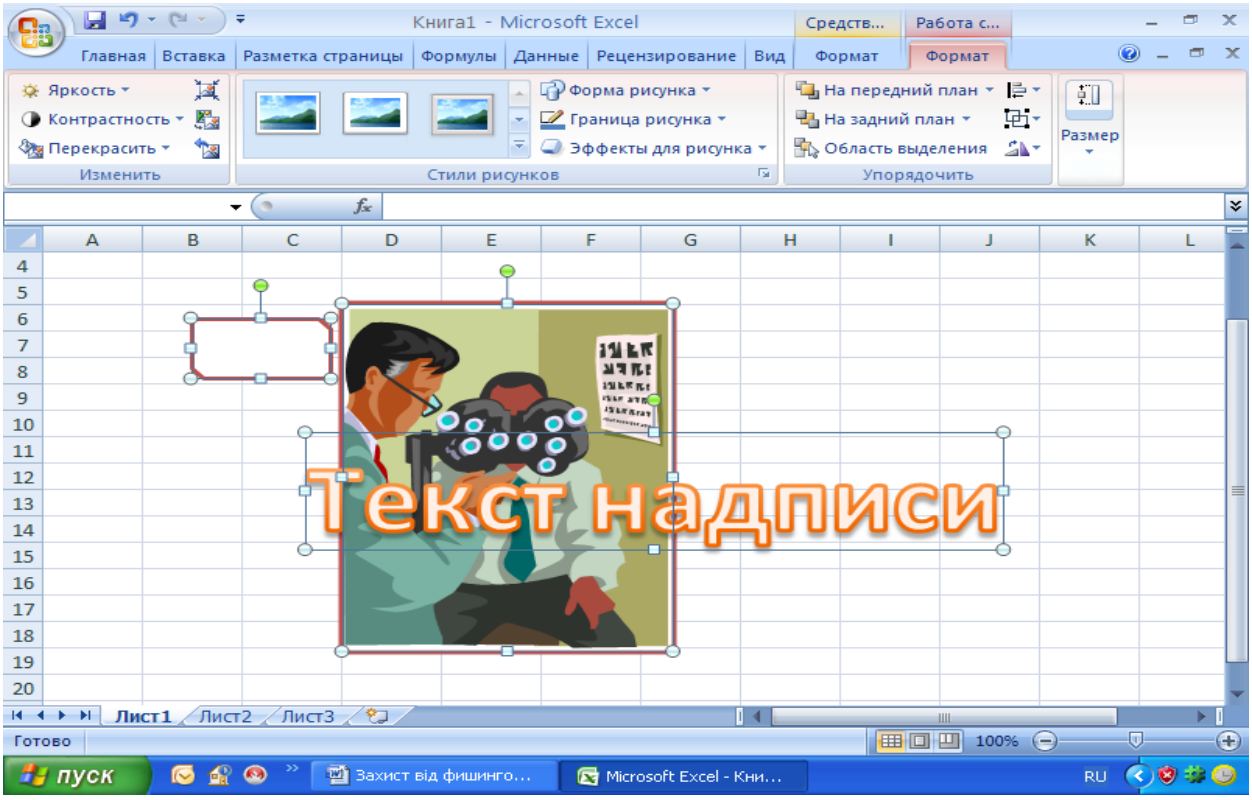
2. На вкладці Властивості зніміть прапорець Захист комірки, а також прапорець Заблокувати текст (якщо він є).

ПРИМІТКА. Немає необхідності розблокувати кнопки й елементи керування, щоб користувачі могли працювати з ними. Можна розблокувати впроваджені діаграми, поля уведення тексту й інші проекти, створені засобами малювання, які повинні бути доступні користувачам для зміни.

3. На вкладці Рецензування групі Зміни виберіть команду Захистити лист (рис. 3.25).

4. У списку Дозволити всім користувачам цього листа відзначте прапорцями елементи, зміна яких повинна бути доступною користувачам (рис. 3.26).

5. У діалоговому вікні Пароль для відключення захисту листа введіть пароль для захисту листа, натисніть кнопку ОК, а потім ще раз уведіть пароль для підтвердження.



Ри с. 3.24 Графічні проекти

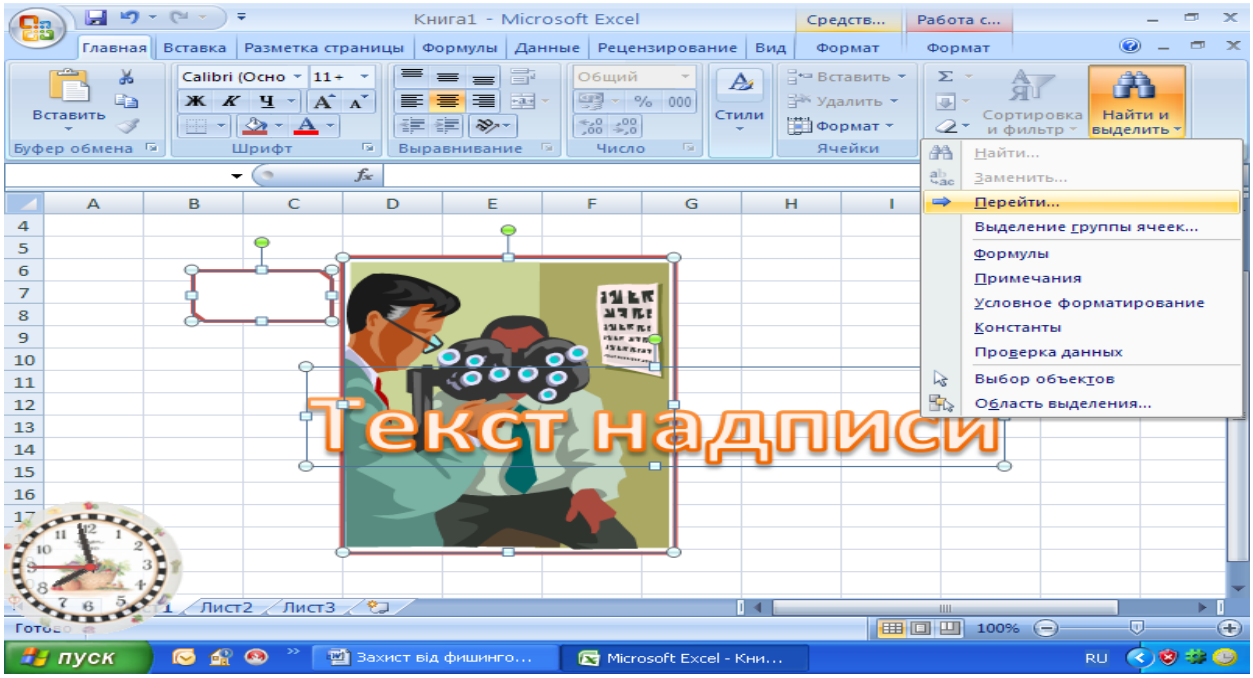


Рис. 3.25 Вікно переходу до виділення проектів

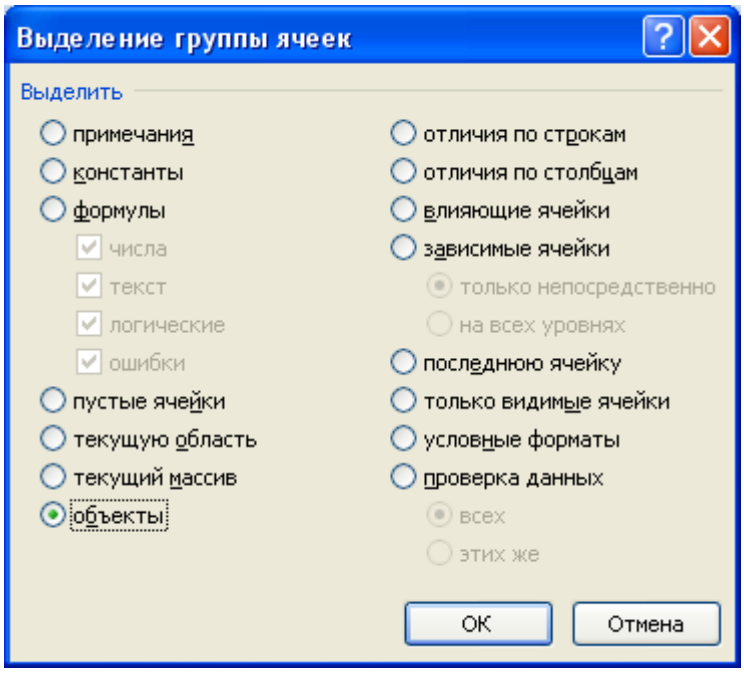


Рис. 3.26 Вікно відбору проектів

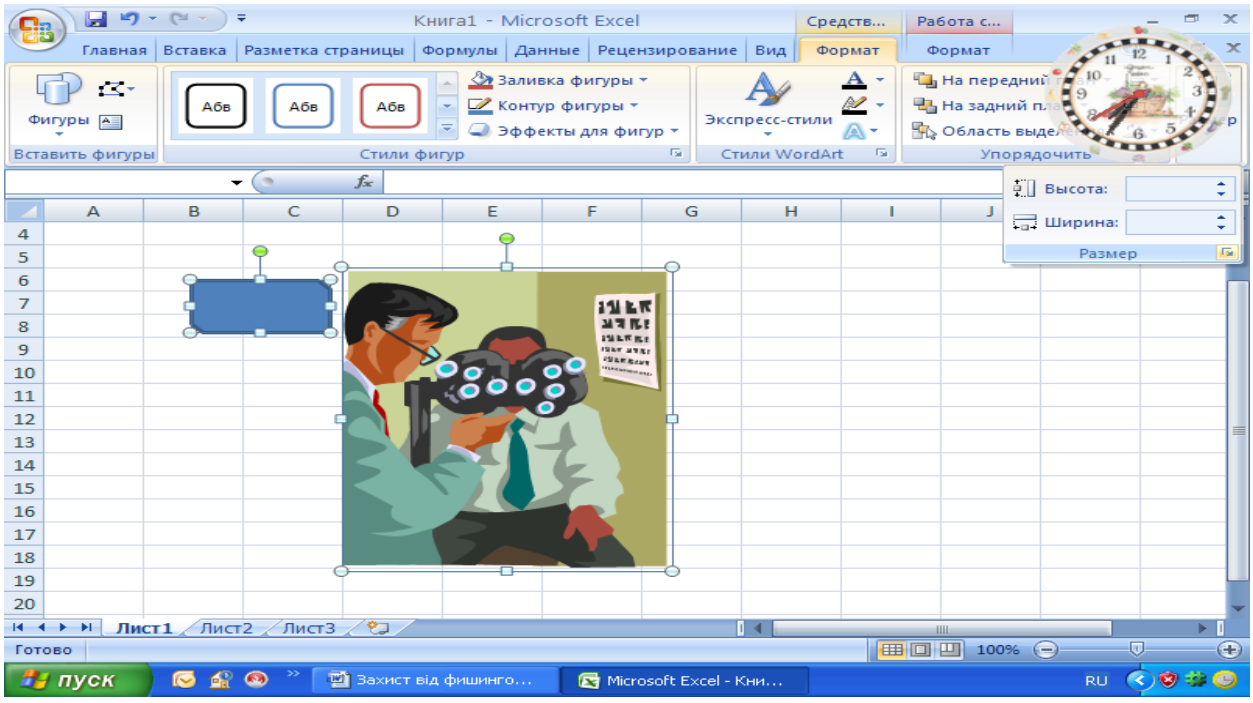


Рис. 3.27 Вікно відкриття діалогового вікна Розмір та Властивості

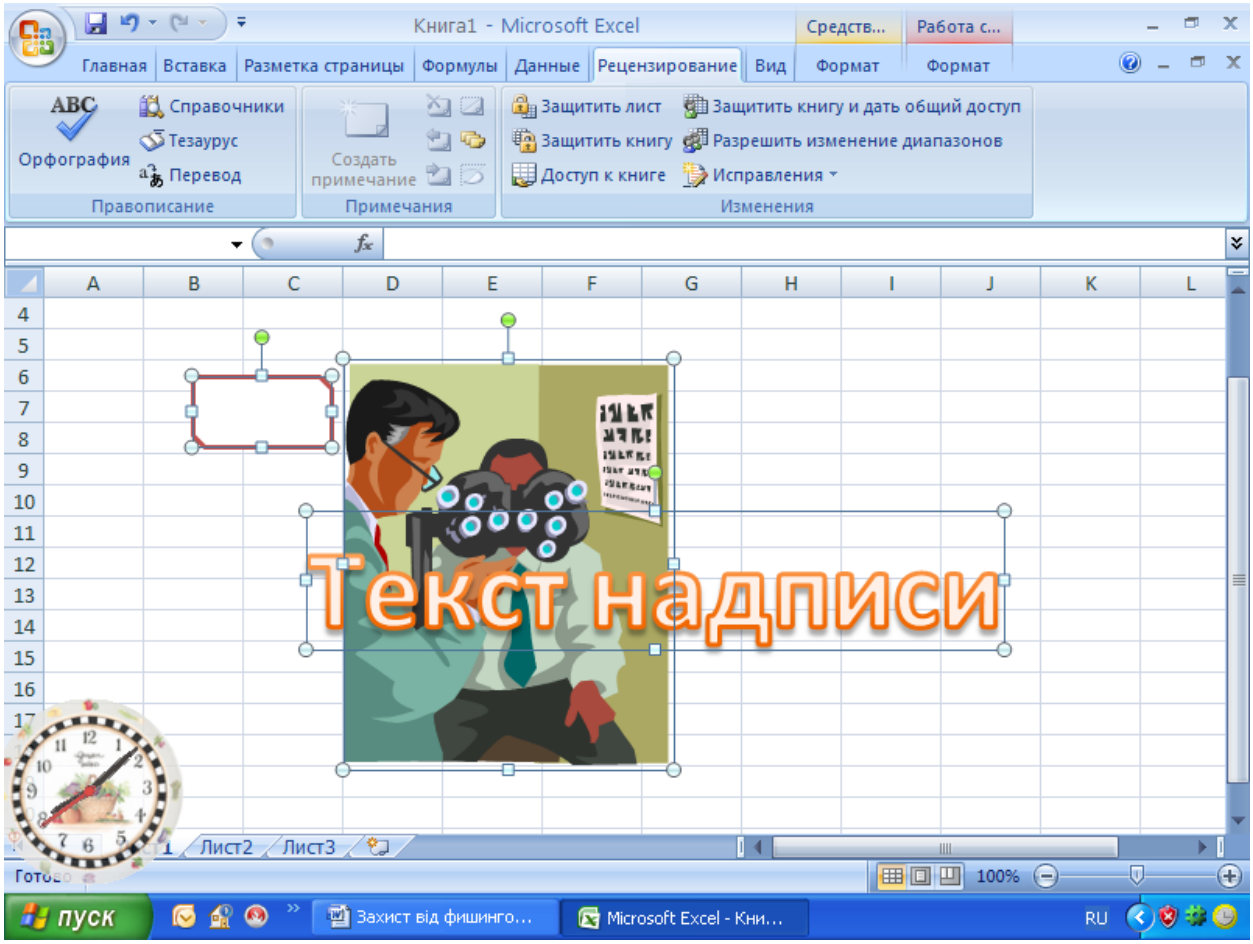


Рис. 3.28 Вікно відбору команди Захист листа

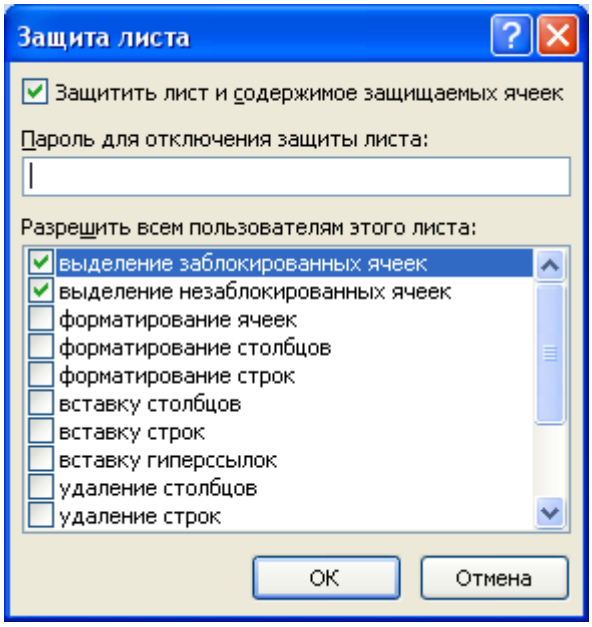


Рис. 3.29 Вікно дозволу визначених параметрів користувачам

Таблиця 3.1

Дозволені параметри користувача

Зніміть цей прапорець	Щоб не дати можливості користувачам
виділення заблокованих комірок	Переміщати покажчик миші на комірки, для яких установлений прапорець Захищена комірка, що, на вкладці Захист у діалоговому вікні Формат комірок. За замовчуванням користувачам дозволено виділяти захищені комірки.
виділення незаблокованих комірок	Переміщати покажчик миші на комірки, для яких знятий прапорець Захищена комірка, що, на вкладці Захист у діалоговому вікні Формат комірок. За замовчуванням користувачам дозволено виділяти незахищені комірки й можна переміщатися між незахищеними комірками на захищеному листі, натискаючи клавішу TAB.
форматування комірок	Змінювати параметри в діалогових вікнах Формат комірок або Умовне форматування. Якщо умовні формати були застосовані до установки захисту листа, форматування продовжує змінюватися, якщо користувач уводить значення, що задовольняє іншій умові.
форматування стовпців	Використовувати будь-які команди форматування стовпців, включаючи зміну ширини стовпця або приховання стовпців (вкладка Головна, група Комірки, кнопка Формат).
форматування рядків	Використовувати будь-які команди форматування рядків, включаючи зміну висоти рядка або приховання рядків (вкладка Головна, група Комірки,

	кнопка Формат).
вставку стовпців	Вставляти стовпці.
вставку рядків	Вставляти рядки.
вставку гіперпосилань	Вставляти нові гіперпосилання (Гіперпосилання. Кольоровий підкреслений текст або графічний об’єкт, із клацання по якому мишкою приводить до переходу до файлу, фрагменту файла, або веб-сторінки в Інтрамережі, або Інтернеті. Гіперпосилання можуть також вказувати на групи новин і вузли Gopher, Telnet і FTP.) на незахищені комірки.
видалення стовпців	Видаляти стовпці. ПРИМІТКА. Якщо команда видалення стовпців захищена, а команда вставка стовпців не захищена, користувач не зможе видаляти стовпці, які він вставить.
видалення рядків	Видаляти рядки. ПРИМІТКА. Якщо команда видалення рядків захищене, а команда вставки рядків не захищена, користувач не зможе видаляти рядки, які він вставить.
сортування	Використовувати команди для сортування даних (вкладка - Дані, група - Сортування й фільтр). ПРИМІТКА. Користувачі не зможуть сортувати діапазони, що містять заблоковані комірки на захищеному листі, незалежно від настроювання цього параметра.

використання автофільтра	Використовувати кнопки зі стрілками для зміни фільтра в діапазонах, якщо застосовуються автофільтри. ПРИМІТКА. Користувачі не зможе застосувати або видалити автофільтри на захищеному листі, незалежно від настроювання цього параметра.
використання звітів зведеної таблиці	Форматувати, змінювати макет, обновляти або змінювати яким-небудь іншим способом звіти зведеної таблиці (Звіт зведеної таблиці. Інтерактивйий перехресний звіт Microsoft Excel, який містить зведені дані і виконуючий аналіз таких даних, як записи бази даних з різних джерел, в тому числі зовнішніх по відношенню до Microsoft Excel.), а також створювати нові звіти.
зміна проектів	Виконувати наступні дії: ▪ Вносити зміни в графічні проекти - у тому числі карти, впроваджені діаграми, фігури, текстові поля й елементи керування - які не були розблоковані перед установкою захисту листа. Наприклад, якщо на листі є кнопка, що запускає макрос, її можна нажати, щоб запустити макрос, але не можна видалити. ▪ Яким-небудь чином змінювати (наприклад, форматувати) впроваджену діаграму. Діаграма як і раніше буде обновлятися при змінах у джерелі її даних. ▪ Додавання або зміна приміток.
зміна сценаріїв	Перегляд сценаріїв, які були сховані, зміна сценаріїв з установленою забороною на зміни й видален-

	ня цих сценаріїв. Користувачі можуть змінювати значення в змінюваних комірках, якщо комірки не захищені, і додавати нові сценарії.
Уміст	Вносити зміни в елементи, що є частиною діаграми, такі як ряди даних, осі й легенди. Діаграма як і раніше буде відбивати зміни, внесені в її джерело даних.
Проекти	Вносити зміни в графічні проекти (включаючи фігури, текстові поля й елементи керування), якщо проекти не були розблоковані перед установкою захисту листа діаграми.

ПРИМІТКА. Пароль задавати необов'язково. Однак якщо не задати пароль, будь-який користувач зможе зняти захист із листа, і змінити захищені елементи. Переконайтеся, що обрано пароль, який легко запам'ятати, тому що якщо пароль буде загублений, одержати доступ до захищених елементів листа буде неможливо.

Захист елементів книги

1. На вкладці Рецензування групі Зміни виберіть команду Захистити книгу.
2. У розділі Захистити книгу виконайте одну з наступних дій:

- Щоб захистити структуру книги, установіть прапорець Структура.
- Щоб при кожному відкритті книги її вікна зберігали свій розмір і положення, установіть прапорець Вікна (рис. 3.30).

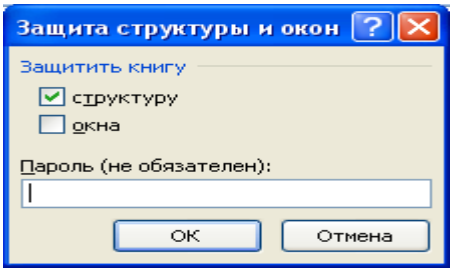


Рис. 3.30 Вікно захисту книги.

Таблиця 3.2

Додаткові відомості про елементи, які можно вибрати

Установіть прапорець	Щоб заборонити користувачам
Структура	Перегляд аркушів, які були сховані. Переміщення, видалення, приховання або перейменування аркушів. Вставку нових аркушів або листів діаграм (Лист діаграми. Лист книги, який містить тільки діаграму. Листи діаграми дозволяють переглядати діаграму або звіт зведеної діаграми окремо від даних листа або звіту зведеної таблиці.). ПРИМІТКА. Користувачі зможуть вставляти впроваджені діаграми (Впроваджена діаграма. Діаграма, яка поміщена на звичайний лист, а не на окремий лист діаграми. Впроваджені діаграми зручні для перегляду або друку звіту зведеної діаграми разом з вихідними даними і іншими довідками, які містяться на листі.) впроваджений лист. Переміщення або копіювання аркушів в іншу книгу. У звітах зведеної таблиці - відображення вихідних даних комірки в області даних або відображення сторінок полів сторінки на окремих аркушах. Для сценаріїв - створення підсумкового звіту зі сценаріях. У пакеті аналізу - використання інструмента аналізу, що відображає результати в новому листі. Запис нових макросів. ПРИМІТКА. При запуску макросу, що включає операцію, що не може бути виконана в захищеній книзі, з'являється попередження, а виконання макросу припиняється.
Вікна	Зміна розміру й положення вікон книги при її відкритті.

	Переміщення, зміна розміру або закриття вікон. ПРИМІТКА. Користувачі зможуть приховувати й відображати вікна.

3. Щоб інший користувач не зміг зняти захист із листа, уведіть пароль у поле Пароль (не обов'язковий), натисніть кнопку ОК, а потім ще раз уведіть цей пароль для підтвердження.

ПРИМІТКА. Пароль задавати необов'язково. Однак якщо не задати пароль, будь-який користувач зможе зняти захист із книги, і змінити захищені елементи. Переконайтеся, що обрано пароль, який легко запам'ятати, тому що якщо пароль буде загублений, одержати доступ до захищених елементів книги буде неможливо.

Захист елементів загальної книги

Якщо книга вже є загальною (Загальна книга. Книга, налагоджена для одночасного перегляду і змін з мережі декількома користувачами.)

Для того щоб закрити спільний доступ до книги, необхідно виконати наступні дії:

1. Попросіть інших користувачів зберегти й закрити загальну книгу, щоб запобігти втраті не збережених даних.

2. Щоб зберегти копію відомостей журнала змін (Журнал змін. Відомості в загальній книзі про зміни, які внесені в ході останніх сеансів роботи. Зберігаються відомості про того, хто вніс зміни, коли зміни були зроблені і які дані були змінені.), які будуть загублені при закритті загального доступу до книги, виконайте наступні дії:

1. На вкладці Рецензування групі Зміни виберіть команду Виправлення, а потім виберіть у списку пункт Виділяти виправлення.

2. Зніміть прапорець Відслідковувати зміни (рис. 3.31).

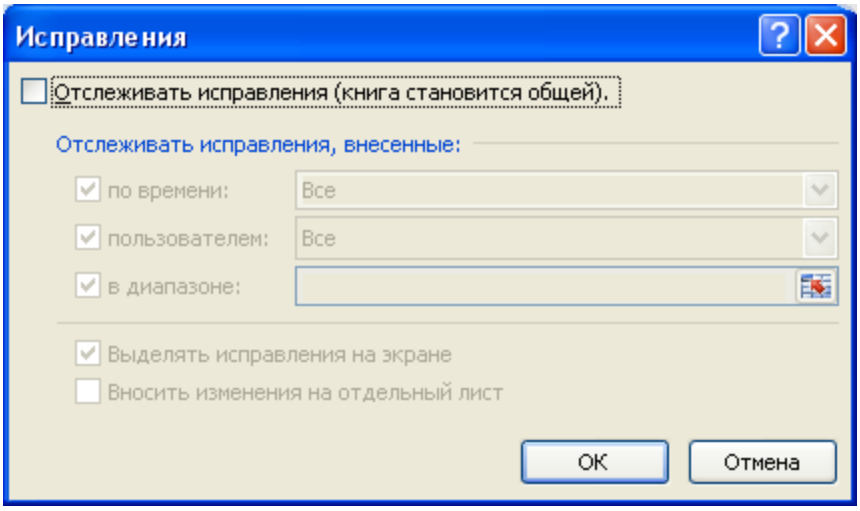


Рис. 3.31 Вікно вибору параметрів

3. Установіть прапорець Вносити зміни на окремий лист, а потім натисніть кнопку ОК.

Виконайте одну з наступних дій:

1. Щоб надрукувати лист журналу, натисніть кнопку Друк .

2. Щоб скопіювати журнал в іншу книгу, виділіть комірки, які потрібно скопіювати, натисніть кнопку Копіювати на вкладці Головна в групі Буфер обміну, перемкніться у вікно іншої книги, виберіть місце для розміщення скопійованих даних, а потім натисніть кнопку Вставити на вкладці Головна в групі Буфер обміну.

ПРИМІТКА. Поточну версію книги можна також зберегти або надрукувати, тому що цей журнал може бути не застосований до наступних версій книги. Наприклад, адреси комірок, включаючи номера рядків, у скопійованому журналі можуть уже не відповідати дійсності.

3. У загальній книзі на вкладці Рецензування в групі Зміни натисніть кнопку Доступ до книги.

4. На вкладці Виправлення переконайтеся, що ви - єдиний користувач у списку Файл відкритий наступними користувачами (рис.3.32)

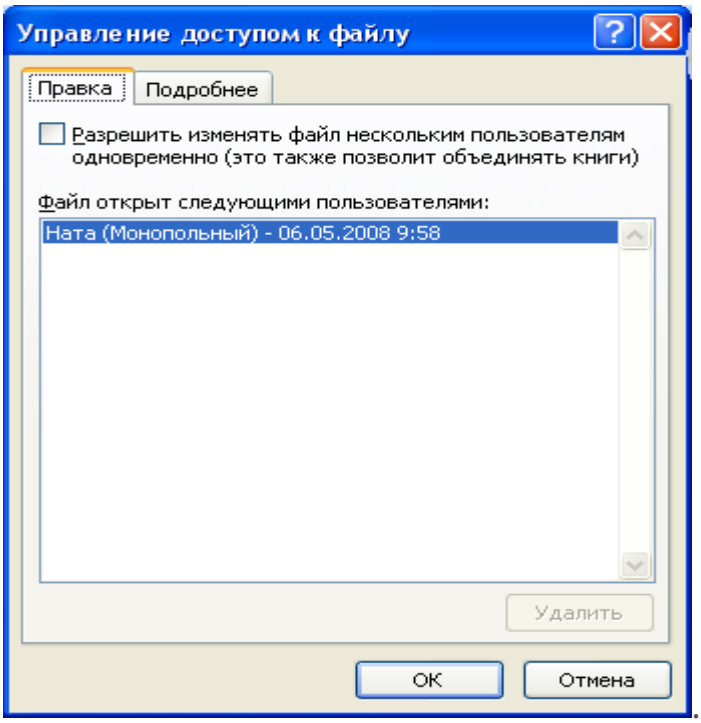


Рис. 3.32 Вікно Доступ до книги

5. Зніміть прапорець Дозволити змінювати файл декільком користувачам одночасно (це також дозволить поєднувати книги).

ПРИМІТКА. Якщо цей прапорець недоступний, необхідно спочатку зняти захист із книги, а потім зняти цей прапорець. Виконайте наступні дії:

1. Натисніть кнопку ОК, щоб закрити діалогове вікно Доступ до книги.

2. На вкладці Рецензування групі Зміни виберіть команду Захист книги.

3. Якщо буде запропоновано, уведіть пароль (Пароль. Спосіб обмеження доступу до книги, листу або частини листа. В Microsoft Excel довжина пароля не повинна перевищувати 255 букв, цифр, пробілів і інших символов. При введенні пароля враховується регистр букв.), а потім натисніть кнопку ОК.

4. На вкладці Рецензування в групі Зміни виберіть команду Доступ до книги.

5. На вкладці Виправлення зніміть прапорець Дозволити змінювати файл декільком користувачам одночасно (це також дозволить поєднувати книги).

6. Якщо з'явиться повідомлення про вплив на інших користувачів, натисніть кнопку Так.

При необхідності надайте певним користувачам доступ до діапазонів, захистіть аркуші й елементи книги й задайте паролі для перегляду й зміни.

1. На вкладці Рецензування у групі Зміни виберіть команду Доступ до книги.
2. Установіть прапорець Загальний доступ із виправленнями.
3. Щоб зобов'язати інших користувачів уводити пароль для відключення журналу змін або видалення книги із загального користування, уведіть пароль у поле Пароль (не обов'язковий), натисніть кнопку ОК, а потім уведіть пароль ще раз для підтвердження.
4. Якщо буде запропоновано, збережіть книгу.

Основні відомості про безпеку макросів

В Microsoft Office Excel можна вибирати настроювання безпеки для керування ситуацією при відкритті книги з макросами. Наприклад, можна зробити так, щоб запускалися тільки макроси, що мають цифровий підпис розроблювача, чиє ім'я втримується в списку надійних джерел.

Настроювання безпеки макросів і її дія

Змінити налагодження безпеки макросів можна в центрі управління безпекою (кнопка Microsoft Office  , кнопка - Параметри Excel, категорія - Центр управління безпекою, рис. 3.33, кнопка - Параметри центру управління безпекою, категорія - Параметри макросів, рис. 3.34; або вкладка - Розробник, група - Код, кнопка - Безпека макросів). Проте потрібно врахувати, що при роботі в локальній мережі системний адміністратор міг змінити налагодження за умовчанням і зробити неможливим їх зміну користувачем.

Примітка. Усі зміни параметрів макросів, зроблені в застосуванні Excel в категорії Параметри макросів, діють тільки в цьому застосуванні й не впливають на інші застосування Office.

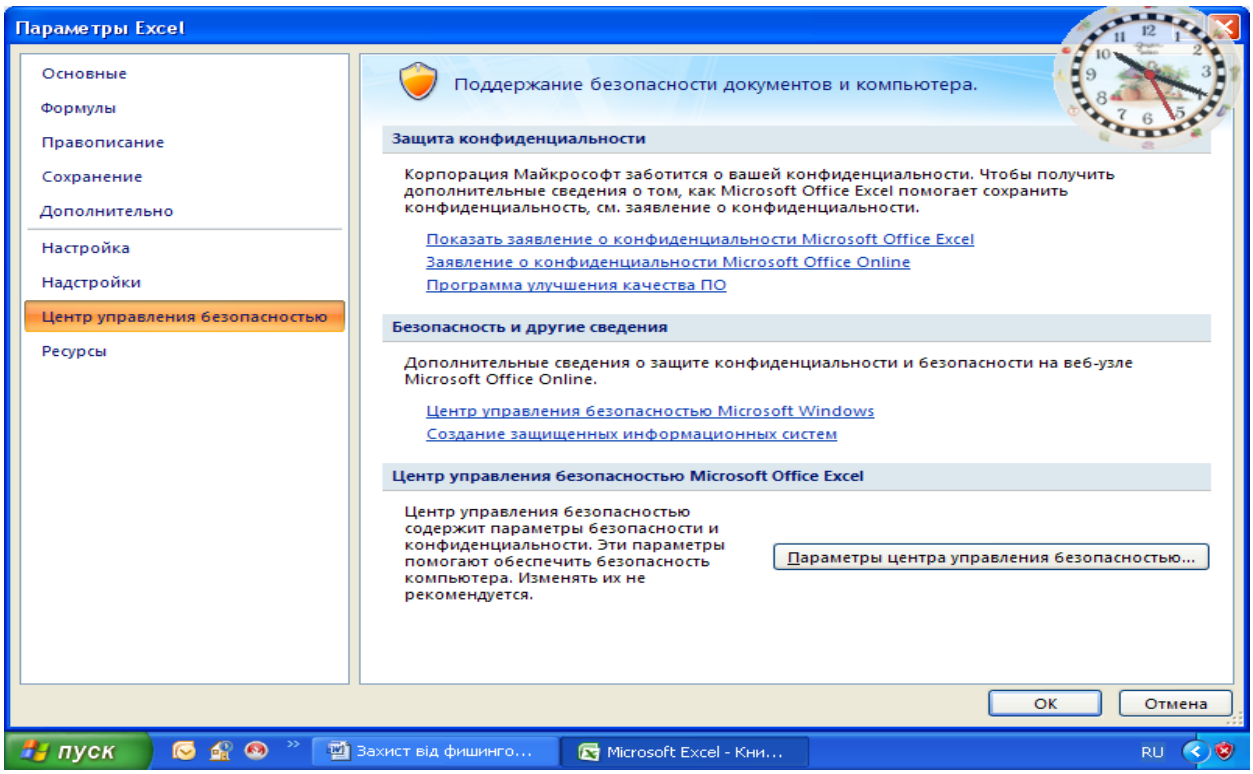


Рис. 3.32 Вікно параметрів Excel

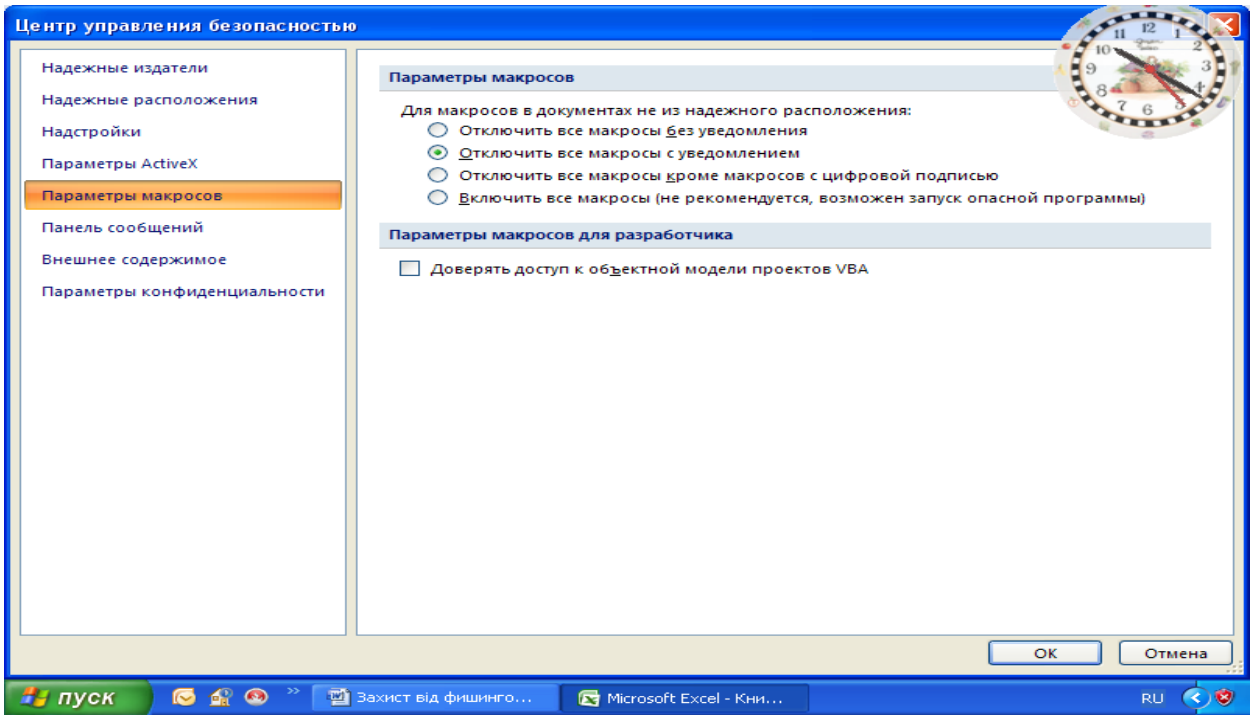


Рис. 3.33 Вікно Параметри макросів

Таблиця 3.3

Параметр безпеки макросів

Параметр безпеки макросів	Ціль
Відключити всі макроси без повідомлення	Цей варіант варто вибрати, якщо не довіряєте макросам. У документах будуть відключені всі макроси й всі повідомлення системи безпеки про макроси. Якщо в деяких документах є непідписані макроси, до яких є довіра, ці документи потрібно помістити в надійне розташування. Документи, розміщені в надійних розташуваннях, запускаються без перевірки системою безпеки центра керування безпекою.
Відключити всі макроси з повідомленням	Даний варіант установлений за замовчуванням. У цьому випадку самі макроси відключаються, але при їхній наявності видаються повідомлення системи безпеки. Тут можна вибрати включення макросів залежно від ситуації.
Відключити всі макроси крім макросів із цифровим підписом	Цей варіант подібний до варіанта Відключити всі макроси з повідомленням, але, якщо макрос має цифровий підпис довіреного видавця й ви вже довіряли цьому видавцеві, виконання цього макросу дозволяється. Якщо ви ще не довіряли цьому видавцеві, видається оповіщення. Тут можна дозволити виконання підписаних макросів або довіритися видавцеві. Всі непідписані макроси відключаються без оповіщення.
Включити всі макроси (не рекомендується, можливий запуск небезпе-	Дане настроювання тимчасово дозволяє виконання всіх макросів. Цей варіант не рекомендується для постійного користування, оскільки він робить

чної програми)	комп'ютер уразливим для потенційно небезпечних програм.
Довіряти доступ до про'єктної моделі проектів VBA	Цей варіант призначений тільки для розроблювачів.

Цифрові підписи і їхня дія

У 2007 Office для надання можливості розроблювачам макросів цифрового підпису використовується технологія Microsoft Authenticode. (Цифровий підпис. Шифрований електронний підпис, який підтверджує достовірність макроса або документа. Наявність цифрового підпису підтверджує, що макрос або документ був отриманий від власника підпису і не був змінений.)

Проекта макроса (Проект макроса. Сукупність компонентів, в тому числі форм, текста програми і модулів класів, які складають макрос. Проекти макросів, створені в редакторі Microsoft Visual Basic для додатків, можно включати в надбудови і більшість додатків Microsoft Office.) Сертифікат, використовується для створення такого підпису, підтверджує, що макрос або документ виходять від їхнього творця, що підписав, а підпис підтверджує, що макрос або документ не були змінені.

Підписувати файли й проекти макросів можна після установки цифрового сертификата (Цифровий сертифікат. Вкладення в файл, проект макроса або повідомлення електронної пошти, яке підтверджує його достовірність, яке забезпечує шифрування або надає підпис, який піддається перевірці. Для цифрового підписання проектів макросів необхідно встановити цифровий сертифікат).

Цифровий підпис макросів

Макроси варто підписувати тільки після того, як вони протестовані й готові до реалізації, тому що при будь-якій зміні коду підписаного макросу цифровий підпис знімається. Однак якщо на комп'ютері встановлений відповідний цифровий сертифікат, макрос автоматично підписується заново при збереженні. Щоб не допустити випадкової зміни макросу або порушення його підпису користувачами, варто заблокувати макрос перед підписанням. Цифровий підпис тільки гарантує безпеку даного

проекту. Він не підтверджує авторство проекту. Таким чином, блокування проекту макросу не перешкодить іншому користувачеві замінити даний цифровий підпис іншім. Системні адміністратори компаній можуть заново підписувати шаблони й надбудови для точного контролю над тим, які макроси виконуються на комп'ютерах користувачів.

При створенні надбудови, що додає в проект макросу текст програми, цей текст перед збереженням повинен визначати, чи підписаний проект, і сповіщати користувача про наслідки зміни підписаного проекту.

Одержання цифрового сертифіката для постановки підпису

Цифровий сертифікат можна одержати в комерційному центрі сертифікації (Центр сертифікації (ЦС) в адміністратора з безпеки локальної мережі компанії або в професійного фахівця з інформаційних технологій. Комерційна організація, яка випускає цифрові сертифікати, що відслідковує, кому вони були призначені, яка підписує сертифікати для посвідчення їх дійсності і відслідковуюча за терміном дії випущених сертифікатів),

Створення власного цифрового сертифіката для постановки власних підписів

Власний сертифікат можна створити за допомогою програми, наприклад, Selfcert.exe.

ПРИМІТКА. Створювані за допомогою цієї програми цифрові сертифікати не підтверджені ніяким офіційним органом сертифікації, тому проекти макросів, підписані з використанням таких сертифікатів, називаються проектами із власними підписами. Додатка Microsoft® Office довіряють власним сертифікатам тільки на тих комп'ютерах, де даний сертифікат внесений у сховище особистих сертифікатів.

Створення цифрового сертифіката для власного підпису

Створення сертифіката:

1. Виконайте одну з наступних дій:

- В Microsoft Windows Vista натисніть кнопку Пуск, послідовно виберіть Усі програми, Microsoft Office, Засоби Microsoft Office і Цифровий сертифікат для проектів VBA. У поле Ім'я сертифіката введіть описове ім'я для сертифіката.

- В Microsoft Windows XP натисніть кнопку Пуск, послідовно виберіть Усі програми, Microsoft Office, Засоби Microsoft Office і Цифровий сертифікат для проектів VBA. У поле Ім'я сертифіката введіть описове ім'я для сертифіката.

2. Коли з'явиться повідомлення про підтвердження сертифіката, натисніть кнопку ОК.

Щоб переглянути сховище особистих сертифікатів, виконайте наступні дії.

1. Відкрийте оглядач Internet Explorer.
2. У меню Сервіс виберіть Властивості оглядача, а потім - вкладку Зміст.
3. Натисніть кнопку Сертифікати й перейдіть на вкладку Особисті.

Цифровий підпис проекту макросу

1. Відкрийте файл, що містить проект макросу, який потрібно підписати.
2. Виконайте наступні дії в додатках Word, Excel або PowerPoint

Випуск 2007 Microsoft Office:

- На вкладці Розроблювач (рис. 3.34)у групі Код натисніть кнопку Visual Basic (рис. 3.35).
- У меню Сервіс (Tools) виберіть пункт Макрос і потім клацніть Редактор Visual Basic.
- У вікні проекту Visual Basic виберіть проект, що потрібно підписати.

3. У меню Сервіс виберіть Цифровий підпис.
4. Виконайте одну з наступних дій.

- Якщо цифровий сертифікат не був заздалегідь обраний або необхідно скористатися іншим сертифікатом, натисніть кнопку Вибрати, виберіть сертифікат і двічі натисніть кнопку ОК.
- Для використання поточного сертифіката натисніть кнопку ОК.
- ПРИМІТКИ
- Макроси варто підписувати тільки після їхнього тестування й готовності до поширення, оскільки при будь-якій зміні програмного коду підписаного проекту макросу його цифровий підпис видаляється. Однак при наявності на комп'ютері дій-

сного цифрового сертифіката, що використовувався раніше для підпису даного проекту, змінений проект макросу при збереженні буде автоматично підписаний заново.

▪

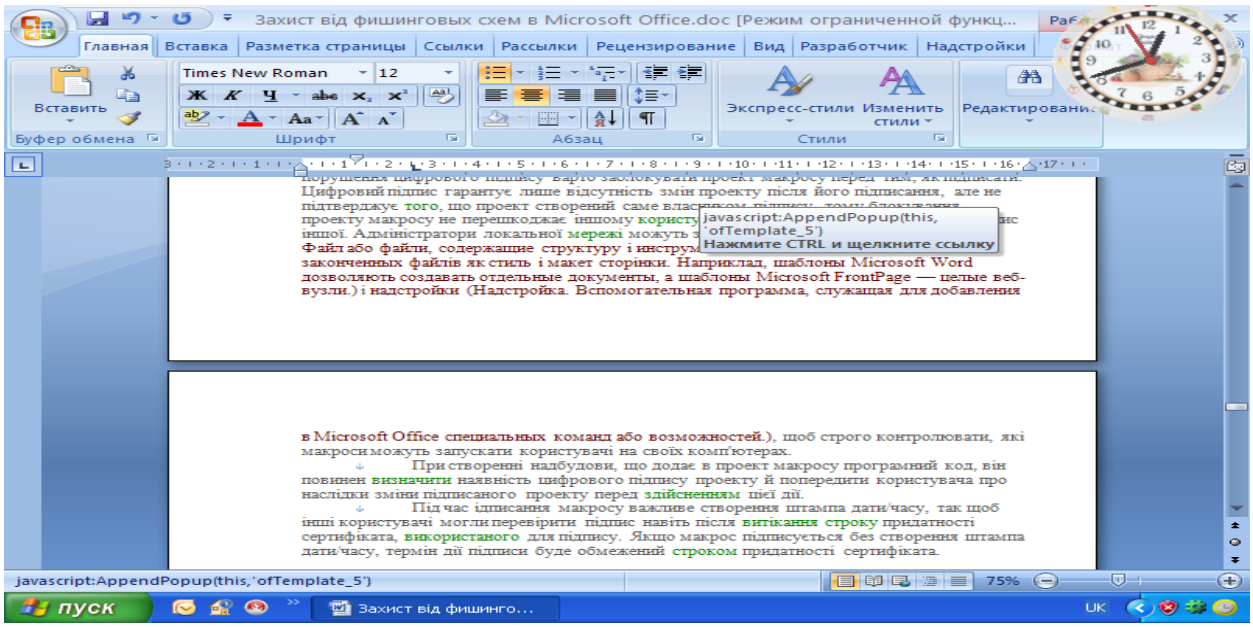


Рис. 3.34 Вікно Розроблювача

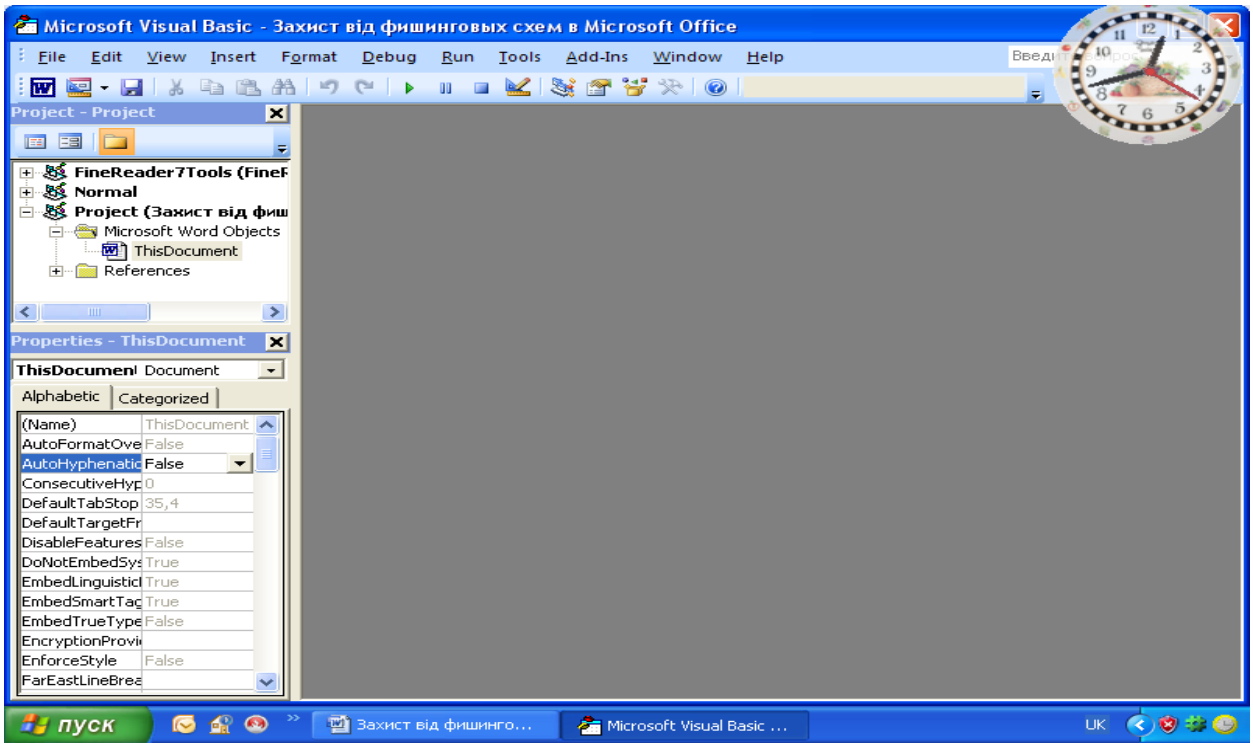


Рис. 3.35 Вікно Visual Basic

▪ Для запобігання випадкової зміни користувачами проекту макросу й порушення цифрового підпису варто заблокувати проект макросу перед тим, як підпи-

сати. Цифровий підпис гарантує лише відсутність змін проекту після його підписання, але не підтверджує того, що проект створений саме власником підпису, тому блокування проекту макросу не перешкоджає іншому користувачеві замінити даний цифровий підпис іншим. Адміністратори локальної мережі можуть заново підписати шаблони (Шаблон. Файл або файли, які містять структуру і інструменти для створення таких елементів файлів як стиль і макет сторінки. Наприклад, шаблони Microsoft Word дозволяють створювати окремі документи, а шаблони Microsoft FrontPage — цілі веб-вузли.) і надбудови (Надбудова. Допоміжна програма, яка служить для добавления в Microsoft Office спеціальних команд або можливостей.), щоб суворо контролювати, які макроси можуть запускати користувачі на своїх комп'ютерах.

- При створенні надбудови, що додає в проект макросу програмний код, він повинен визначити наявність цифрового підпису проекту, і попередити користувача про наслідки зміни підписаного проекту перед здійсненням цієї дії.
- Під час підписання макросу важливе створення штампа дати/часу, так щоб інші користувачі могли перевірити підпис навіть після витікання строку придатності сертифіката, використаного для підпису. Якщо макрос підписується без створення штампа дати/часу, термін дії підписи буде обмежений терміном придатності сертифіката.

Захист інформації у Microsoft Access 2003

Паролі MS Access

Паролі зберігаються в заголовку файлу. Заголовок, зашифрований за стандартом RC4, але ключ шифрування має довжину 32 біта і зберігається в одній із системних DLL. Знаючи цей ключ, можна знайти будь-який пароль на базу MS Access. Інформація про користувачів зберігається у файлі system.mdw. Паролі, зашифровані за алгоритмом DES, але ключ шифрування зберігається в системній DLL. У такий спосіб можливо визначити пароль будь-якого користувача, у тому числі й адміністратора.

У Microsoft Access використовуються три типи паролів. Обраний тип парольного захисту визначає рівень доступу користувачів до бази даних і об'єктам, що міститься в ній.

Паролі баз даних

Якщо встановлений пароль бази даних, уведення цього пароля потрібно від кожного користувача, що відкриває базу даних. Визначення пароля бази даних є найпростішим засобом захисту від відкриття бази даних несанкціонованим користувачем. Однак після відкриття бази даних інших засобів захисту при цьому не мається, якщо додатково не визначений захист на рівні користувачів.

Microsoft Access зберігає пароль бази даних у незашифрованому вигляді. Якщо це порушує безпеку бази даних, що захищається паролем, то для захисту бази даних не слід використовувати пароль. Замість цього, визначите захист на рівні користувачів, що дозволяє керувати доступом до важливої інформації у базі даних.

Паролі облікових записів користувачів.

Коли для робочої групи визначений захист на рівні користувачів, стає можливим використання паролів облікових записів. Пароль облікового запису користувача забороняє іншим користувачам реєстрацію з використанням даного облікового запису.

Microsoft Access за замовчуванням надає порожній пароль убудованого облікового запису користувача «Admin» і всім новим обліковим записам користувачів, створюваним у робочій групі. При організації захисту бази даних розроблювач повинен визначити паролі для наступних облікових записів:

- обліковий запис користувача «Admin» (для активізації діалогового вікна Вхід);
- обліковий запис користувача, що є власником бази даних і таблиць, які містяться в ній, запитів, форм, звітів і макросів;
- будь-який обліковий запис користувача, доданий у групу «Admins».

Крім того, можна додати паролі для створюваних облікових записів користувачів або надати можливість користувачам додати власні паролі.

Користувачі можуть створювати або змінювати власні паролі облікових записів. Однак якщо користувач забув свій пароль, то зняти цей пароль може тільки адміністратор.

Паролі Microsoft Visual Basic для додатків (VBA).

На додаток до паролів, описаних вище, можна задавати паролі Visual Basic для додатків (VBA). Ці паролі використовуються для захисту програм мовою VBA у стандартних модулях і модулях, таких як модулі з програмами форм і звітів. Цей пароль вводиться при першій спробі відкрити будь-яку програму VBA і запобігає редагуванню, вирізанню, вставці, копіюванню, експорту й видалення програми несанкціонованими користувачами.

Установлення пароля баз даних.

Закрийте базу даних. Якщо база даних відкрита для загального доступу в мережі, переконайтеся, що всі інші користувачі закрили її.

Зробіть резервну копію бази даних і збережіть її на диску “С” вашого комп'ютера.

У меню **Файл** виберіть команду **Відкрити**. Відкрийте базу даних у **режимі Монопольно** (рис. 3.36). У меню **Сервіс** виберіть команду **Захист** і підкоманду **Задати пароль бази даних**. Уведіть пароль у поле **Password**.

Угоди про паролі

Імена облікових записів можуть мати довжину від 1 до 20 символів і можуть складатися з букв, цифр, пробілів і символів із розширених наборів, за винятком наступних:

- Знаки " \ [ ] : | < > + = ; , . ? *
- Пробіли на початку імені;
- Керуючі знаки (із кодами ASCII від 10 до 31).

Примітка:

У паролях враховується регістр символів.

Для підтвердження пароля введіть його ще раз у поле **Підтвердження**, а потім натисніть кнопку **OK** (рис. 3.37). Тепер пароль заданий. При наступному відкритті бази даних з'являється діалогове вікно, у яке необхідно ввести пароль.

Примітки:

Пароль бази даних зберігається в базі даних, а не у файлі робочої групи. Якщо таблиця з захищеної паролем бази даних є зв'язаною, то при встановленні зв'язку пароль зберігається (поміщається в тимчасовий буфер) у базі даних, із якою зв'язується таблиця. Це дозволить будь-якому користувачу бачити ваші дані.

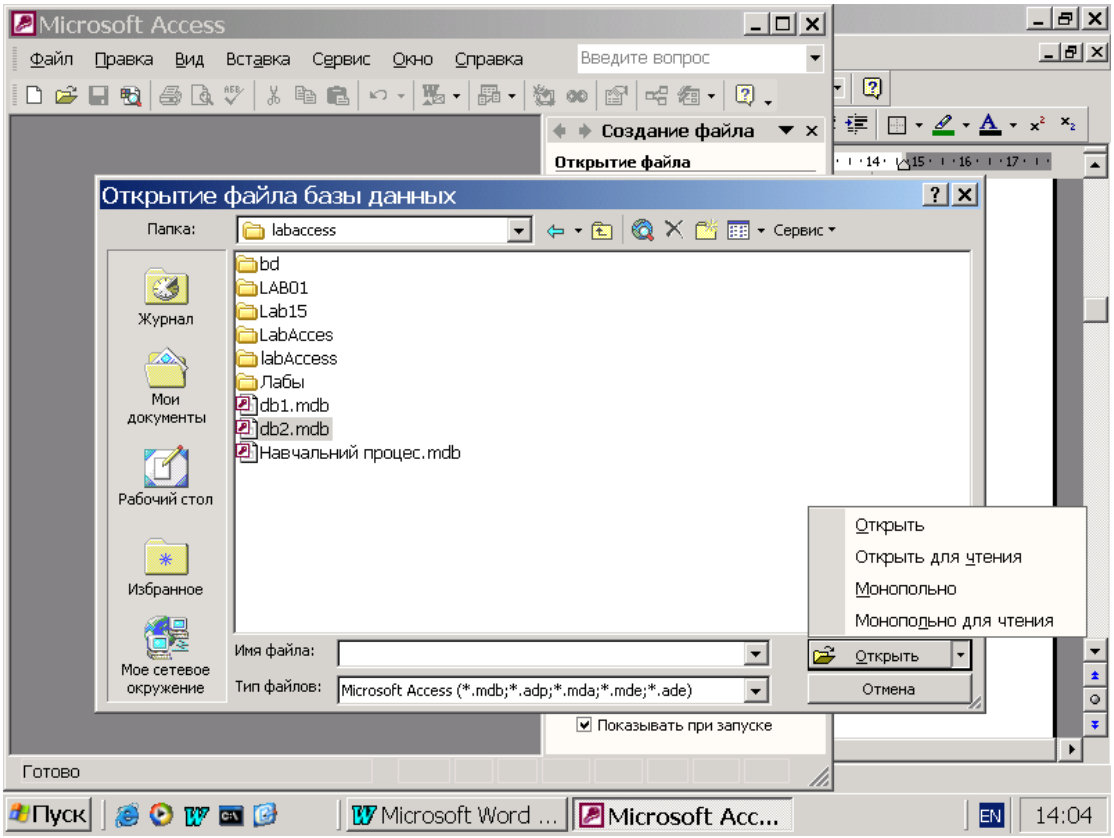


Рис. 3.36. Вібір монопольного режиму відкриття бази даних.

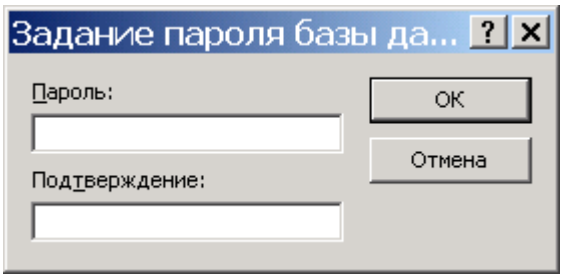


Рис. 3.37. Вікно введення паролю.

Установлення пароля в проекті Microsoft Access (.adp)

На відміну від бази даних Microsoft Access у проекті не можна захистити форми, звіти або макроси за допомогою захисту на рівні користувачів, а також не можна установити пароль на файл проекту Microsoft Access (.adp). Для захисту об'єктів або форми звіту можна сховати ці об'єкти у вікні бази або даних настроїти параметри запуску. Для захисту доступу до макетів форм і звітів у проекті Microsoft Access можна задати параметри запуску або зберегти проект Microsoft Access у вигляді файлу .ade. Для захисту доступу до макросів у файлі проекту скористайтеся параметрами запуску. Сторінку доступу до даних можна захистити за допомогою засобів захисту файлів і каталогів операційної системи. Для захисту програми Visual Basic для додатків можна перетворити файл проекту у файл .ade або установити пароль.

Відображення й приховання об'єктів бази даних у вікні бази даних.

У списку **Об'єкти** вікна бази даних виберіть тип об'єкта бази даних, властивості якого потрібно змінити. Натисніть кнопку **Властивості** на панелі інструментів **База даних**. Установіть або зніміть прапорець **Прихований** (рис.3.38).

Примітка:

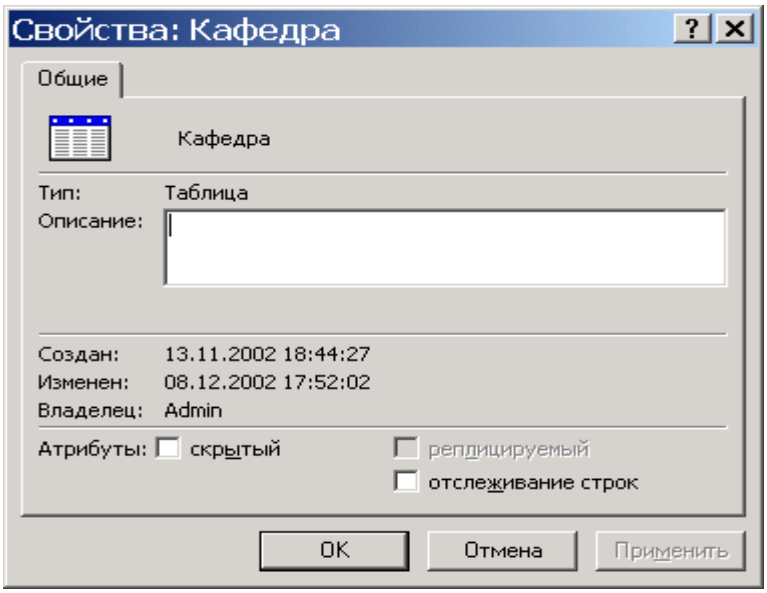


Рис. 3.38. Вікно присвоєння або зняття атрибуту прихований.

У проекті Microsoft Access не можна змінювати властивості таблиць, або запитів схем бази даних, тому що ці об'єкти знаходяться в базі даних Microsoft SQL Server. Допускається зміна властивостей форм, звітів, макросів і модулів, тому що ці об'єкти знаходяться в самому проекті Microsoft Access, а не в базі даних Microsoft SQL Server. Можна також змінювати властивості сторінок доступу до даних.Відображення або приховання об'єктів, схованих за замовчуванням.

Якщо потрібно виконати які-небудь дії з об'єктами, що були визначені як сховані, можна відобразити ці об'єкти у вікні бази даних, не скасовуючи їхнього атрибута приховання.

У меню **Сервіс** виберіть команду **Параметри**. Виберіть вкладку **Вид**. **Установіть або зніміть прапорець** сховані об'єкти в групі **Відображати**. Щоб показати розходження між схованими й іншими об'єктами, сховані об'єкти відображаються у вигляді сірих значків.

Аналогічно відображаються або приховуються системні об'єкти.

Використання параметрів запуску.

Для вказівки, наприклад, відображення форми, можливості зміни панелей інструментів, а також контекстних меню, доступних у файлі Microsoft Access, можна скористатися параметрами запуску. Крім того, спеціальний макрос AutoExec дозволяє автоматично виконати макрокоманду або набір макрокоманд при відкритті бази даних. У процесі відкриття бази даних Microsoft Access виконує пошук макросу з цим ім'ям і, якщо такий макрос існує, автоматично запускає його.

параметри або введіть потрібні значення (рис. 3.39). Для одержання додаткових даних про визначений елемент діалогового вікна натисніть кнопку контекстної довідки у верхньому куті вікна і виберіть відповідний елемент.

Захист сторінок доступу до даних.

Сторінками доступу до даних називають файли HTML (Hypertext Markup Language), що містять посилання на дані з бази даних. Сторінки доступу до даних

Налагодження параметрів запуску.

У меню **Сервіс** виберіть команду **Параметри запуску.** Виберіть потрібні

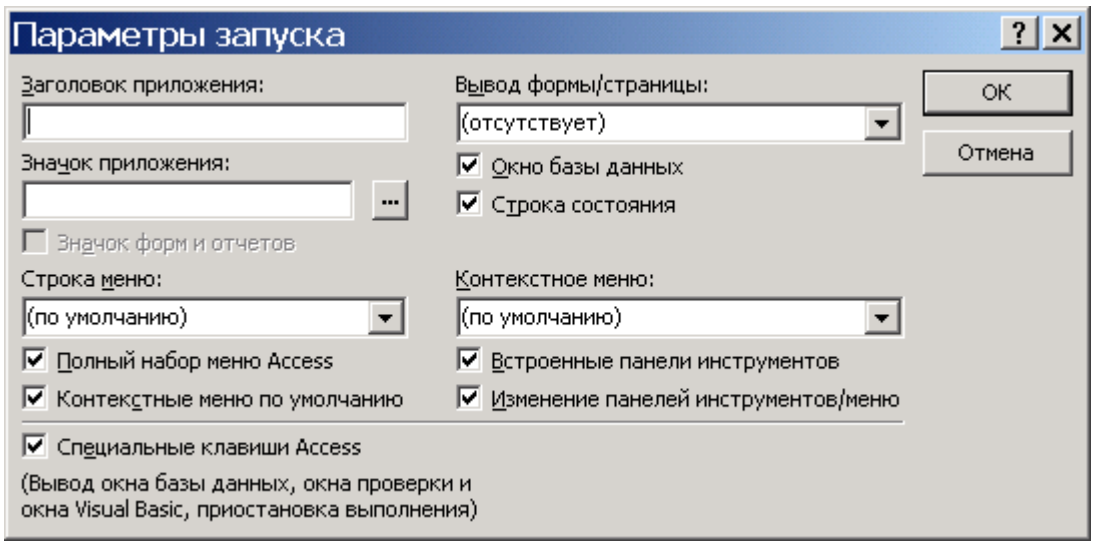


Рис. 3.39. Вікно відбору параметрів запуску.

фактично не зберігаються у файлі Microsoft Access. Через це Microsoft Access не забезпечує контроль за безпекою файлів сторінок доступу до даних. Щоб захистити сторінку доступу до даних, збережену в локальній або мережній файловій системі (у припущенні, що маються відповідні дозволи), можна використовувати наступну операцію.

Відкрийте вікно **Провідник** Windows або каталог **Мій комп'ютер**. Знайдіть каталог, у якому зберігається файл HTML сторінки доступу до даних. За замовчуванням файл зберігається в одному каталозі з базою даних Microsoft Access. Клацніть правою кнопкою файл сторінки доступу до даних (.htm) або каталог, що містить файл, виберіть команду **Властивості** в контекстному меню, а потім установіть прапорець **Тільки для читання**.

Видалення пароля в базі даних Microsoft Access (.mdb)

У меню **Файл** виберіть команду **Відкрити**. Відкрийте базу даних у режимі **Монопольно**. У діалоговому вікні **Необхідно ввести пароль** уведіть пароль бази даних і натисніть кнопку **OK**. У меню **Сервіс** виберіть команди **Захист** і **Видалити пароль бази даних**. Ця команда доступна, коли пароль бази даних уже встановлений. У діалоговому вікні **Видалення пароля** бази даних уведіть поточний пароль.

Створення або зміна пароля облікового запису користувача в базі даних Microsoft Access

Запустіть Microsoft Access із використанням тієї робочої групи, у якій зберігається обліковий запис користувача, і ввійдіть у нього з тим обліковим записом, для якого потрібно створити або змінити пароль. Для перевірки імені поточної робочої групи або для зміни робочої групи використовуйте службову програму «**Адміністратор робочих груп**».

Відкрийте базу даних. У меню **Сервіс** виберіть команду **Захист**, а потім команду **Користувачі й групи** (рис.3.40). На вкладці **Зміна пароля** залишіть поле **Поточний пароль** порожнім, якщо обліковий запис раніше не мав пароля.

У противному випадку введіть у поле **Поточний пароль** старий пароль. Уведіть новий пароль у поле **Новий пароль**. Повторно введіть новий пароль у поле Підтвердження і натисніть кнопку **OK**.

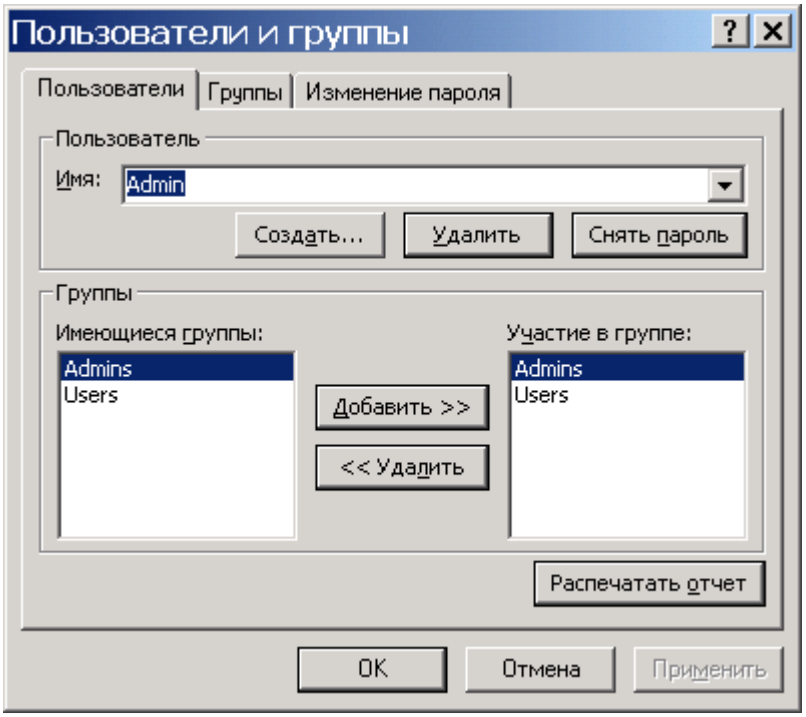


Рис. 3.40. Вікно користувачів та груп.

Зняття пароля облікового запису користувача

Для виконання даної процедури необхідно ввійти в базу за обліковим записом члена групи «Admins». Запустіть Microsoft Access із використанням файлу робочої

групи, у якому зберігається обліковий запис користувача. Довідатися про ім'я поточного файлу робочої групи або змінити робочу групу можна за допомогою адміністратора робочих груп.

Відкрийте базу даних. У меню **Сервіс** виберіть команду **Захист**, а потім команду **Користувачі й групи**. На вкладці **Користувачі** введіть ім'я облікового запису користувача в поле **Ім'я**. Натисніть кнопку **Зняти пароль**.

Захист паролем програми Microsoft Visual Basic для додатків (VBA)

Для запобігання перегляду й внесення небажаних змін у програму Microsoft Visual Basic для додатків (VBA) можна захистити програму за допомогою пароля. Відкрийте проект Microsoft Access (.adp) або базу даних Microsoft Access (.mdb), що містить програму VBA, яку потрібно захистити. У меню **Сервіс** вікна бази даних виберіть команду **Макрос** і підкоманду **Редактор Visual Basic** (рис. 3.41).

Примітка:

Для запуску редактора Visual Basic можна також натиснути клавіші **ALT+F11**. У меню **Tools** редактора Microsoft Visual Basic виберіть команду **Ім'я бази даних або проекту Microsoft Access Project Properties**. На вкладці **Protection** установіть прапорець **Lock project for viewing**. Якщо пароль заданий, але прапорець **Lock project for viewing** не установлений, програму зможе переглядати й редагувати будь-який користувач, але діалогове вікно **Project Properties** буде захищено. Уведіть пароль у поле **Password**.

Підтвердіть пароль, повторно ввівши його в поле **Confirm password**, і натисніть кнопку **OK**. Тепер пароль заданий. При наступному відкритті бази даних з'являється діалогове вікно, у яке необхідно ввести пароль.

Захист інформації у Microsoft Access 2007

1. Можливості системи безпеки в Office Access 2007

Нижче наведений список засобів забезпечення безпеки в Office Access 2007.

- Перегляд даних навіть при відключеному коді Microsoft Visual Basic для додатків (VBA) або відключених компонентах у базі даних. Якщо в Microsoft Office Access 2003 установлюється рівень безпеки «Високий», необхідно підписати кодом

базу даних і надати їй стан довіреної, щоб можна було переглянути дані. В Office Access 2007 можна відкривати бази даних, і переглядати дані без запиту про включення вмісту бази даних.

- Спрощене відкриття баз даних. Якщо файли бази даних (як у новому форматі Office Access 2007, так і в більше ранніх) розташовані в надійному місці, наприклад, у папці або в загальному мережевому ресурсі, які зазначені як надійні, вони будуть відкриватися, і оброблятися без повідомлень із попередженнями й запитом про включення або відключення вмісту. При відкритті в Office Access 2007 баз даних із більше ранніх версій Access, наприклад, файлів із розширеннями mdb або mde, які мають цифровий підпис, і видавець яких уважається надійним, такі файли теж доступні без питань про довіру. Однак варто пам'ятати, що код VBA у підписаних базах даних не буде працювати, поки видавець не буде визнаний надійним, а також у тому випадку, якщо підпис стане недійсним. Підпис стає недійсним, коли хто-небудь, крім особи, що підписала, виконує неприпустимі дії з умістом бази даних.
- Центр керування безпекою. «Центр керування безпекою» — це діалогове вікно, у якому можна задавати й міняти параметри безпеки в Access. Воно використовується для створення або зміни надійних розташувань, а також для настроювання параметрів безпеки для Office Access 2007. Ці параметри визначають поводження нових і існуючих баз даних при їхньому відкритті в Access. Програмні засоби центра керування безпекою дозволяють оцінити компоненти бази даних і визначити, чи безпечно відкривати базу даних і чи варто заборонити користувачеві включати її..
- Менше повідомлень із попередженнями. У попередніх версіях Access користувачам доводилося мати справа з різними попереджуючими повідомленнями, що стосуються, наприклад, безпеки макросів і ізольованого режиму. За замовчуванням при відкритті бази даних Office Access 2007 поза довіреним розташуванням

Рис. 3.41 Вікно повідомлень

з'являється єдиний засіб, називаний «Панель повідомлень» (рис. 3.41).

- Якщо точно відомо, що можна довіряти вмісту бази даних, використовуйте засіб «Панель повідомлень», щоб включити всі компоненти — запити на зміну (запити, які додають, видаляють або змінюють дані), макроси, елементи керування Active, вираження (функції, що повертають одне значення) і програми на VBA — при відкритті бази даних, утримуючої один або кілька цих компонентів.
- Нові способи підпису й поширення файлів, створених у форматі Office Access 2007. У попередніх версіях Access для застосування сертифіката безпеки до індивідуальних компонентів бази даних використовувався редактор Visual Basic. В Office Access 2007 вона впаковується, а потім підписується й поширюється. При витягу бази даних із підписаного пакета й переміщенні в надійне розташування її відкриття відбувається без відображення панелі повідомлень. Якщо база даних із підписаного пакета відправляється в ненадійне розташування, але є надійний сертифікат пакета, і підпис дійсний, то немає необхідності вирішувати питання про довіру. Якщо впаковується й підписується база даних, що не має стану довіреного цифрового підпису, необхідно використовувати панель повідомлень для надання їй стану довіреної щораз при її відкритті, за винятком тих випадків, коли вона розміщена в надійному розташуванні.
- Більше стійкий алгоритм шифрування баз даних у форматі Office Access 2007 із використанням пароля бази даних. У процесі шифрування відбувається перемішування даних у таблицях, що виключає несанкціонований перегляд цих даних.
- Новий підклас макрокоманд, що виконуються при відключеній базі даних. Ці безпечні макрокоманди включають також можливості виправлення помилок. Макроси (навіть утримуючі команди, які Access відключає) можна впроваджувати безпосередньо у форми, звіти або властивості елементів керування, які будуть правильно працювати з модулем коду VBA, або макросом із більше ранніх версій Access.
- Починаючи роботу з базами даних, варто пам'ятати наступні правила.
- При відкритті бази даних у надійному розташуванні всі компоненти запускаються без перевірки на довіру.

- При впакуванні, підписуванні й розгортанні бази даних із більше ранніх версій Access (файли з розширеннями mdb або mde) усі компоненти запускаються без необхідності вирішувати питання про довіру в тому випадку, якщо вона має дійсний цифровий підпис надійного видавця, і сертифікат уважається надійним.
- При підписуванні й розгортанні бази даних, що не має стану довіри, у ненадійному розташуванні центр керування безпекою за замовчуванням відключає її, і щораз при відкритті потрібно включати її вміст.

2. Office Access 2007 і захист на рівні користувача

- Office Access 2007 не передбачає захист на рівні користувача для баз даних, створених у новому форматі (файли з розширенням accdb або accde). Однак при відкритті бази даних із більше ранньої версії Access, що має захист на рівні користувача, в Office Access 2007 ці параметри будуть продовжувати працювати.
- При перетворенні подібної бази даних у новий формат додаток Access автоматично видаляє всі параметри безпеки, і застосовує правила захисту файлів ACCDB і ACCDE.
- І, нарешті, варто пам'ятати, що щораз при відкритті бази даних, створеної в Office Access 2007, усі користувачі мають можливість перегляду всіх її проектів.

Структура системи безпеки Office Access 2007

1. Для розуміння структури системи безпеки Office Access 2007 необхідно пам'ятати, що база даних Access не є файлом, подібним до книги Microsoft Office Excel 2007 або документу Microsoft Office Word 2007. На відміну від них база даних являє собою набір про'єктів — таблиць, форм, запитів, макросів, звітів і т.д. — які часто є взаємозалежними. Наприклад, при створенні форми уведення даних не можна вводити в неї, або зберігати в ній дані, якщо елементи керування в цій формі не пов'язані з таблицею.

2. Деякі компоненти Access можуть бути небезпечні, у тому числі запити на зміну (запити, які додають, видаляють або змінюють дані), макроси, вираження (функції, що повертають одне значення) і код VBA. Щоб захистити дані, Office

Access 2007 і центр керування безпекою виконують ряд перевірок на безпеку щораз при відкритті бази даних. Процес відбувається в такий спосіб:

3. При відкритті в Office Access 2007 ACCDB- або ACCDE-Файлу додаток Access повідомляє розташування бази даних центру керування безпекою. Якщо це розташування надійне, вона працює з повним набором функціональних можливостей. При відкритті бази даних із більше ранньої версії Access в Office Access 2007 у центр керування безпекою передаються розташування й цифровий підпис, якщо він є в базі даних.

Центр керування безпекою перевіряє дійсність цього «посвідчення», щоб визначити, чи має база даних стан довіреної, а потім інформує додаток Access про те, як треба її відкривати. Додаток Access або відключає її, або відкриває з повним набором функціональних можливостей.

ПРИМІТКА.

- Варто пам'ятати, що параметри, обрані користувачем або системним адміністратором у центрі керування безпекою, управляють рішеннями про довіру, прийнятими при відкритті бази даних в Access.
- Якщо центр керування безпекою відключає який-небудь уміст, то при відкритті бази даних відображається панель повідомлень. Щоб включити відключений уміст, клацніть Параметри, а потім виберіть параметри в діалоговому вікні, що з'явилося. Відключений уміст буде включено, і база даних відкриється заново з повним набором функціональних можливостей (рис. 3.42). У противному випадку при відкритті бази даних, створеної в більше ранньому форматі (файли з розширенням mdb або mde), у якої немає підпису й стани довіреної, додаток Access за замовчуванням відключає будь-який виконуваний уміст.

Режим відключення

Коли центр керування безпекою визначає, що база даних не має стану довіреної, Office Access 2007 відкриває її в режимі відключення — тобто відключає будь-який виконуваний уміст. Це справедливо як для баз даних, створених у новому форматі Office Access 2007, так і для файлів, створених у попередніх версіях Access ві-

дключені компоненти не будуть працювати. Office Access 2007 відключає наступні компоненти:

- Код VBA і всі посилання в ньому, а також усі небезпечні вираження.
- Небезпечні макрокоманди у всіх макросах. «Небезпечними» є команди, що дозволяють користувачеві змінювати базу даних або одержувати доступ до ресурсів поза базою даних. Однак макрокоманди, які Access відключає, іноді можуть уважатися «безпечними». Наприклад, при наявності довіри до творця бази даних, можна довіряти й усім небезпечним макрокомандам.

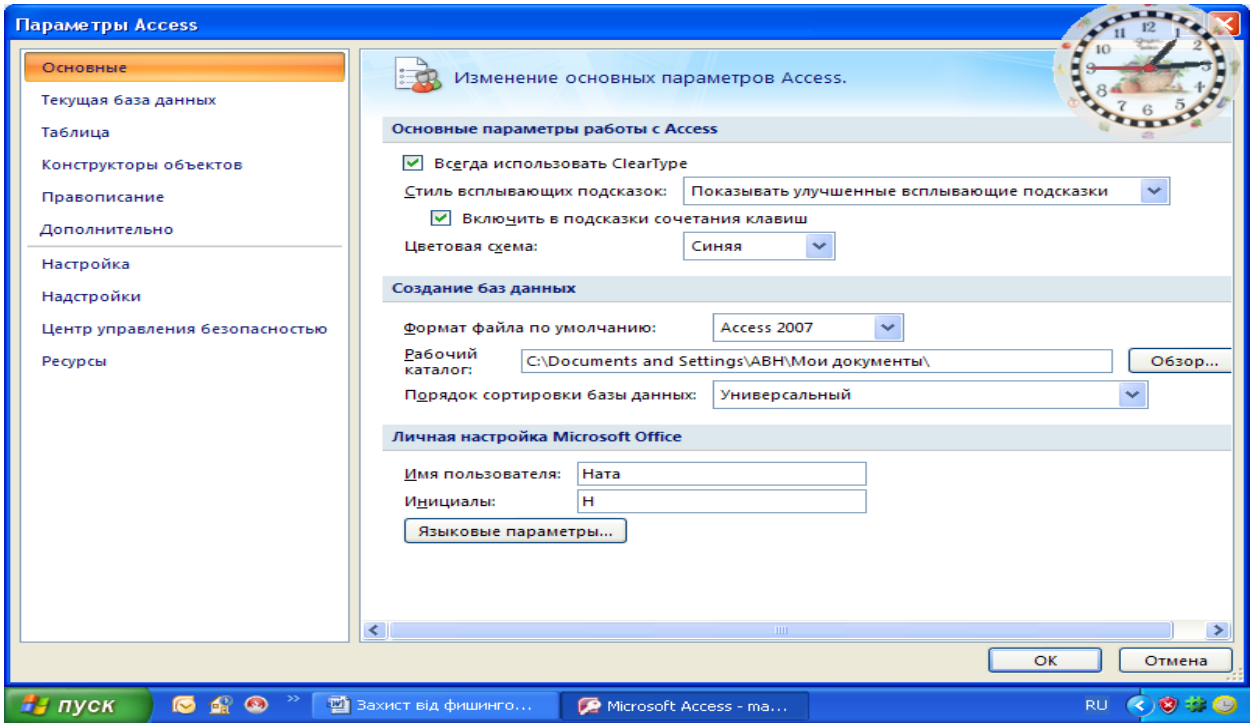


Рис. 3.42 Вікно відбору параметрів відкрита бази даних

Наступні типи запитів.

- Запити на зміну додають, обновляють або видаляють дані.
- Керуючі запити (DDL-Запити) Використовуються для створення або зміни проектів бази даних, таких як таблиці й процедури.
- SQL-Запити до сервера відправляють команди безпосередньо на сервер бази даних, що підтримує стандарт Open Database Connectivity (ODBC). Запити до сервера працюють із таблицями на сервері, минаючи ядро бази даних Access.

Елементи керування Active.

При відкритті бази даних може бути почата спроба завантаження надбудов — програм, що розширюють функціональні можливості Access для відкритої бази даних. Крім того, користувач може запустити майстер, що створює проекти в базі даних. При завантаженні надбудови або запуску майстри Access відправляє відомості про це в центр керування безпекою, що приймає додаткові рішення з довірі або відключає, або включає проект або дії. Якщо центр керування безпекою відключив базу даних, але користувач не згодний із таким рішенням, майже завжди можна скористатися панеллю повідомлень, щоб включити вміст. Виключенням із цього правила є надбудови. Якщо в центрі керування безпекою (в області Надбудови) установлений прапорець Вимагати підпис довіреного видавця для розширень додатків, додаток Access пропонує включити надбудову, але цей процес відбувається без використання панелі повідомлення.

Використання бази даних Office Access 2007 у надійному розташуванні

Якщо база даних Office Access 2007 розміщена в надійному розташуванні, при її відкритті працюють усі коди VBA, макроси й безпечні вираження. При цьому не виникає необхідність вирішувати питання довіри.

Процес використання бази даних Office Access 2007 у надійному розташуванні включає три основних етапи.

1. Використання центра керування безпекою для пошуку або створення надійного розташування.
2. Збереження, переміщення або копіювання бази даних Office Access 2007 у надійне розташування.
3. Відкриття й використання бази даних.

Описана нижче послідовність кроків пояснює, як знайти або створити надійне розташування, а потім додати туди базу даних.

Запуск центра керування безпекою

1. Клацніть значок Кнопка Microsoft Office , а потім виберіть команду Параметри Access.

ПРИМІТКА. Відкривати базу даних не потрібно.

Відкриється діалогове вікно Параметри Access.

2. Виберіть пункт Центр керування безпекою, і у групі Центр керування безпекою Microsoft Office Access натисніть кнопку Параметри центра керування безпекою (рис. 3.43).

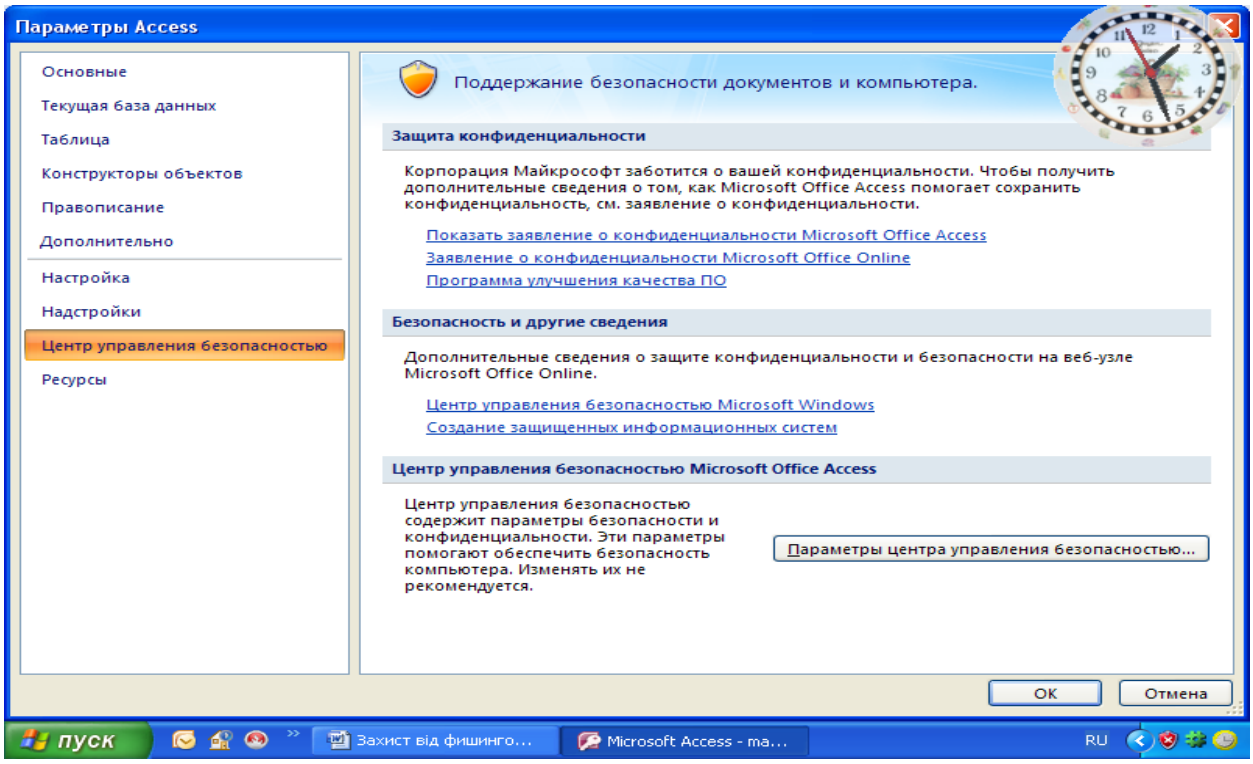


Рис. 3.43 Вікно управління безпекою

3. Виберіть Надійні розташування (рис. 3.44), а потім виконайте одну з наступних дій.

4. Укажіть шлях до одного або декількох надійних розташувань.
5. Створіть нове надійне розташування. Для цього натисніть кнопку Додати нове розташування, а потім укажіть значення параметрів у діалоговому вікні Надійне розташування Microsoft Office (рис. 3.45).

Розміщення бази даних у надійному розташуванні

- Для переміщення або копіювання файлу бази даних у надійне розташування можна використовувати будь-який спосіб. Наприклад, скористатися провідником Windows або відкрити файл в Access і зберегти його в надійному розташуванні.

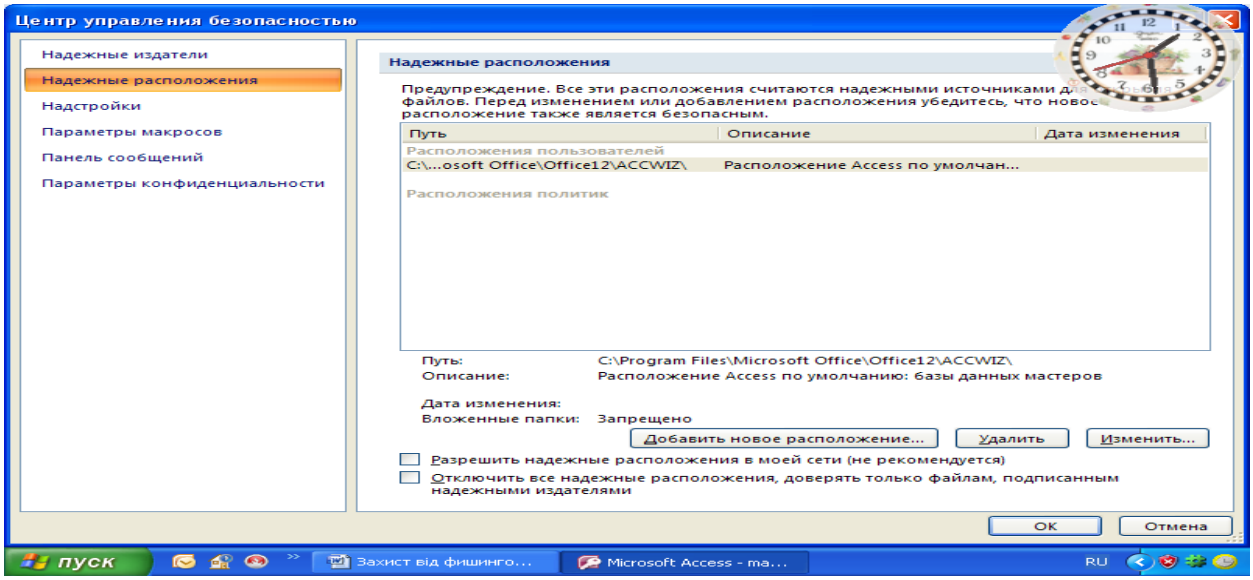


Рис. 3.44 Вікно вибору надійного розташування

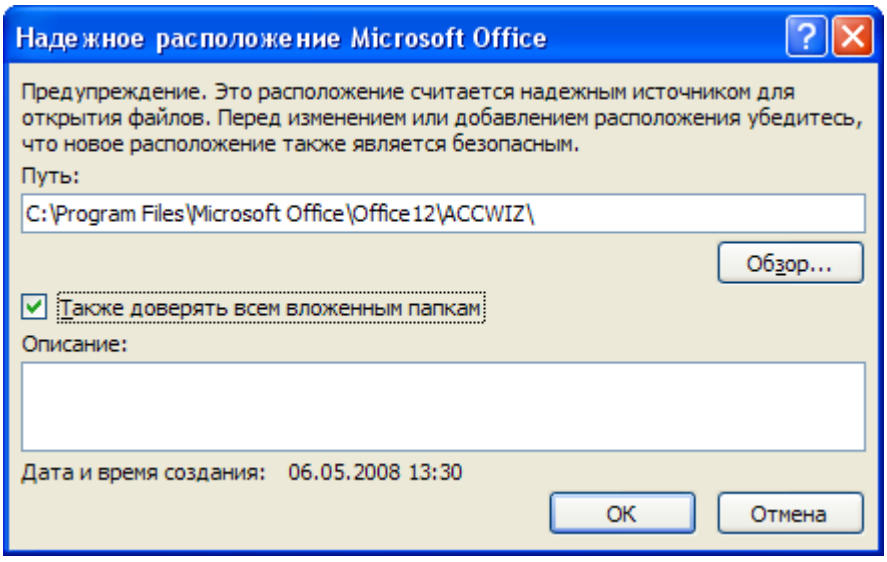


Рис. 3.45 Вікно вибору надійного розташування баз

Відкриття бази даних у надійному розташуванні

- Для відкриття файлу можна використовувати будь-який звичний спосіб. Наприклад, вибрати й потім двічі клацнути файл у провіднику Windows або, якщо

вже запущений Access, нажати кнопку Microsoft Office  для пошуку й відкриття файлу.

Упакування, підпис і поширення бази даних Office Access 2007

Office Access 2007 спрощує й прискорює процес додавання підпису й поширення бази даних. Після створення ACCDB- або ACCDE-Файлу можна впакувати його, застосувати до пакета цифровий підпис, а потім поширити підписаний пакет серед інших користувачів. Засіб підписування пакетів поміщає базу даних у файл розгортання Access (із розширенням accdc), підписує пакет, а потім поміщає пакет, підписаний кодом, у зазначене розташування. Користувачі потім можуть витягати базу даних із пакета й працювати безпосередньо в ній, а не у файлі пакета.

Ураховуйте наступні відомості при роботі.

- Упакування бази даних і підпис пакета є способами передачі довіри. Коли користувач одержує пакет, підпис підтверджує, що в базу даних не були внесені несанкціоновані зміни. При довірі до автора можна включити вміст.
- Новий засіб підписування пакетів застосовано тільки до баз даних у форматі Office Access 2007. До складу Office Access 2007 входять і колишні засоби для підписування й поширення баз даних, створених у більше ранньому форматі. Ці засоби не можна використовувати для підписування й поширення файлів, створених у новому форматі.
- У пакет можна включити тільки одну базу даних.
- У цьому процесі підпис кодом додається до всіх проектів бази даних, а не тільки до макросів або програмних модулів. Також відбувається стиск файлу пакета з метою зменшення часу на завантаження.
- Бази даних можна витягати з файлів пакета, розташованих на серверах Служби Windows SharePoint Services 3.0.

ПРИМІТКА. Щоб виконати дії, описані в цих етапах, необхідно мати щонайменше один доступний сертифікат безпеки. При відсутності сертифіката його можна створити за допомогою засобу SelfCert.

Створення підписаного пакета

1. Відкрийте базу даних, для якої потрібно створити пакет і підписати його.

2. Натисніть кнопку Microsoft Office , виберіть команду Опублікувати, а потім команду Впакувати й підписати (рис. 3.46).

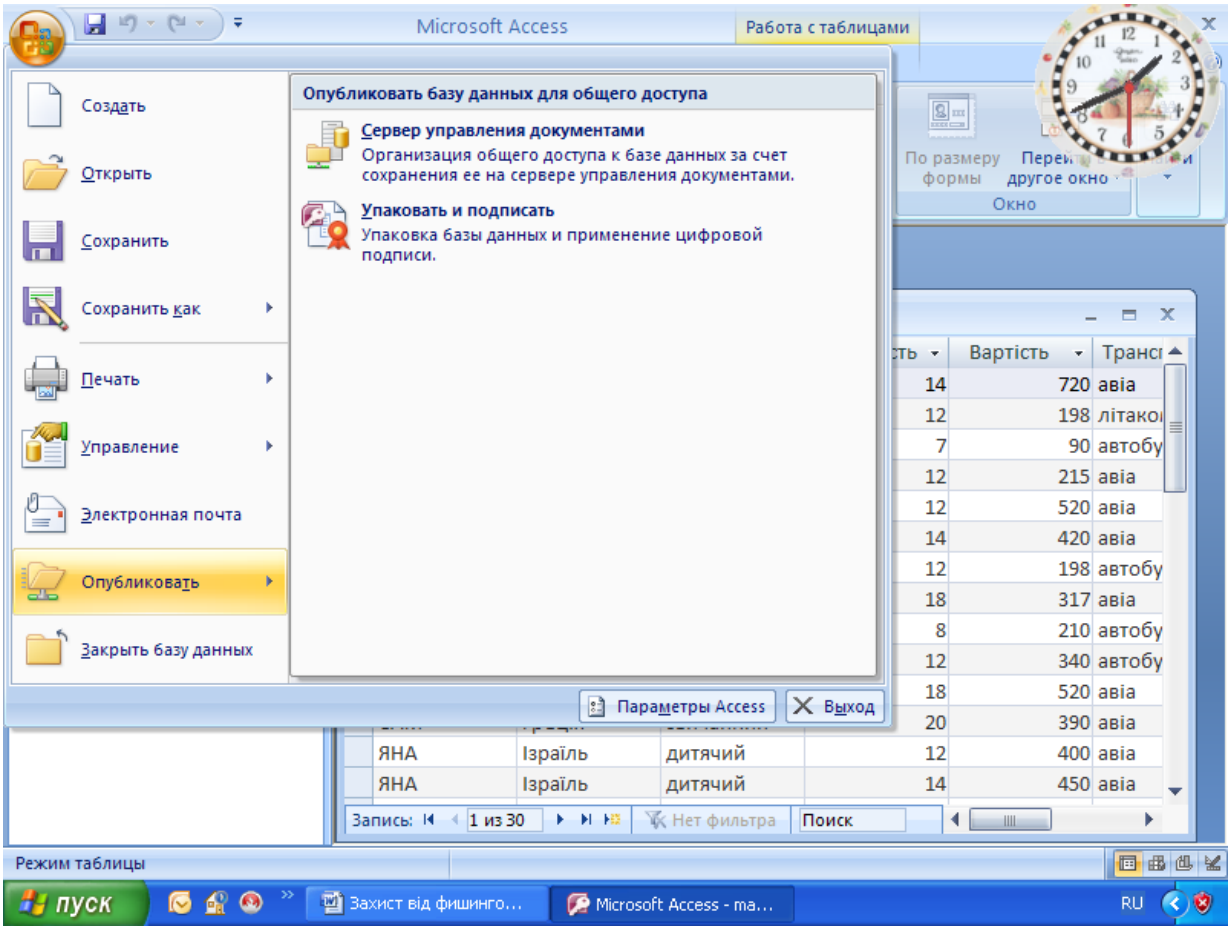


Рис. 3.46 Вікно Публікації

Відкриється діалогове вікно Вибір сертифіката.

3. Виберіть цифровий сертифікат, а потім натисніть кнопку ОК.

Відкриється діалогове вікно Створити підписаний пакет Microsoft Office Access.

4. У списку Зберегти у виберіть розташування для підписаного пакета бази даних.

5. У поле Ім'я файлу введіть ім'я для підписаного пакета, а потім натисніть кнопку Створити.

Access створить ACCDC-Файл і помістить його в обране розташування.

Витяг і використання підписаного пакета

1. Клацніть значок Кнопка Microsoft Office , а потім виберіть команду Відкрити.

Відкриється діалогове вікно Відкрити.

2. У списку Тип файлів виберіть варіант Підписані пакети Microsoft Office Access (*.accdc).

3. Скористайтеся списком Папка, щоб знайти папку, що містить ACCDC-Файл, виділіть цей файл і натисніть кнопку Відкрити.

4. Виконайте одну з наступних дій:

- Якщо обрано параметр довіри до цифрового сертифіката, застосованому до розгорнутого пакета, з'явиться діалогове вікно Витягти базу даних в. Перейдіть до наступного етапу.
- Якщо параметр довіри до цифрового сертифіката ще не обраний, з'явиться попередження (рис. 3.47).

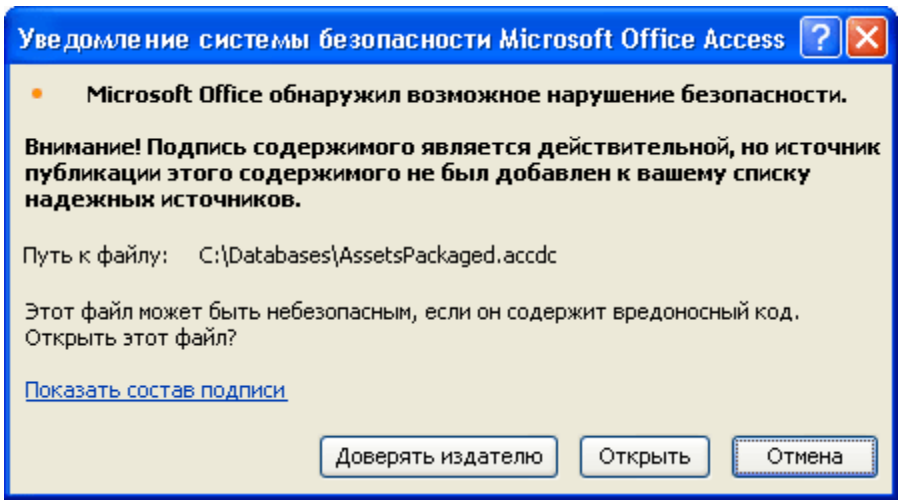


Рис. 3.47 Вікно попередження

Якщо ви довіряєте базі даних, натисніть кнопку Відкрити. Якщо ви довіряєте всі сертифікатам цього постачальника, натисніть кнопку Довіряти всьому від видавця. Відкриється діалогове вікно Витягти базу даних в.

5. У списку Зберегти в можна вибрати розташування для бази даних, а в поле Ім'я файлу - увести для неї інше ім'я.

6. Натисніть кнопку ОК.

6. Включення відключеного вмісту при відкритті бази даних

За замовчуванням Access відключає весь виконуваний уміст у базі даних, якщо вона не має стану довіреної або не розміщена в надійному розташуванні. При відкритті такої бази даних Access відключає цей уміст, і відображає панель повідомлень (рис. 3.48).

Рис. 3.48 Вікно панелі повідомлень

На відміну від Access 2003 в Office Access 2007 при відкритті бази даних не відображається набір модальних діалогових вікон (це діалогові вікна, у яких необхідно прийняти яке-небудь рішення для того, щоб продовжити роботу). Однак при необхідності можна додати ключ реєстру, щоб в Office Access 2007 відображалися колишні модальні діалогові вікна. Незалежно від поводження Access при відкритті бази даних можна надати дозвіл виконуваному вмісту у файлі в тому випадку, якщо ця база даних отримана від надійного видавця.

Надання базі даних стану довіри

1. На панелі повідомлень натисніть кнопку Параметри.

Відкриється діалогове вікно Параметри безпеки Microsoft Office.

2. Виберіть варіант Включити цей уміст, а потім натисніть кнопку ДОК.

Якщо панель повідомлень не відображається

- На вкладці Робота з базами даних у групі Відображення виберіть параметр Панель повідомлень.

ВАЖЛИВО. При виконанні цих дій Access включає весь відключений уміст, у тому числі потенційно небезпечний код, доти, поки база даних не буде закрита. Якщо небезпечний код ушкодить дані або комп'ютер, додаток Access не зможе скасувати його дії.

Закриття бази даних

- Клацніть значок Кнопка Microsoft Office  , а потім виберіть команду Закрити базу даних.

При повторному відкритті бази даних знову відображається панель повідомлень. У цьому випадку можна закрити панель повідомлень, залишивши вміст у відключеному стані або сховавши панель. У кожному разі результат буде один — відключений уміст залишиться відключеним.

Відключення вмісту

1. На панелі повідомлень натисніть кнопку Параметри.

Відкриється діалогове вікно Параметри безпеки Microsoft Office.

2. Виберіть варіант Установити захист від невідомого вмісту (рекомендується) і натисніть кнопку ОК.

Access відключить усі потенційно небезпечні компоненти.

Приховання панелі повідомлень

- Не ухвалюючи рішення щодо довірі, натисніть кнопку Закрити (X) у верхньому куті панелі повідомлень.
- Панель повідомлень закриється.

Відображення панелі повідомлень

- На вкладці Робота з базами даних у групі Відображення виберіть пункт Панель повідомлень. Щоб відобразити панель повідомлень, можна також закрити й знову відкрити базу даних.

7. Додавання ключа реєстру для відображення модальних діалогових вікон

Увага! Невірна зміна параметрів реєстру може привести до істотного ушкодження операційної системи з необхідністю її переустанови. Корпорація Майкрософт не гарантує можливість дозволу проблем, що виникають через зміну реєстру. Перед зміною реєстру виконайте архівацію всіх важливих даних.

1. Натисніть кнопку Пуск і виберіть команду Виконати.
2. У поле Відкрити введіть regedit, а потім натисніть клавішу УВЕДЕННЯ.

Запуститься редактор реєстру.

3. Розгорніть папку HKEY_CURRENT_USER (рис. 3.49)і вкажіть наступний розділ реєстру:

Software\Microsoft\Office\12.0\Access\Security

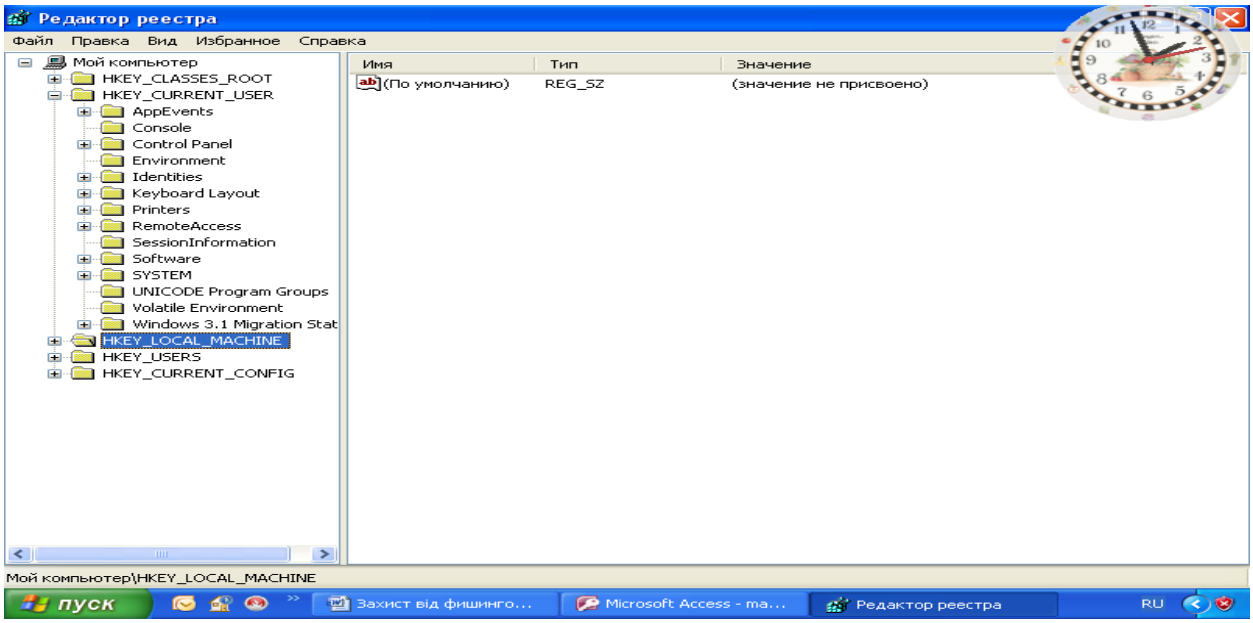


Рис. 3.49 Вікно реєстру

4. У правій області редактора реєстру клацніть правою кнопкою миші порожнє місце, виберіть команду Створити, а потім виберіть варіант Параметр DWORD. З'явиться новий порожній параметр типу DWORD.

5. Уведіть наступне ім'я параметра: ModalTrustDecisionOnly.

6. Двічі клацніть новий параметр.

Відкриється діалогове вікно Зміна параметра DWORD.

7. У поле Значення поміняйте значення 0 на 1, а потім натисніть кнопку ОК.

8. Закрийте редактор реєстру.

Тепер при відкритті бази даних, що включає небезпечний уміст, замість панелі повідомлень буде відображатися ряд діалогових вікон. Щоб повернутися до вихідного варіанта, повторіть ці дії, і поміняйте значення 1 на 0.

8. Використання пароля для шифрування бази даних Office Access 2007

Засіб шифрування в Office Access 2007 являє собою два поєднаних і поліпшених засоби колишніх версій — кодування й паролів баз даних. При використанні пароля для шифрування бази даних усі дані не читаються в інших програмних засобах,

і для того щоб використовувати цю базу даних, користувачі повинні вводити пароль. При шифруванні в Office Access 2007 використовується більше стійкий алгоритм, ніж у попередніх версіях Access.

Шифрування з використанням пароля бази даних

Відкрийте в монопольному режимі базу даних, що потрібно зашифрувати.

1. Клацніть значок Кнопка Microsoft Office , а потім виберіть команду Відкрити.
2. У діалоговому вікні відкрити знайдіть файл, якому потрібно відкрити, і виділіть його.
3. Виберіть команду Монопольно (рис. 3.50).
4. На вкладці Робота з базами даних клацніть Зашифрувати за допомогою пароля.

Відкриється діалогове вікно Завдання пароля бази даних (рис. 3.51).

5. Уведіть пароль у поле Пароль, а потім повторіть його в поле Перевірити.

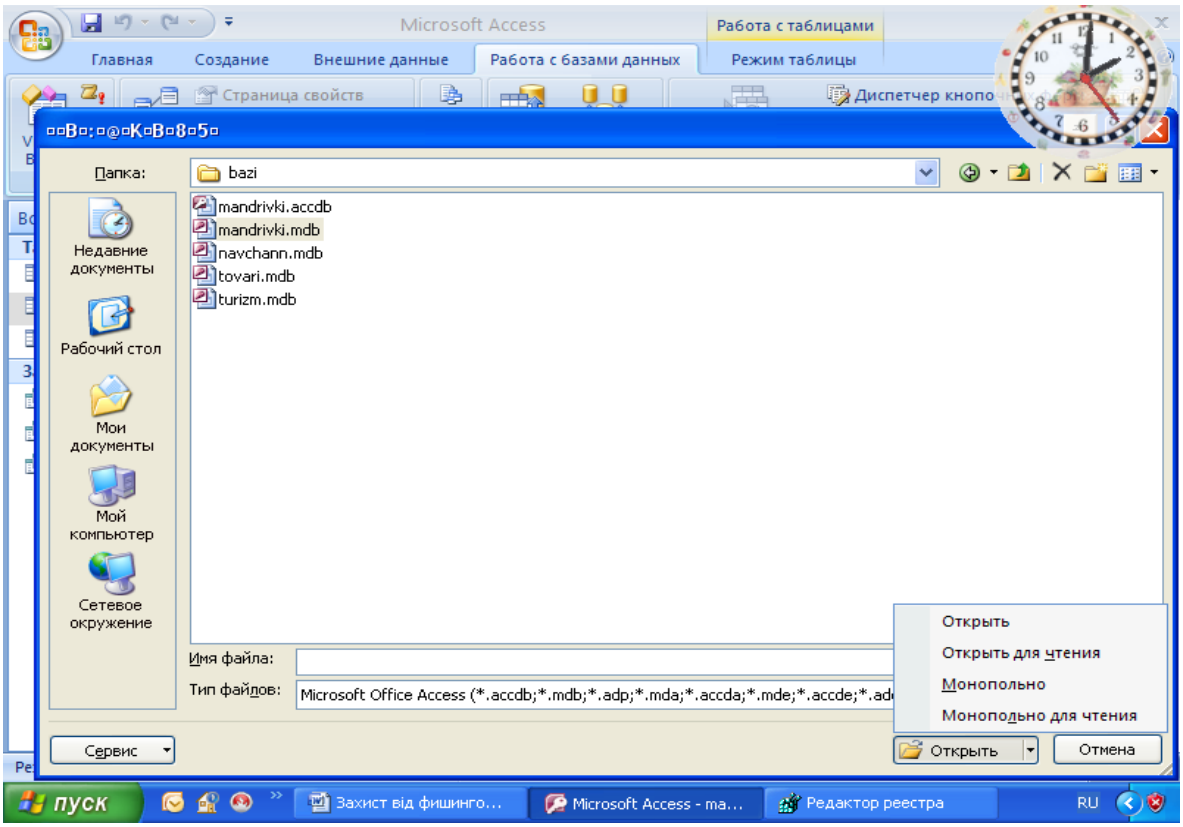
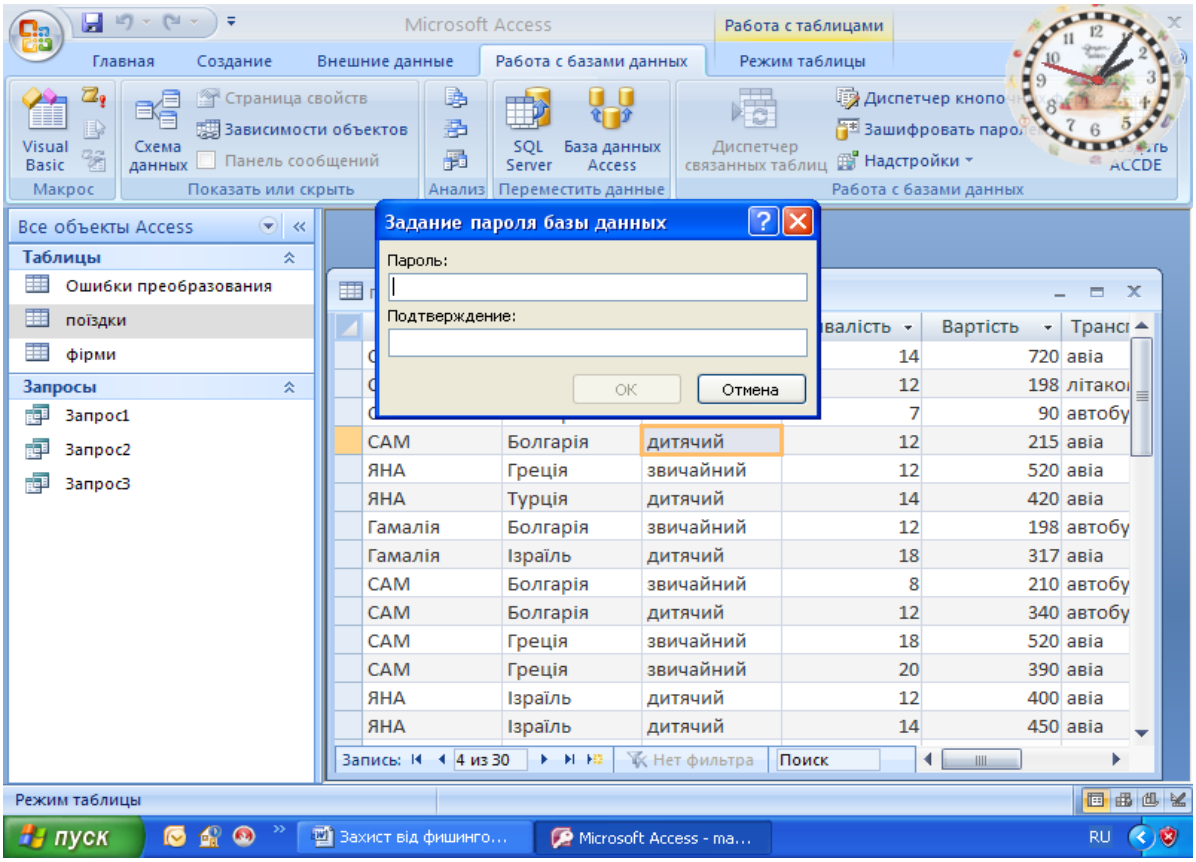


Рис. 3.50 Відкриття бази даних у монопольному режимі



САМ	Болгарія	дитячий	12	215	авіа
ЯНА	Греція	звичайний	12	520	авіа
ЯНА	Турція	дитячий	14	420	авіа
Гамалія	Болгарія	звичайний	12	198	автобу
Гамалія	Ізраїль	дитячий	18	317	авіа
САМ	Болгарія	звичайний	8	210	автобу
САМ	Болгарія	дитячий	12	340	автобу
САМ	Греція	звичайний	18	520	авіа
САМ	Греція	звичайний	20	390	авіа
ЯНА	Ізраїль	дитячий	12	400	авіа
ЯНА	Ізраїль	дитячий	14	450	авіа

Рис. 3.51 Вікно введення пароля

ПРИМІТКА. Використовуйте надійні паролі, що представляють собою сполучення прописних і малих літер, цифр і символів. Паролі, що не містять набір таких елементів, є ненадійними. Надійний пароль: Y6dh!et5. Ненадійний пароль: House27. Паролі повинні складатися не менш чим з 8 символів. Рекомендується використовувати фразу-пароль, що складається з 14 або більше символів..

2. Натисніть кнопку ОК.

Розшифрування й відкриття бази даних

1. Відкрийте зашифровану базу даних точно так само, як, звичайно, відкривається будь-яка інша.

Відкриється діалогове вікно Необхідно ввести пароль.

2. Уведіть пароль у поле Введіть пароль бази даних і натисніть кнопку ОК.

Видалення пароля

1. На вкладці Робота з базами даних клацніть Дешифрувати базу даних.

Відкриється діалогове вікно Видалити пароль бази даних.

2. Уведіть пароль у поле Пароль і натисніть кнопку ОК.

9. Про роботу системи безпеки з базами даних із попередніх версій Access, відкритих в Office Access 2007

При відкритті в Office Access 2007 бази даних, створеної в одній із попередніх версій Access, усі засоби безпеки, застосовані до неї, будуть продовжувати працювати. Наприклад, захист на рівні користувача.

За замовчуванням додаток Access відкриває всі старі бази даних, що не мають стану довірених, у монопольному режимі й зберігає їхній стан. Можна включати відключений уміст щораз при відкритті такої бази даних, або застосувати цифровий підпис, скориставшись сертифікатом від надійного видавця, або помістити базу даних у надійне розташування.

Для баз даних із більше ранніх версій, ніж Office Access 2007, підпис кодом - це процес застосування цифрового підпису до компонентів бази даних. Цифровий підпис являє собою зашифровану електронну печатку для завірення. Вона підтверджує, що макроси, програмні модулі й інші виконувані компоненти бази даних створені особою, що додала підпис, і ніхто іншой не змінював їх після підпису.

Щоб застосувати підпис до бази даних, насамперед необхідно мати цифровий сертифікат. Якщо бази даних створюються для комерційного поширення, потрібно одержати сертифікат у комерційному центрі сертифікації, наприклад, VeriSign, Inc. або GTE. Центр сертифікації наводить довідки про виготовлювача бази даних, щоб упевнитися в його надійності.

Якщо базу даних планується використовувати в особистих цілях або в невеликій робочій групі, можна скористатися передбаченим в Microsoft Office Professional 2007 засобом створення сертифікатів із власним підписом. У наступних розділах пояснюється, як установити й використовувати засіб, названий SelfCert.exe, для створення сертифіката із власним підписом. Цей сертифікат варто додати в список надійних джерел, а потім підписати базу даних.

Створення сертифіката із власним підписом

1. Натисніть кнопку Пуск, виділіть пункт Усі програми, потім - пункти Microsoft Office і Засоби Microsoft Office, і виберіть команду Цифрове посвідчення

для проектів VBA, або перейдіть до папки, що містить програмні файли Office Professional 2007. Папкою за замовчуванням є папка Диск:\Program Files\Microsoft Office\Office12. У ній знайдіть і двічі клацніть файл SelfCert.exe.

Відкриється діалогове вікно Створення цифрового сертифіката (рис. 2.52)

2. У поле Ім'я вашого сертифіката введіть ім'я для нового сертифіката.

3. Два рази натисніть кнопку ОК (рис. 3.53).

Підпис кодом бази даних

1. Відкрийте базу даних, до якої потрібно додати підпис.

2. На вкладці Засобу бази даних у групі Макрос виберіть команду Visual Basic, щоб запустити редактор Visual Basic (рис. 2.54)

Натисніть клавіші ALT+F11.

3. У вікні проекту виберіть базу даних, макрос або модуль, до яких потрібно додати підпис.

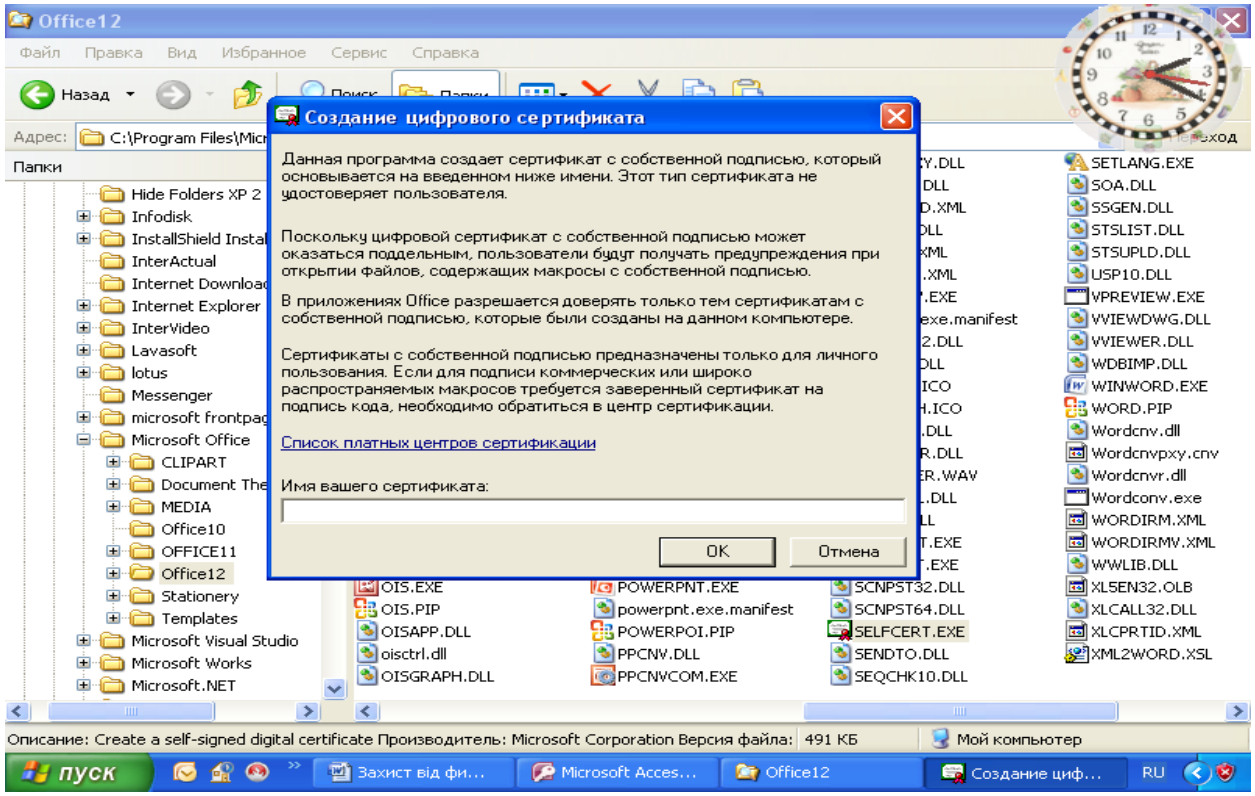


Рис. 3.52 Вікно створення цифрового сертифіката

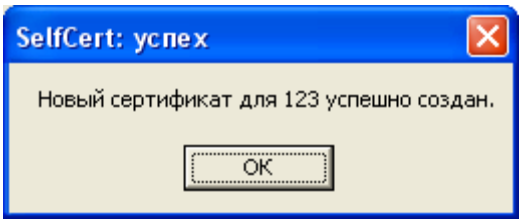


Рис. 3.53 Вікно повідомлення

4. У меню Сервіс виберіть команду Цифрові підписи.

Відкриється діалогове вікно Цифрові підписи (рис. 3.55).

5. Натисніть кнопку Вибір, щоб вибрати сертифікат.

Відкриється діалогове вікно Вибір сертифіката (рис. 3.56)

6. Виберіть необхідний сертифікат.

Якщо виконані дії, описані в попередньому розділі, то це сертифікат, створений за допомогою засобу SelfCert.

7. Щоб закрити діалогове вікно Сертифікат, натисніть кнопку ОК, а потім натисніть кнопку ОК ще раз, щоб закрити діалогове вікно Цифровий підпис.

ПРИМІТКА. Варто пам'ятати, що ці дії застосовні тільки для баз даних, створених у попередніх версіях Access, при їхньому використанні в Office Access 2007.

Установка засобу SelfCert.exe

1. Запустіть настановний диск Office Professional 2007 або інший засіб установки.

2. У вікні установки клацніть Додати, або видалити компоненти, а потім натисніть кнопку продовжити.

ПРИМІТКА. При роботі в середовищі, де Office Professional 2007 установлюється на окремі комп'ютери не з диска, а адміністраторами, виконайте наступні дії.

1. В Microsoft Windows натисніть кнопку Пуск, а потім виберіть команду Панель керування.

2. Двічі клацніть компонент Установка й видалення програм.

3. і натисніть кнопку Змінити. Виділіть Випуск 2007 системи Microsoft Office

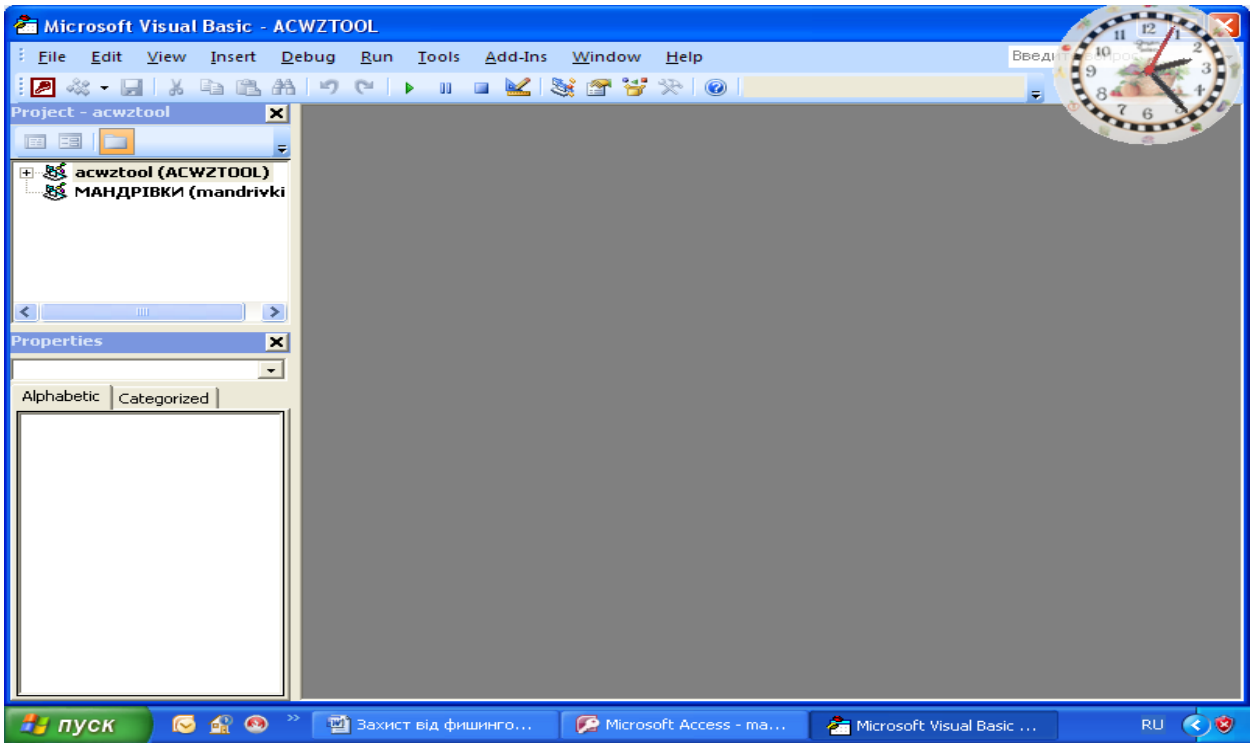


Рис. 3.54 Вікно редактора Visual Basic

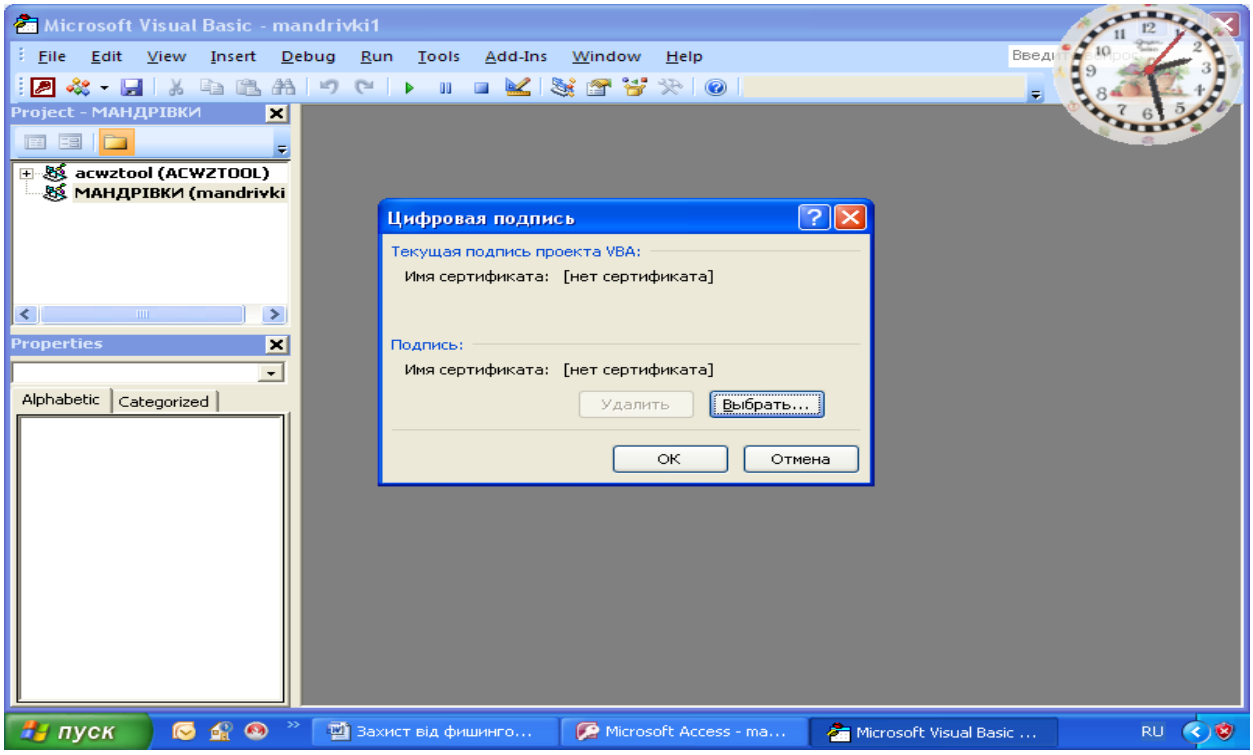


Рис. 3.55 Цифрові підписи

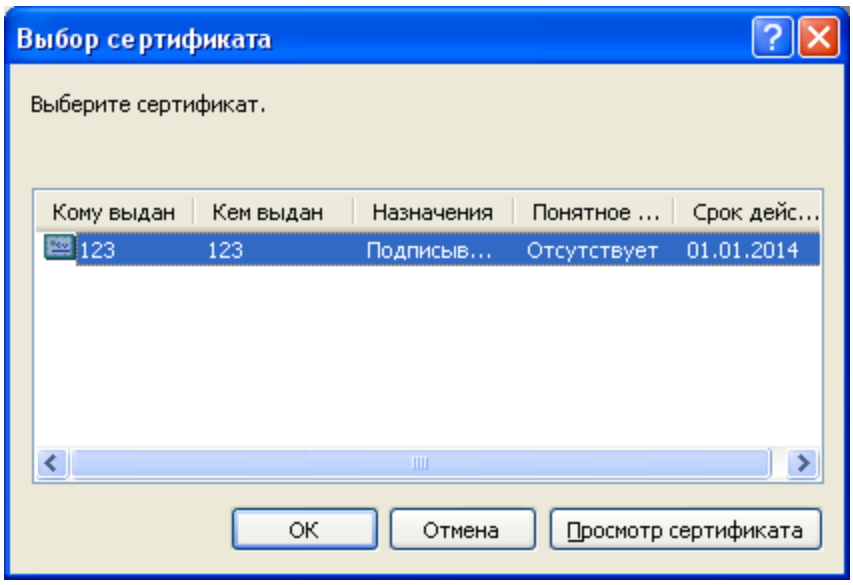


Рис. 3.56 Вибір сертифіката

Почнеться процес установки.

4. Установіть перемикач у положення Додати, або видалити компоненти й натисніть кнопку продовжити.

5. Виконайте наступні дії.

3. Розгорніть вузли Microsoft Office і Загальні ресурси Office, клацнувши плюс (+) поруч із ними.

4. Клацніть Цифрове посвідчення для проектів VBA.

5. Клацніть Запускати з мого комп'ютера.

6. Натисніть кнопку продовжити, щоб установити компонент.

7. Після завершення установки натисніть кнопку Закрити, і поверніться до першої послідовності дій у цьому розділі.

Зміна параметра реєстру

ВАЖЛИВО. Виконання цих кроків дозволить запускати небезпечні вираження у всіх екземплярах Access всіх користувачів даного комп'ютера.

1. Натисніть кнопку Пуск і виберіть команду Виконати.

2. У поле Відкрити введіть regedit, а потім натисніть клавішу УВЕДЕННЯ.

Запуститься редактор реєстру.

3. Розгорніть папку HKEY_LOCAL_MACHINE і вкажіть наступний розділ реєстру:

\Software\Microsoft\Office\12.0\Access Connectivity Engine\Engines

4. У правій області редактора реєстру двічі клацніть параметр SandboxMode.

Відкриється діалогове вікно Зміна параметра DWORD.

5. У поле Значення поміняйте значення 3 на 2 і натисніть кнопку ОК.

6. Закрийте редактор реєстру.

Це важливо. Варто пам'ятати, що, якщо база даних не має стану довіреної, Access відключає будь-які небезпечні вираження незалежно від того, чи змінений даний параметр реєстру.

Пошук паролів у документах Microsoft Office за допомогою спеціальних програм.

Для пошуку паролів методом перебору або з використанням словників розроблене спеціальне програмне забезпечення. Наведемо деякі приклади даного типу програмного забезпечення:

Advanced Office 97 Password Recovery - Дозволяє знаходити всі паролі Word 97/2000, Excel 97/2000, Access 97/2000 (крім паролів користувачів/груп).

Advanced Office 95 Password Recovery.

Дозволяє знаходити всі паролі документів Office 95 (Word, Excel і Access).

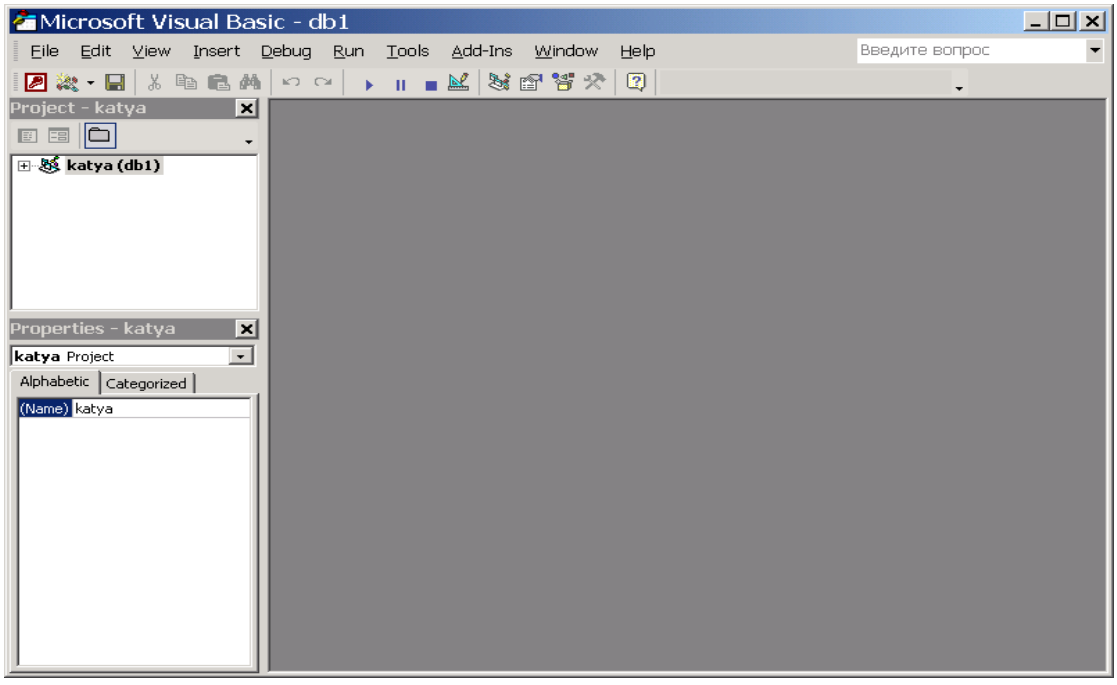


Рис.3.57 Вікно редактора Visual Basic

Advanced VBA Password Recovery.

Дозволяє знаходити всі паролі на VBA-макроси Word/Excel 97. Для макросів Office 2000 є комерційна версія програми.

Advanced Outlook Password Recovery. Паролі MS Outlook.

Для визначення паролю документа (може включати до 15 символів Microsoft Word, Excel, в тому числі, маленькі та великі літери латинського та національного алфавітів, спеціальні символи !@#$%^&*()_+-=<>,./?[]{}~:;`'|"\ та до 13 символів Microsoft Access) Microsoft Office необхідно провести запуск програми Advanced Office 97 Password Recovery використавши пусковий файл ao97pr.exe, після чого на екрані з'явиться діалогове вікно (рис. 3.58) в якому необхідно вибрати захищений файл та підібрати необхідні параметри пошуку і подати команду почати перебір із підменю пароль.

Можливі три режими переборів паролів:

Прямий перебір. Цей режим включає використання для порівняння готових паролів, які знаходяться в додатковому словнику, а також режими використання визначених символів, масок і т.п.

Перебір за маскою. Використовується в тому випадку коли відомий один або декілька символів паролю. Цей режим включає використання для порівняння паролів символів масок у якості яких використовується символ „?". В тих випадках, коли відомо, що в самому паролі мається символ „?" в масці необхідно змінити його на символ „*" , або „#".

Атака за словником. Цей режим включає використання для порівняння готових паролів, які знаходяться в додатковому словнику. Використовується в тому випадку коли необхідно використати нейменше часу на знаходження паролю, але не завжди приводить до необхідного результату.

Використання опції **Почати з** може бути корисним, коли відомі деякі символи паролю.

Після успішного опрацювання паролю програмою буде виведене діалогове віконце (рис.3.59) з вказанням знайденого паролю та деякими параметрами пошуку.

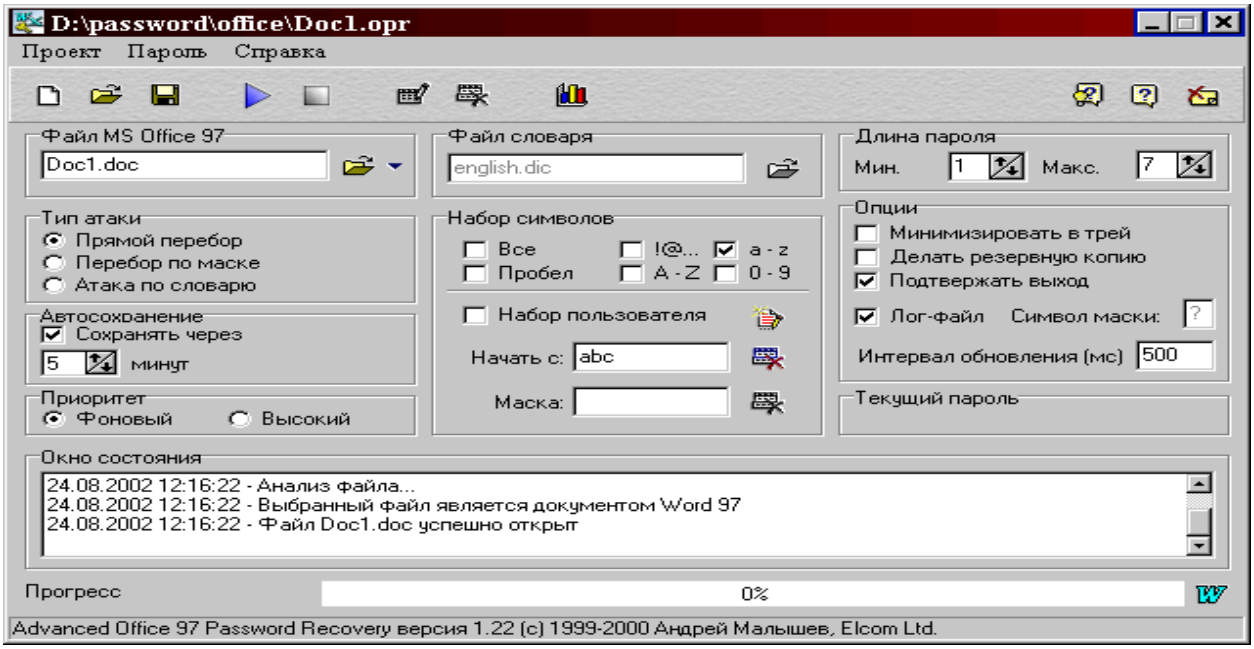


Рис. 3.58. Діалогове вікно програми Advanced Office 97 Password Recovery

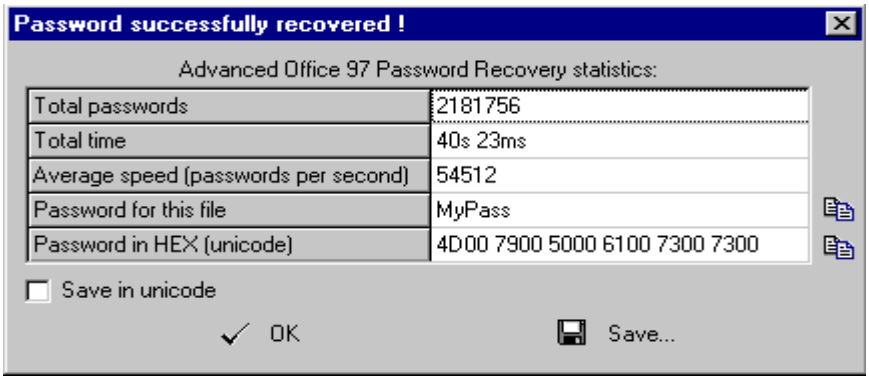


Рис.3.59. Діалогове вікно результатів пошуку

Час пошуку залежить від параметрів, приклад яких наведено в табл.3.4

Табл.3.4

Залежність часу пошуку паролів від деяких параметрів паролю.

Набір символів	**Довжина**	**Кількість комбінацій**	**Час пошуку**
Усі, що друкуються	**1..5**	**7,820,126,720**	**2 годин**
Цифри, великі/маленькі бу-	**6**	**62,523,502,592**	**17 годин**

кви пробіли			
Цифри, маленькі букви пробіли	**7**	**94,931,877,888**	**26 годин**

Контрольні питання

1. В якому файлі зберігається інформація про користувачів?
2. Використання бази даних Office Access 2007 у надійному розташуванні.
3. Вимоги до паролів документів Microsoft Office.
4. Вимоги до паролів у програмі MS Access.
5. Відключення оповіщень системи безпеки для веб-вузлів шляхом їхньої позначки як надійних вузлів в Internet Explorer.
6. Де зберігаються окремі типи паролів у програмі MS Access?
7. Дії із системою безпеки Microsoft Office.
8. Додавання захисту в форму документу Microsoft Word.
9. Дозвіл вибіркового виправлення захищеного документа.
10. Елементи керування Active в програмі MS Access.
11. За яким стандартом шифрується пароль у заголовку файлу?
12. Залежність часу пошуку паролю від його параметрів.
13. Запуск центра керування безпекою Access 2007.
14. Захист від фішингових схем в Microsoft Office.
15. Захист елементів книги та листів в Microsoft Excel.
16. Захист інформації у Microsoft Excel.
17. Захист конфіденційності даної книги в Microsoft Excel.
18. Зміна параметра реєстру.
19. Зміна пароля в Microsoft Word.
20. Маски пошуку паролів.
21. Надання базі даних стану довіри.
22. Одержання цифрового сертифіката для постановки підпису.
23. Основні відомості про безпеку макросів.

24. Перегляд параметрів конфіденційності.

25.Підпис кодом бази даних.

26.Порядок захисту сторінки доступу.

27.Порядок приховування, відображення елементів баз даних.

28.Порядок установлення, зняття паролю програми Microsoft Visual Basic для додатків.

29.Порядок установлення, зняття паролю баз даних.

30.Порядок установлення, зняття паролю облікового запису користувача.

31.Послідовність встановлення захисту на книгу в Microsoft Excel.

32.Послідовність встановлення захисту на комірки в Microsoft Excel.

33.Послідовність встановлення захисту на листи в Microsoft Excel.

34.Послідовність встановлення захисту на файл в у Microsoft Word.

35.Послідовність встановлення захисту на файл при його відкритті.

36.Послідовність встановлення захисту на файл при його зміні.

37.Послідовність встановлення захисту на файл цифровим підписом.

38.Послідовність зняття захисту з тексту в Microsoft Word.

39.Послідовність зняття захисту на книгу в Microsoft Excel.

40. Приєднання сертифіката.

41.Приклади й характеристики фішингових схем.

42.Режими підбору паролів та їх характеристики.

43.Складові діалогово віконця програми Advanced Office 97 Password Recovery.

44.Стандартні ознаки фішингової схеми.

45.Створення підписаного пакета Access 2007.

46.Створення сертифіката із власним підписом в Access 2007.

47.Структура системи безпеки Office Access 2007

48.Типи захисту тексту в у Microsoft Word.

49. Цифровий підпис макросів.

50.Шифрування з використанням пароля бази даних.

51.Як приховати формули в комірках у Microsoft Excel?

52.Які програмні продукти застосовуються для пошуку паролів?

53.Які типи паролів використовуються в програмі MS Access?

Розділ 4.
ШИФРУВАННЯ ДАНИХ.

ВСТУП.

Щоб зробити інформацію недоступною для супротивника, використовується сукупність методів перетворення даних, звана криптографією. Системи шифрування можуть здійснювати криптографічні перетворення даних на рівні файлів або на рівні дисків. До програм першого типу можна віднести архіватори типу ARJ і RAR і т. д., які дозволяють використовувати криптографічні методи для захисту архівних файлів. Прикладом систем другого типу може служити програма шифрування Diskreet, що входить до складу популярного програмного пакету Norton Utilities.

Проблемою захисту інформації шляхом її перетворення займається криптология (kryptos - таємний, logos - наука). Кріптология розділяється на два напрями - криптографію і криптоаналіз. Цілі цих напрямів прямо протилежні.

Криптографія займається пошуком і дослідженням математичних методів перетворення інформації. Сфера інтересів криптоаналізу - дослідження можливості розшифровування інформації без знання ключів.

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, проте їй властиві і переваги: висока продуктивність, простота, захищеність і т. д. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

При оцінці ефективності шифру зазвичай керуються правилом голландця Огюста Керкхоффа (1835 - 1903 р.р.), згідно якому стійкість шифру визначається тільки секретністю ключа, тобто криптоаналітику відомі всі деталі процесу (алгоритму) шифрування і дешифрування, але невідомо, який ключ використаний для шифрування даного тексту. Криптостойкостью називається характеристика шифру, визначальна його стійкість до дешифрування без знання ключа (тобто стійкість до криптоаналізу). Є декілька показників криптостойкости, серед яких: кількість всіх можливих ключів і середній час, необхідний для криптоаналізу.

Одним з найперших шифрувальних пристосувань була скитала (за іншими джерелами – сцитала), яка застосовувалася в V столітті до н.е. під час війни Спарти проти Афін. Скитала - це циліндр, на який, виток до витка, намотувалася вузька папірусова стрічка (без прогалин і нахлестів). Потім на цій стрічці уздовж осі циліндра

(стовпцями) записувався необхідний для передачі текст. Стрічка змотувалася з циліндра і відправлялася одержувачеві. Отримавши таке повідомлення, одержувач намотував стрічку на циліндр такого ж діаметру, як і діаметр скитали відправника. В результаті можна було прочитати зашифроване повідомлення.

Арістотелю належить ідея дешифрування такого шифру. Він запропонував виготовити довгий конус і, починаючи з основи, обгорнути його стрічкою із шифрованим повідомленням, поступово зсовувати її до вершини. На якійсь ділянці конуса розпочинатимуть бути видимим ділянки читаного тексту. Так визначається секретний розмір циліндра.

Коди з'явилися в глибокій старовині у вигляді криптограм (по-грецьки - тайнопис). Св'ященні іудейські тексти шифрувалися методом заміни. Замість першої літери алфавіту писалася остання літера, замість другої - передостання і так далі. Шифр Цезаря реалізується заміною кожної літери в повідомленні іншою літерою цього ж алфавіту, віддаленою від неї в алфавіті на фіксоване число літер. У Стародавній Греції (II ст. до н.е.) був відомий шифр, званий "квадрат Полібія". Шифрувальна таблиця була квадратом із п'ятьма стовпцями і п'ятьма рядками, які нумерувалися цифрами від 1 до 5. У кожну клітину такого квадрата записувалася одна літера. В результаті кожній літері відповідала пара чисел, і шифрування зводилося до заміни літери парою чисел.

Класифікація криптоалгоритмів

Залежно від наявності або відсутності ключа алгоритми для кодування, діляться на тайнопис і криптографію. Залежно від відповідності ключів шифрування і дешифрування – на симетричні й асиметричні. Залежно від типу використовуваних перетворень – на підстановочні й перестановочні. Залежно від розміру шифрованого блоку – на потокові й блокові шифри.

Криптографія спільно з криптоаналізом (метою якого є протистояння методам криптографії) складають комплексну науку – криптологію.

Необхідно відзначити, що в літературі з даного предмету зустрічаються різні вживання основних термінів, таких як "криптографія", "тайнопис" і деяких інших.

Більш того, і у класифікації криптоалгоритмів можна зустріти різні думки. Відносно криптоалгоритмів існує декілька схем класифікації, кожна з яких заснована на групі характерних ознак. Таким чином, один і той же алгоритм "проходить" відразу за декількома схемами, опиняючись в кожній з них.

Основною схемою класифікації всіх криптоалгоритмів є наступна:

Тайнопис.

Відправник і одержувач проводять над повідомленням перетворення, відомі тільки їм двом. Стороннім особам невідомий сам алгоритм шифрування. Деякі фахівці вважають, що тайнопис не є криптографією взагалі.

Криптографія з ключем.

Алгоритм дії з передавання даних відомий усім стороннім особам, але він залежить від деякого параметра – "ключа", яким володіють тільки відправник і одержувач.

Симетричні криптоалгоритми.

Для зашифровування і розшифровування повідомлення використовується один і той же блок інформації (ключ).

Асиметричні криптоалгоритми.

Алгоритм такий, в якому для зашифровування повідомлення використовується один ("відкритий") ключ, відомий усім охочим, а для розшифровування – інший "закритий"), що існує тільки у одержувача.

Весь подальший матеріал буде присвячений криптографії з ключем, оскільки більшість фахівців саме за відношенням до цих криптоалгоритмів використовують термін криптографія. Так, наприклад, будь-який криптоалгоритм з ключем можна перетворити на тайнопис, просто "зашивши" в початковому коді програми деякий фіксований ключ. Зворотне ж перетворення практично неможливе.

Залежно від характеру дій, які робляться над даними, алгоритми підрозділяються на:

Перестановочні.

Блоки інформації (байти, біти) не змінюються самі по собі, але змінюється їх порядок проходження, що робить інформацію недоступною сторонньому спостерігачу.

Підстановочні.

Самі блоки інформації змінюються за законами криптоалгоритма. Переважна більшість сучасних алгоритмів належать цій групі.

Примітка:

Будь-які криптографічні перетворення не збільшують об'єм інформації, а лише змінюють її представлення. Тому, якщо програма шифрування значно збільшує об'єм вихідного файлу, то в її основі лежить неоптимальний, а можливо й узагалі некоректний криптоалгоритм. Зменшення об'єму закодованого файлу можливо тільки за наявності вбудованого алгоритму архівації у криптосистемі і за умови можливості стискання інформації.

Залежно від розміру блоку інформації криптоалгоритми діляться на:

Потокові шифри.

Одиницею кодування є один біт. Результат кодування не залежить від того, який раніше пройшов вхідний потік. Схема застосовується в системах передачі потоків інформації, тобто в тих випадках, коли передача інформації починається й закінчується в довільні моменти часу і може випадково уриватися. Найбільш поширеними представниками потокових шифрів є скремблери.

Блокові шифрию

Одиницею кодування є блок з декількох байтів (4-32). Результат кодування залежить від усіх початкових байтів цього блоку. Схема застосовується при пакетній передачі інформації й кодуванні файлів.

Всі використовувані в даний час криптосистеми з відкритим ключем опираються на один з наступних типів необоротних перетворень.

Розкладання великих чисел на прості множники (алгоритм RSA, автори - Райвест, Шамір і Адлеман - Rivest, Shamir, Adleman).

Обчислення логарифма або піднесення до ступеня (алгоритм DH, автори - Діффі і Хелман)

Розглянемо простий приклад необоротних функцій. Легко в думці знайти добуток двох простих чисел 18 і 23. Але спробуйте швидко в думці знайти два прості числа, добуток яких дорівнює 2345. Такі ж труднощі виникають і при використанні обчислювальної техніки для відшукання двох простих співмножників для дуже великого числа: знайти співмножники можна, але буде потрібно багато часу.

Таким чином, в системі кодування, заснованій на розкладанні на множники, використовуються два різних ключи: один для шифрування повідомлення, а другий - відмінний від першого, але пов'язаний з ним, - для дешифрування. Ключ шифрування заснований на добутку двох величезних простих чисел, а ключ дешифрування - на самих простих числах.

У асиметричних системах доводиться застосовувати довгі ключі (512 бітів і більше). На жаль, довгий ключ різко збільшує час шифрування відкритого повідомлення. Крім того, генерація ключів стає дуже тривалою. Зате пересилати ключі можна за незахищеними (незасекреченими, відкритими) каналами зв'язку. Це особливо зручно, наприклад, для комерційних партнерів, розділених великими відстанями.

Ніж довший ключ, тим вищий рівень безпеки, більше криптостійкість шифру. Проте процеси шифрування і дешифрування займають багато часу, а значить, зменшується швидкість обміну інформацією.

У симетричних алгоритмах використовують коротші ключі, тобто шифрування і дешифрування відбуваються швидше. Але в таких системах розподіл (розсилка) ключів є складною процедурою із-за необхідності тримати в таємниці інформацію про секретний ключ. Використання кур'єрів для розсилки ключів - дорога, складна і повільна процедура.

У США для передачі секретних повідомлень найбільшого поширення набув стандарт DES (Data Encryption Standard). "Потрійний DES" передбачає для підвищення стійкості повідомлення триразове шифрування даних з різними ключами. Стандарт шифрування даних DES був розроблений фірмою IBM на початку 70-х років і спочатку називався Lucifer.

Складний алгоритм DES використовує ключ завдовжки 56 біт і вимагає від криптоаналітика перебору 72 квадрилліонів (1015) можливих ключових комбінацій.

Недоліком шифру DES є мала довжина ключа - 56 біт і повільна програмна реалізація (великий об'єм обчислень).

Свій розвиток DES отримав в ГОСТ 28147-89, який збільшив довжину ключа до 256 біт.

У аддитивному методі літери алфавіту замінюються числами, до яких потім додаються числа секретної псевдовипадкової числової послідовності (гами). Гама генерується залежно від наявного ключа. Зазвичай для шифрування використовується логічна операція що "Виключає АБО". Для розшифровування та ж гамма накладається на зашифровані дані. Метод гамирування широко використовується у військових системах.

Огляд методик рандомізації повідомлень

Рандомізація повідомлень робить навіть одне й теж повідомлення в декількох копіях несхожими. Дві основні методики внесення випадковості в процес шифрування представляють з себе : а) внесення випадкових біт у сам шифрований файл з ігноруванням їх на дешифруючій стороні, б) шифрування початкового файлу випадковим ключем.

Наступним удосконаленням, направленим на підвищення стійкості всієї системи в цілому є створення ключів сеансу. Ця операція, необхідна в тих випадках, коли проводиться часте шифрування схожих блоків даних одним і тим же ключем. Наприклад, це має місце при передачі інформації або команд в автоматизованих системах управління, в банківських операціях і багатьох інших випадках передачі інформації, яка має визначений наперед відомий формат.

В цьому випадку необхідне введення якої-небудь випадкової величини в процес шифрування. Це можна зробити декількома способами:

1. Записом в початок файлу даних псевдовипадкової послідовності байт наперед обумовленої довжини з відкиданням її при дешифрувані – цей метод працюватиме тільки при застосуванні алгоритмів створення ланцюжків із пам'яттю (CBC,CFB,OFB).

2. Застосуванням модифікованих алгоритмів створення ланцюжків, які при шифруванні кожного блоку змішують з ним або на:

а) фіксовану випадкову величину, прикріплену до початку зашифрованого файлу;

б) значення, що обчислюються за допомогою того ж шифру й ключа від наперед обумовленої величини .

3. Створенням спеціально для кожного файлу абсолютно випадкового ключа, так званого ключа сеансу, яким і шифрує весь файл (сам же ключ сеансу шифрується первинним ключем, званим у цьому випадку ключем майстра і поміщається на початку зашифрованого файлу).

Із-за більшої опрацьованості останнього методу звичайно, застосовується саме він.

Генератори випадкових і псевдовипадкових послідовностей

Генератори випадкових послідовностей грають велику роль у сучасній криптографії. У тому випадку, коли послідовність, що генерується, заснована тільки на можливостях ЕОМ, вона називається псевдовипадковою. Дійсно випадковими є тільки деякі фізичні процеси і людський чинник.

Найбільша проблема всіх методів рандомізації повідомлень – це породження дійсно випадкової послідовності біт. Річ у тому, що генератори випадкових послідовностей, які використовуються для загальних цілей, наприклад, в мовах програмування, є насправді псевдовипадковими генераторами. Річ у тому, що у принципі існує кінцева, а не нескінченна безліч станів ЕОМ, і, як би складно не формувалося в алгоритмі число, воно все одно має відносно небагато біт інформаційної насиченості.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

- зашифроване повідомлення повинне піддаватися читанню тільки за наявності ключа;

- число операцій, необхідних для визначення ключа, який використовується для шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів повинно мати сувору нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);
- знання алгоритму шифрування не повинне впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення в процесі шифрування, повинен бути повністю і надійно приховані в шифрованому тексті;
- довжина шифрованого тексту повинна бути рівній довжини початкового тексту;
- не повинно бути простих і легко встановлюваних залежністю між ключами, послідовно використовуваними в процесі шифрування;
- будь-який ключ з множини можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Системи шифрування даних, які передаються за мережами

Розрізняють два основні способи шифрування: канальне шифрування і крайове (абонентське) шифрування.

У разі канального шифрування захищається вся інформація, яка передається за каналами зв'язку, включаючи службову. Цей спосіб шифрування має наступну пере-

вагою - вбудовування процедур шифрування на канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи. Проте у даного підходу є і істотні недоліки:

- шифрування службових даних ускладнює механізм маршрутизації мережевих пакетів і вимагає розшифровування даних в пристроях проміжної комунікації (шлюзах, ретрансляторах і т.п.);
- шифрування службової інформації може привести до появи статистичних закономірностей в шифрованих даних, що впливає на надійність захисту і накладає обмеження на використання криптографічних алгоритмів.

Крайове (абонентське) шифрування дозволяє забезпечити конфіденційність даних, які передаються між двома абонентами. В цьому випадку захищається тільки зміст повідомлень, вся службова інформація залишається відкритою. Недоліком є можливість аналізувати інформацію про структуру обміну повідомленнями, наприклад про відправника і одержувача, про час і умови передачі даних, а також про об'єм передаваних даних.

Криптоаналіз

Можна стверджувати, що впродовж століть дешифруванню криптограм допомагає частотний аналіз появи окремих символів і їх поєднань. Вірогідність появи окремих літер в тексті сильно розрізняється. Для української мови, наприклад, літера "о" з'являється в 45 разів частіше за літеру "ф". Відносна частота появи пропуску або розділового знаку складає 0,174.

Аналізуючи достатньо довгий текст, зашифрований методом заміни, можна за частотами появи символів провести зворотну заміну і відновити вихідний текст.

При проведенні криптоаналізу потрібно за невеликим відрізком тексту вирішити, що є дешифрованим текстом: осмислене повідомлення або набір випадкових символів. Часто криптоаналітики розкривають шифри на ЕОМ методом перебору ключів. В процесі криптоаналізу доводиться перебирати мільярд ключів з швидкістю тисяча ключів в секунду, на що йде близько 12 днів. Уручну виконати аналіз без-

лічі фрагментів текстів, що дешифруються, неможливо. Тому задачу виділення осмисленого тексту (тобто виявлення тексту, що правильно дешифрується) вирішують за допомогою ЕОМ. В цьому випадку використовують теоретичні положення, розроблені в кінці XIX століття петербурзьким математиком Марковим А.А., так звані ланцюги Маркова.

Слід відмітити, що, на думку деяких фахівців, немає нерозкриваних шифрів. Розсекретити будь-яку шифрограму (зламати) можна або за великий час, або за великі гроші. У другому випадку для дешифрування буде потрібно використання декількох суперкомп'ютерів, що приведе до істотних матеріальних витрат.

Шифрування даних за допомогою спеціальних програм та утиліт.

Програма Super File Encryption

Потужна та зручна в роботі програма призначена для того, щоб зашифрувати і захистити дані – зручна для офісів, які тримають важливі документи. Щоб зашифрувати або розшифровувати файли/каталог, просто виділіть файли або каталоги, і виберіть команду **Зашифрувати** або **Розшифрувати**. Програмне забезпечення також дозволяє мати зв'язок безпечної електронної пошти за Інтернетом, запобігаючи доступу неправомочних людей, що пробують читати файли.

Після запуску програми з'явиться діалогове вікно куди необхідно ввести пароль (рис.4.1) .

Примітка:

При першому запуску програми вікно буде мати два поля в які необхідно внести ваш початковий пароль. Після запуску програми з'явиться діалогове вікно (рис. 4.2). Для шифрування файлу (ів) необхідно натиснути клавішу **Encrypt**, і **вибрати файли** для шифрування. Після цього програма проводить шифрування файлів і показує їх у своєму діалоговому вікні (рис. 4.2). Для дешифрування файлу (ів) необхідно їх вказати в діалоговому вікні (рис. 4.2) і натиснути клавішу **Decrypt**. Після

цього програма проведе дешифрування файлу (ів). Для зміни паролю

Рис. 4.1. Початкове вікно введення паролю.

адміністратора і вибору параметрів шифрування необхідно натиснути клавішу **Optima** і вибрати зазначені параметри (рис. 4.3) та змінити пароль (рис.4.4). У вікні рис. 4.3 позначений Ehable 448-bit encryption method -- метод шифрування на 448 битів; Include system or hidden files -- включіть систему приховані файли; Include subfolders -- включіть підкаталоги.

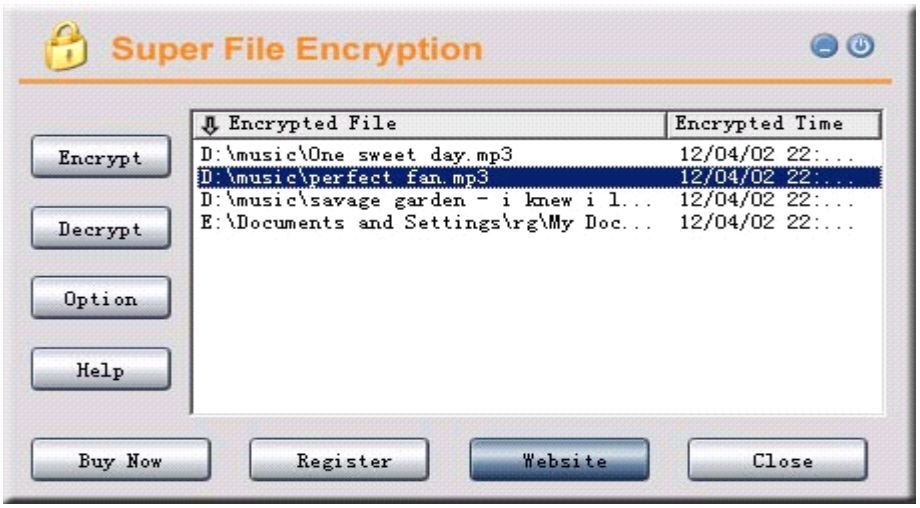


Рис. 4.2. Вікно програми

Можна перевірити результати шифрування , наприклад, через провідник Windows (рис. 4.5)

Рис. 4.3. Вікно добору параметрів шифрування

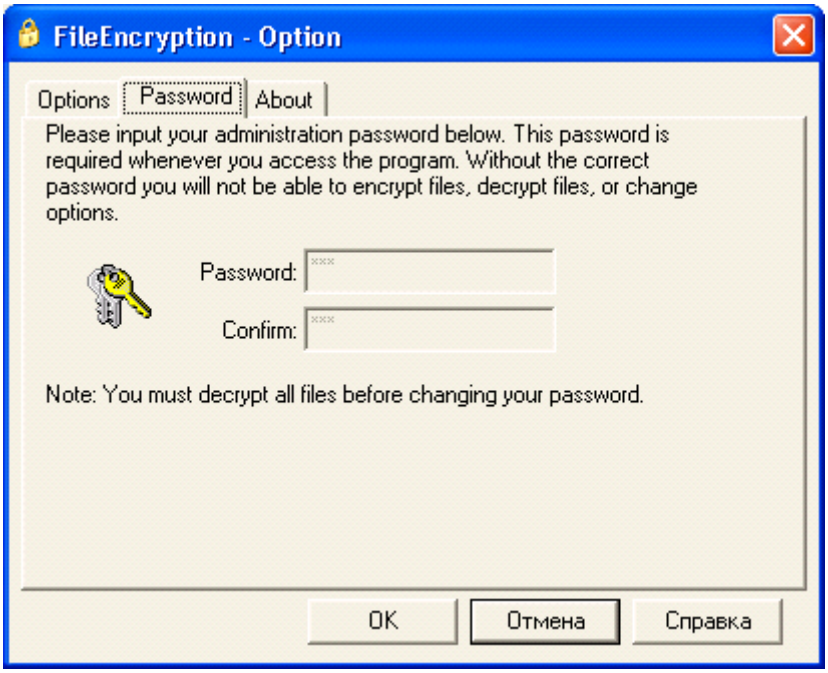


Рис. 4.4. Вікно зміни паролю

Робота з утилітою: (T-CEC Pro)

T-CEC Pro - утиліта для кодування/декодування файлів у будь-якому форматі.

The coding equipment of connection - у російському варіанті " апаратура зв'язку", яка засекречує, (ЗАЗ)". "ЗАЗ" - так в армії називають апаратуру за принципом шифрування якого побудована дана програма.

Після запуску програми з'явиться діалогове вікно (рис. 4.6)

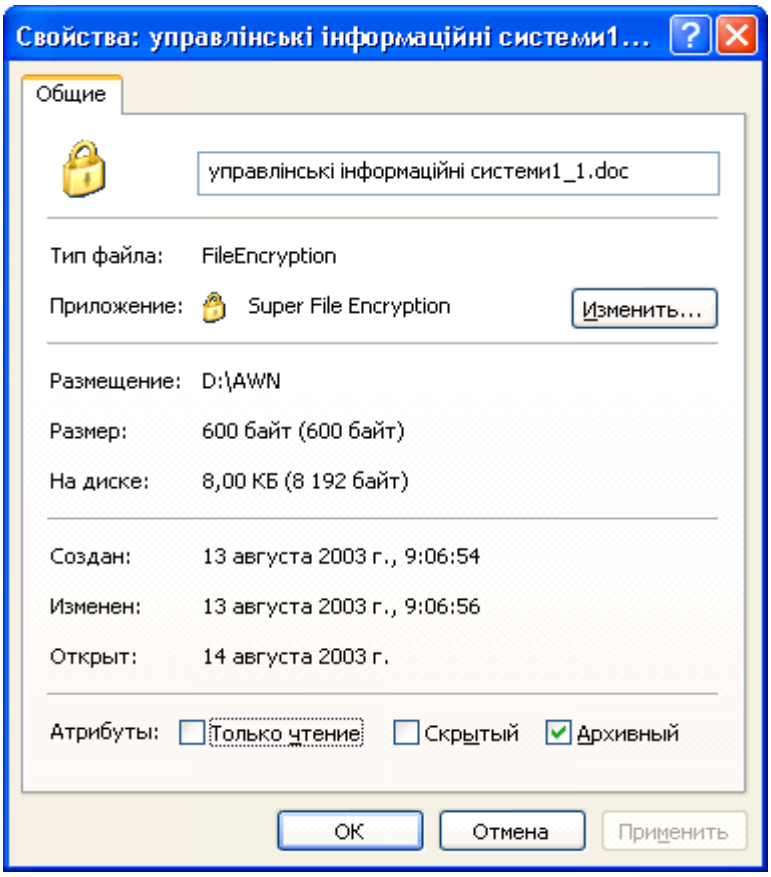


Рис.4.5. Перевірка результатів шифрування з використанням провідника Windows

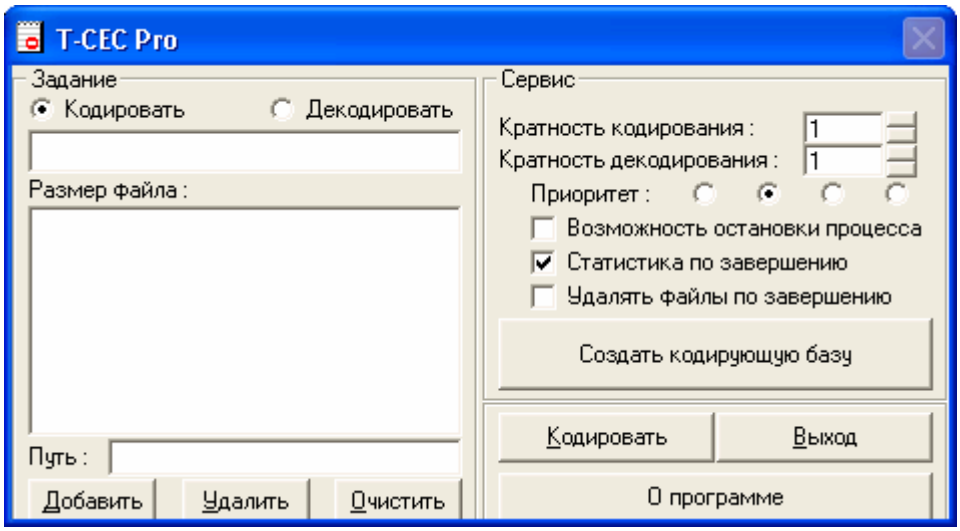
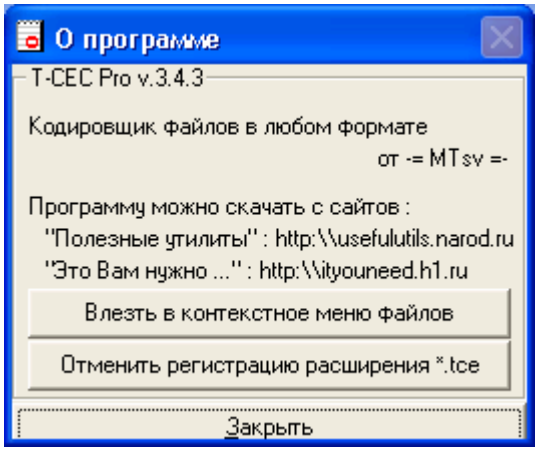


Рис. 4.6. Вікно утиліти

Правила використання.

- у верхній частині вікна вибирається операція (**кодування/декодування**);
- вибирається файл (и) за допомогою кнопки "**Добавити**";
- список можна редагувати за допомогою кнопки "**Видалити**".

- список можна очистити за допомогою кнопки "**Очистити**";
- далі треба створити базу, що кодує, (розмір бази = 256 byte) (використовуємо відповідну кнопку);
- далі натискаємо кнопку "**кодувати/декодувати**" і чекаємо;
- після виконання операції кінцевий файл зберігається й одержує ім'я <вихідне_ім'я>.tce;
- потім старий файл віддаляється зі списку і починається кодування/декодування наступного файлу в списку;
- є можливість багаторазового кодування/декодування;
- є можливість вибору пріоритету роботи програми;
- є можливість увійти в контекстне меню усіх файлів, для цього треба подивитися "Про програму..." (натискаємо відповідну кнопку) (рис. 4.7.);



- Рис. 4.7. Вікно "Про програму..."

- є можливість зареєструвати розширення кодованих файлів, для цього треба подивитися "Про програму..." (рис. 4.8).

Примітка:

Якщо **пошкодите** базу, то утратите **всі** закодовані в ній **документи**. **Робіть кілька копій одної і тієїж бази.**

База повинна бути одна для кодування і декодування.

Система шифрування даних BestCrypt

Забезпечує зручне в роботі безпечне збереження даних і доступні засоби обслуговування контролю (керування) доступом до них. Після, створення контейнера,

дані ніколи не зберігаються в відкритому стані. Вони захищені і зашифровані, яким методом би не копіювали або переміщували дані в контейнер.

BestCrypt використовує наступні алгоритми шифрування:

- алгоритм Blowfish -- з ключовою довжиною 256 битів;
- Twofish алгоритм -- з ключовою довжиною 256 битів;
- Rijndael алгоритм -- з ключовою довжиною 256 битів;
- ГОСТ 28147-89 з ключовою довжиною 256 битів.

Алгоритм Blowfish був розроблений Брюсом Шнеиром у 1993 і тепер дуже популярний у світі.

Twofish алгоритм був також розроблений Брюсом Шнеиром разом із Джоном Келсеем, Крис Хол, Нилсом Фергузоном, Дэвидом Уогнером і Дугом Витингом.

Rijndael винайдений Джоан Даеменом і Винсентом Риджменом, і недавно NIST (національний Інститут Стандартів, і Технологія) вибрала алгоритм як потужний Стандарт Шифрування (AES).

Використання в Мережі

BestCrypt програмне забезпечення для Windows 95/98/ME/NT/2000/XP. Операційна система може використовувати будь-який диск мережі для того, щоб створити контейнер файлів. Цей диск мережі може бути розділений комп'ютером з будь-якою операційною системою, наприклад UNIX операційні системи (OSF/1, LINUX, BSD, SunOS, ЕКС-АН-ПРОВАНС, Novell, Windows NT, Windows 95, Windows 3.xx і інші).

Поняття контейнера.

Контейнер - спеціальний файл, створений користувачем з BestCrypt **Пультом керування**. Це може бути нанесений на карту файл (установлений) на дійсний (віртуальний) диск. Кількість контейнерів програмою не обмежується.

Кожен контейнер має власний пароль. Потрібно визначити пароль, коли створюєте контейнер і використовувати той же самий пароль, коли відкриваєте дійсний (віртуальний) диск, зв'язаний з контейнером. Використовуючи **Пульт керування** BestCrypt можна змінити пароль контейнера.

Примітка:

Якщо забути пароль для зашифрованих даних, то втратите здатність одержати доступ до них.

Цей метод шифрування не дозволяє "відновити" інформацію, не знаючи паролю.

BestCrypt має сильну, убудовану схему шифрування і не містить ніякого "люка". "Люк" – назва особливості, що дозволяє владі з юридичним (законним) дозволом обійти захист і одержувати доступ до даних без дозволу його власника. Багато комерційних і завірених урядом систем містять люки. Єдиний шлях одержати доступ до даним, захищеним BestCrypt полягає в тому, щоб мати відповідний пароль.

Після запуску програми з'являється діалогове вікно (рис. 4.8). Для шифрування файлів спочатку потрібно створити контейнер, для цього з під меню **Контейнер** уводиться команда **Новий Контейнер** і вказується його розміщення, ім'я та інші параметри (рис.4.9).

На кожен контейнер установлюється пароль (рис. 4.10), або проводиться його зміна при необхідності.

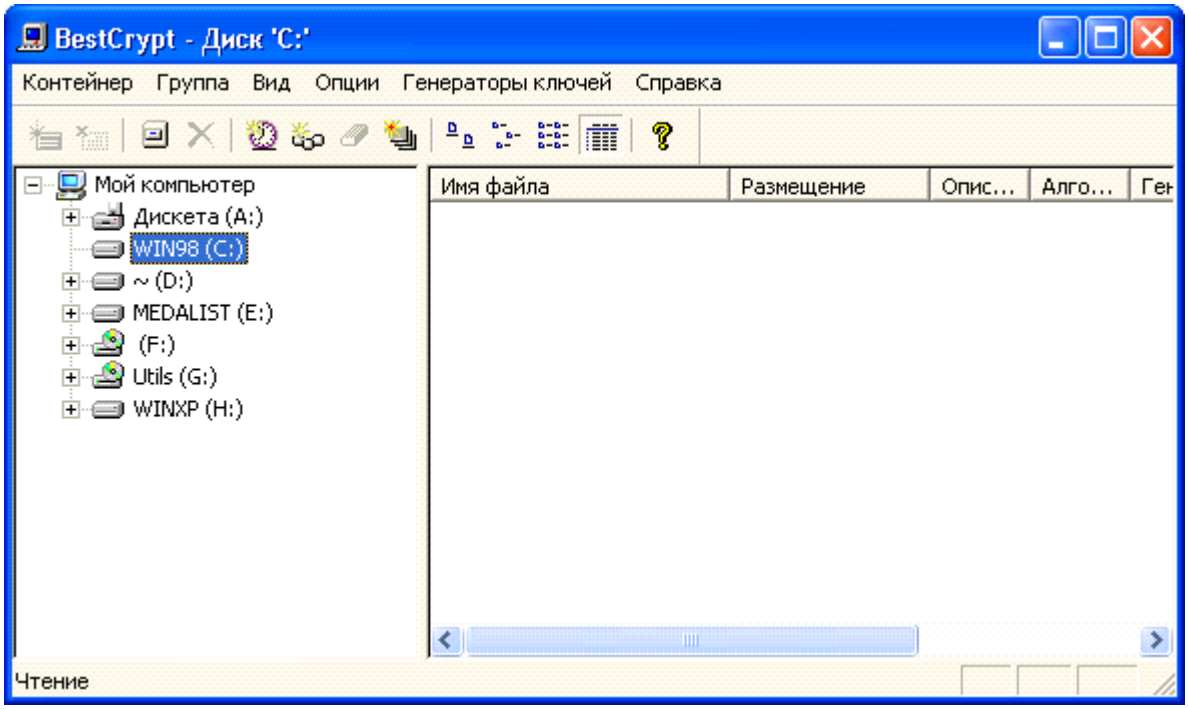


Рис. 4.8. Діалогове вікно програми.

Використання генератора ключів

Використання цієї області, дозволить змінити ключовий алгоритм генератора, що у даний час використовується BestCrypt системою, для того, щоб зробити ключ шифрування для пароля: від GOST до SHA-1. За замовчуванням, BestCrypt уставляє до області Key Генератор той же самий алгоритм, що у даний час використовується для контейнера.

Після створення контейнера можна залишити програму. Секретний дійсний (віртуальний) диск X: тепер доступний точно так само як нормальний дисковод. Усе, що пишеться на диск, буде автоматично зашифровано і потім при необхідності дешифровано, коли необхідно читати дані з диска.

Примітка:

BestCrypt **Пульт керування** показує інформацію в контейнерах у групі **Списку Контейнерів** виразно для кожного користувача, що може почати роботу (ввійти в систему) на комп'ютер під логіном та паролем при якому створювався контейнер, але контейнер буде не видно, якщо увійти до комп'ютера під іншим логіном.

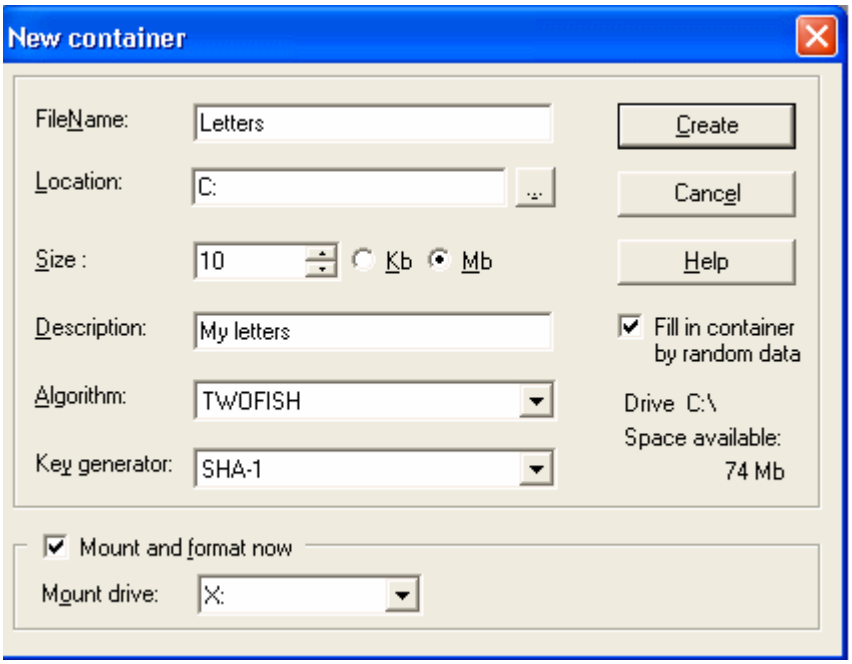


Рис. 4.9. Вікно вибору параметрів нового контейнера

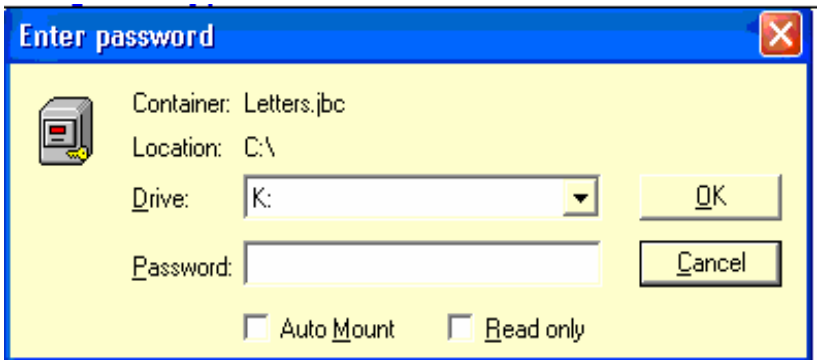


Рис.4.10. Вікно встановлення паролю на контейнер

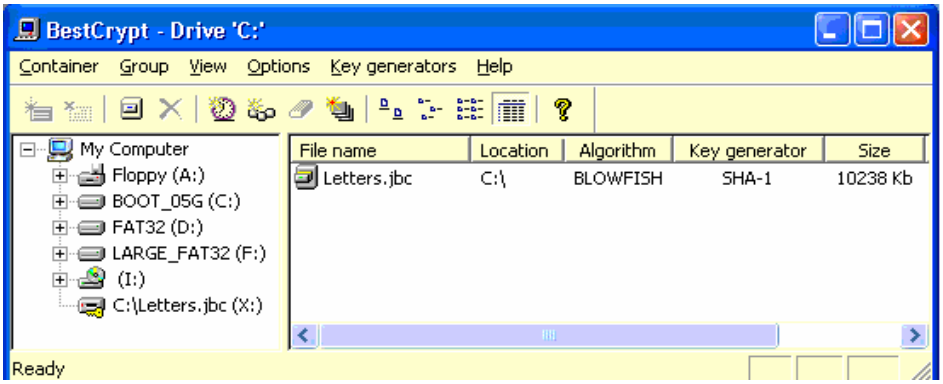


Рис.4.11. Вікно зі створеним контейнером

Робота зі Схованим і Оригінальним контейнерами

Оригінальний файл-контейнер BestCrypt складається з трьох частин:

1. Перші 512 байт, містять дані, необхідні для перевірки цілісності файлу.

2. Ключовий блок даних, що зберігає масив ключів шифрування. Ключовий блок зашифрований випадковими даними, обчисленими з пароля користувача. Один із ключів у масиві використовується для шифрування/дешифрування даних користувача.

3. Зашифровані дані.

При установці оригінального контейнера, BestCrypt перевіряє його цілісність з використанням першої частини контейнера. Потім обчислює випадкові дані відповідно до пароля і використовує їх для дезшифрування ключа шифрування з ключового блоку даних. Програмне забезпечення використовує ключ для забезпечення прозорого шифрування даних у третій частині контейнера.

Якщо створюється схований розділ у контейнері, BestCrypt створює новий ключ шифрування для нього і зберігає його в ключовому блоці даних оригінального контейнера. Місце, де зберігається ключ схованого розділу, відзначено як невикористане, так що неможливо визначити, чи існує ключ чи ні. Вільний дисковий простір у межах контейнера самостійно зашифрований як випадкові дані.

Так, заміна деяких випадкових даних новим випадково сгенерированим ключем, не компрометує сховану частину, оскільки експертиза покаже, що це просто випадкові дані.

Схований розділ збережений у 3-їй частини оригінального контейнера без його власного ключового блоку даних, так що неможливо визначити границі схованого розділу усередині оригінального контейнера.

Процедура установки контейнера зі схованим розділом така ж, як і при установці нормального контейнера.

При установці контейнера після введення пароля, BestCrypt виконує наступні дії:

1. Спочатку програма BestCrypt пробує використовувати пароль для установки оригінального контейнера, начебто в ньому немає схованої частини.
2. Якщо цей пароль непідходить для установки оригінального контейнера, BestCrypt перевіряє існування схованої частини в контейнері і використовує значення випадкових даних, сгенерованих з пароля, для витягу ключа шифрування для схованої частини.
3. Якщо пароль підходить для відкриття схованого розділу, BestCrypt установить цей розділ і повідомить користувачеві, що виявлено схований розділ. Це повідомлення дозволить користувачеві довідатися який об'єкт був установлений - оригінальний контейнер або схована частина.

Примітка:

Допускається наявність записаних даних в оригінальному контейнері перед створенням схованої частини. Але як тільки створений новий схований контейнер, ніякі дані не повинні коли-небудь, записуватися в оригінальний контейнер. Якщо зробити запис в оригінальний контейнер, схована частина може бути ушкоджена!

Утиліта DISKREET.

Утиліта захищає дані від несанкціонованого доступу. Дані кодуються, і без належного пароля їх не можна перетворити до початкового стану.

Захищати інформацію можна двома способами. Перший складається в кодуванні окремих файлів, другий - у створенні деякої захищеної від несанкціонованого доступу області на одному з логічних пристроїв системи. Ця область називається NDisk. Зовні вона виглядає як сховані файли DOS, однак поводиться як самостійний диск. При копіюванні файлів у цю область відбувається автоматичне кодування даних.

Кодування й декодування окремих файлів

Для даного режиму роботи в основному меню потрібно натиснути кнопку **Files**. На відміну від роботи з NDisk індивідуальне кодування припускає окремий пароль для кожного файлу, що захищається. Роскодування відбувається "вручну".

Підміню Files.

Складається з трьох пунктів: Encrypt, Decrypt, File optiions.

Зміна пароля:

1. Увійдіть у **Disk** меню і виберіть опцію **change disk Password**.
2. Виберіть **Proceed** для виклику діалогового вікна, де буде запит про поточний пароль.
3. Уведіть поточний пароль.
4. Якщо потрібно змінити ідентифікатор, відповідайте **Yes**.
5. Уведіть новий пароль. Підтвердіть його.
6. Уведіть знову пароль. Після цього видається запит швидкої зміни пароля - **Quick** або повної перешифрування - **Full**.
7. Виберіть **Quick** чи **Full**. Якщо вибрати **Full**, з'явиться попередження, що спочатку потрібно скинути на дискету **NDisk**. Виберіть **Proceed**, щоб забрати попередження. Потім у діалоговому вікні буде показаний процес перешифрування.

Видалення NDisk.

1. Запустіть **Diskreet** і ввійдіть в основне вікно.
2. Увійдіть у **Options** головного меню і виберіть опцію **Security**.
3. Виділіть той **NDisk**, який потрібно.
4. Увійдіть у **Disk** головного меню і виберіть у ньому опцію **Delete**.
5. Уведіть пароль **NDisk**.
6. Виберіть **Delete**.

Кодування і роскодування окремих файлів

Для того щоб закодувати файл, його не варто копіювати на Ndisk. Можливо закодувати файл у будь-якому каталозі на індивідуальній основі. При цьому кожен закодований файл буде мати свій власний пароль, за допомогою якого в майбутньому можливе розкодування потрібного файлу.

Особливості захисту даних:

- Індивідуальний пароль для кожного кодуємого файлу;
- Неможливість автоматичного роскодування;
- Копіювання, резервування й телекомунікація файлів у закодованому виді.

File керує індивідуальним кодуванням і роскодуванням. Для початку варто установити параметри кодування опцією **File Options**.

Wipe/Delete original files after encryption. Виберіть дану опцію, щоб перемістити вихідний незакодований файл із диска після його кодування.

Set Encrypted file to Hidden. Робить файл невидимим для більшості функцій DOS, таких як DIR і DEL.

Set Encrypted file to Read-Only. Ця опція захищає файл від запису. Файл не може бути вилучений або змінений звичайним шляхом.

Delete Encrypted file after decryption. Виберіть цю опцію, якщо потрібно розкодувати файл або видалити файл у закодованому виді.

Use same password for entire session. Виберіть опцію, якщо потрібно закодувати або розкодувати кілька файлів з однаковим паролем.

Можливе кодування одного файлу декількох файлів в один закодований файл, при роскодуванні вони будуть розділені.

Виконуйте наступні кроки для кодування файлу:

1. Запустіть **Diskreet** і виберіть кнопку **Files** в основному меню.
2. Виберіть опцію **Encrypt**. У діалоговому вікні з'явиться прохання ввести ім'я файлу, який треба закодувати.
3. Уведіть ім'я файлу, включаючи шлях, якщо це необхідно.
4. Уведіть ім'я, яке потрібно призначити закодованому файлу.
5. Уведіть пароль.
6. Для перевірки введіть пароль знову. У діалоговому вікні буде показаний процес кодування файлу, а потім повідомлення про те, що робота виконана.

Кроки для роскодування файлу:

1. Запустіть **Diskreet** і виберіть кнопку **Files** в основному меню.
2. Виберіть опцію **Decrypt**. У діалоговому вікні з'явиться прохання ввести ім'я файлу, який потрібно розкодувати.
3. Уведіть ім'я файлу, включаючи шлях, якщо це необхідно.
4. Уведіть пароль, яким був закодований файл. У діалоговому вікні буде показаний процес роскодування файлу, а потім повідомлення про те, що робота виконана.

Блокування клавіатури й екрана

Якщо потрібно запобігти, доступу до комп'ютера під час відсутності користувача, можна заблокувати клавіатуру і затемнити екран.

1. Увійдіть у меню **Options** і виберіть опцію **Keyboard and Screen Lock**.
2. Виберіть **Enable locking**.
3. Якщо потрібно розблокувати клавіатуру й екран, виберіть гарячу клавішу. Якщо **Quick-Close** також закрита, однією гарячою клавішею будуть закриті і клавіатура й екран.

Розблокувати клавіатуру й екран можна, натиснувши гарячу клавішу. Це не означає, що відразу заробить клавіатура і засвітиться екран. Екран буде як і раніше затемнений, а клавіатура буде сприймати натискання клавіш і видавати звуковий сигнал. Для повного розблокування введіть пароль.

Зміна основного пароля

1. Увійдіть у меню **Options** і виберіть опцію **Change main password**.
2. З'явиться прохання ввести поточний пароль.
3. Уведіть поточний пароль.
4. Уведіть новий пароль.
5. Підтвердіть новий пароль.

Захист інформації за допомогою програми Lock Folder XP

Lock Folder XP - інструмент безпеки, який дозволяє захищати файли, каталоги особистим паролем. Без знання паролю ніхто не може звернутися до інформації. Автоматично проводиться захист даних від шкідливих програм, таких як наприклад, віруси, хропаки, і трояни. Для захисту можна просто перетягнути мишкою (рис. 4.12) файли або каталоги вікна Lock Folder XP, і захист робиться автоматично. Як відомо, понад 80% з відомих порушень безпеки інформації відбувається зсередини організації, не від хакерів! Захист файлів, каталогів, - кращий спосіб гарантувати, що ніхто випадково або навмисно не матиме доступ до даних з кредитних карток, фінансової, оздоровчої, приватної, конфіденційної і т. п. інформації. Захищені файли, каталоги, становляться невидимими, вони не можуть бути видалені, пошкоджені, або фальсифіковані будь-яким іншим шляхом.

Особливості програми:

- Здатність приховування файлів, каталогів від всіх інших користувачі (в тому числі і адміністраторів);
- Захист з використанням пароля для файлів, каталогів;

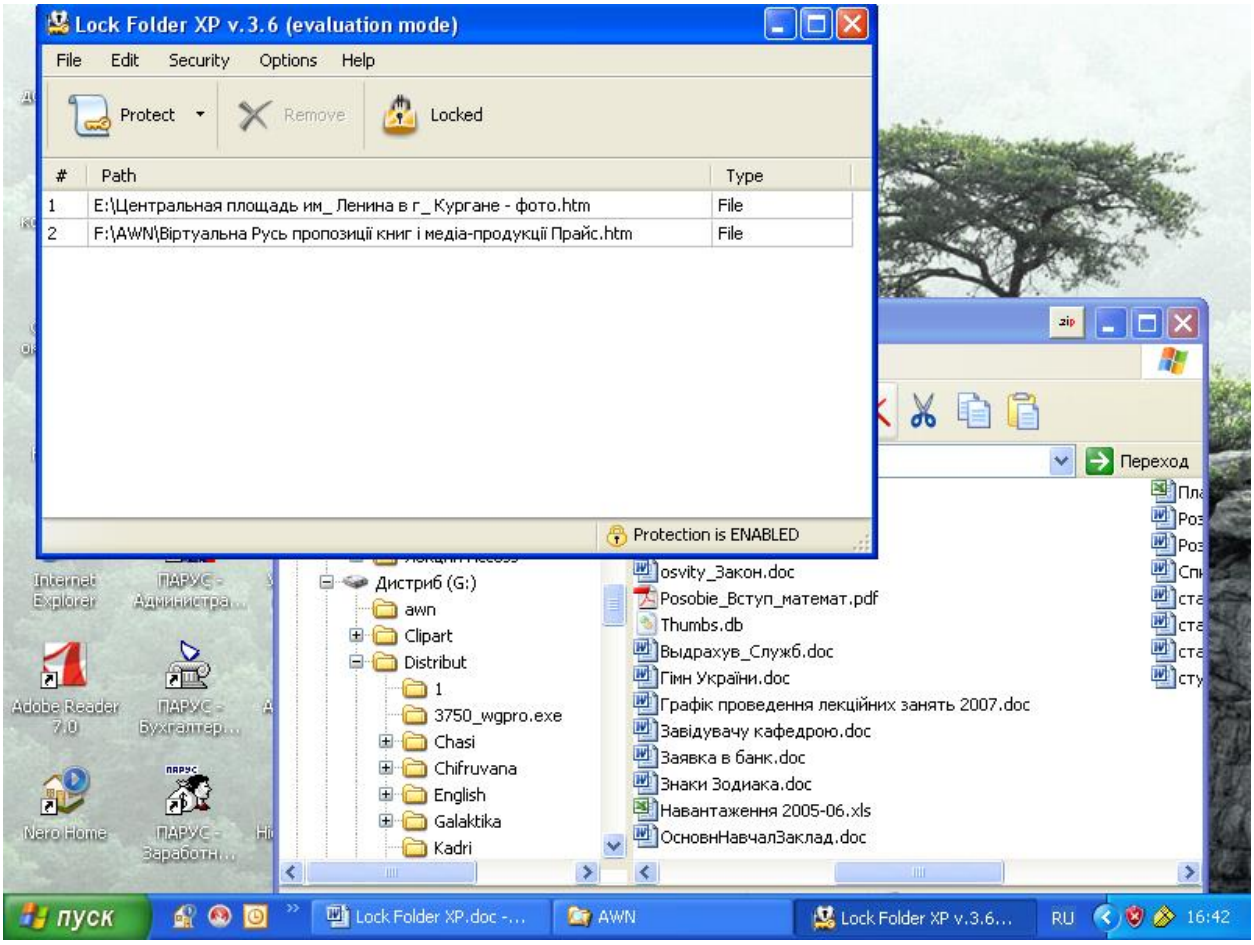


Рис. 4.12. Перетягування файлів до вікна програми

- Обмеження доступу до даних від користувачів локальної та глобально-їмережі;
- Автоматична активація захисту через певний час;
- Підтримка FAT, FAT32, і системи NTFS.

Примітка:

Lock Folder XP не змінює файлову структуру даних, не переміщає захищені дані, і не змінює системні файли Windows.

Приховування файлів і каталогів

Попередження! Не приховуйте системні файли Windows або каталоги. Якщо вказані файли або каталоги будуть приховані, то Windows не може знайти файл, потім Windows може стати нестійким і дані можуть бути пошкоджені або втрачені.

Якщо потрібно, запустити програму Lock Folder XP введіть команду **Пуск** > **Програми** > **Lock Folder XP** , або двічі клацніть по ярлику **Lock Folder XP** на ро-

бочому столі Windows з'явиться вікно запиту пароля (рис.4.13) та початкове вікно (рис. 4.14)

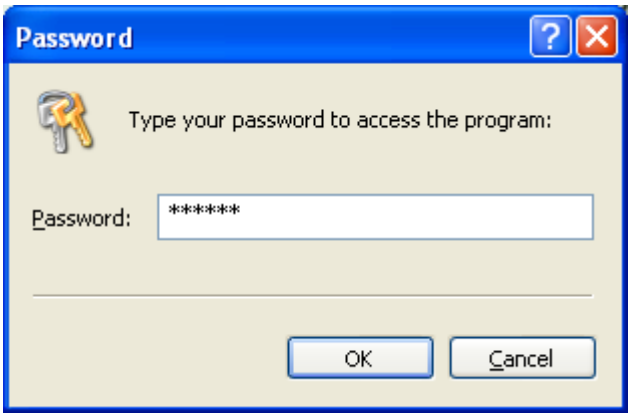


Рис.4.13. Вікно запиту пароля при запуску програми

Для запуску майстра захисту введіть команду **Файл** > **Lock Folder XP Wizard**.

В діалоговому вікні майстра виберіть **Приховати файли, каталоги, або диски**.(рис. 4.15) (можна приховати диски тільки в Windows NT, 2000, і XP).

В наступному вікні відберіть **Приховати файли, каталоги, або диски** (рис. 4.16).

В наступному вікні введіть команду **Add to list** та вкажіть об'єкти які будуть приховані (рис. 4.17).

Введіть команду Далее та **ОК** .

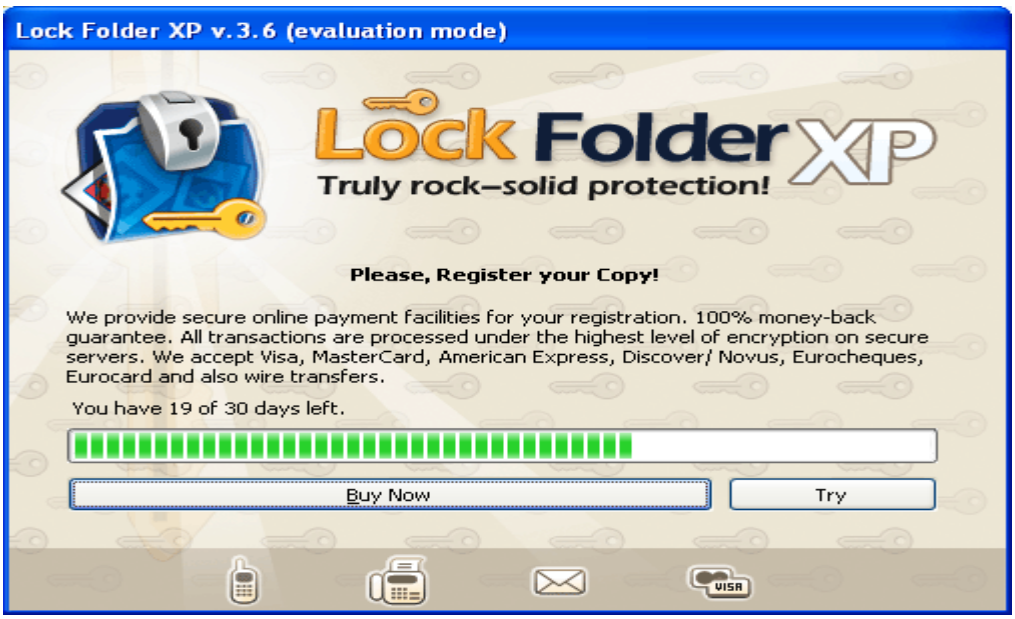


Рис. 4.14. Початкове вікно програми

Примітка:

Якщо необхідно приховати декілька об'єктів введіть команду **Clear All**.

Щоб встановити властивість приховання, необхідно натиснути кнопку **Locked** на панелі інструментів – прихований в системі Windows, або **Unlocked** - видимий.

Кнопка **Remove** дозволяє видалити об'єкти зі списку захищених.

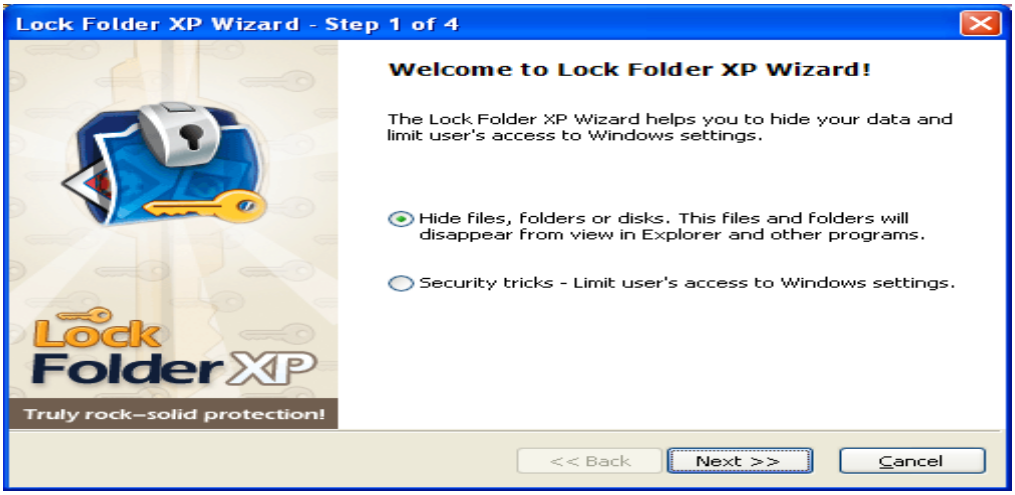


Рис. 4.15. Вікно майстра

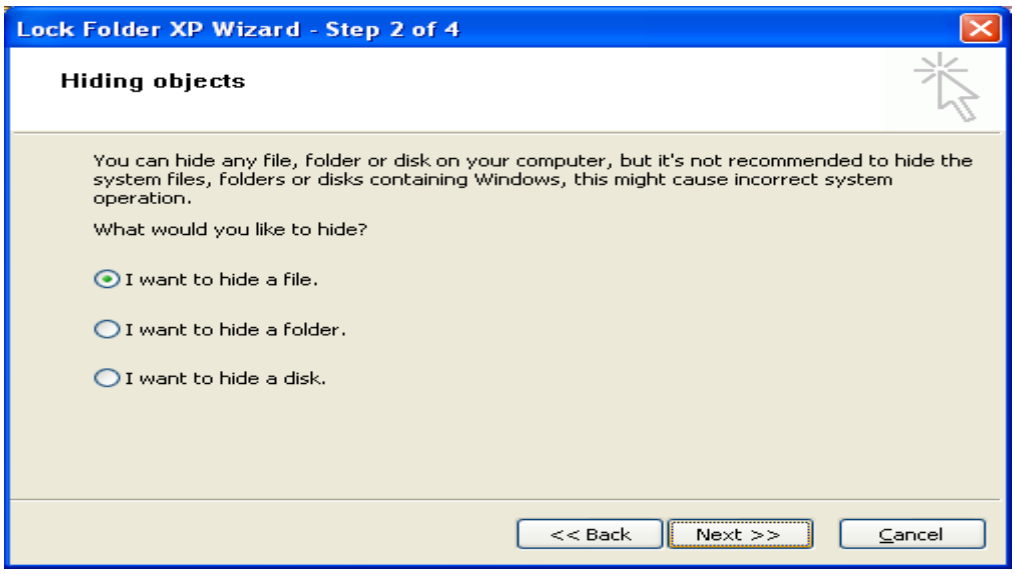


Рис. 4.16. Вікно майстра

Програма дозволяє захищати системні файли та каталоги Windows.

Для цього в першому вікні майстра відбірається потрібна команда та вказуються потрібні параметри аналогічно приховуванню файлів.

Пароль на програму встановлюється при інсталяції її на вінчестер і гарантує неможливість деінсталяції програми без знання паролю (рис. 4.18). Його можна

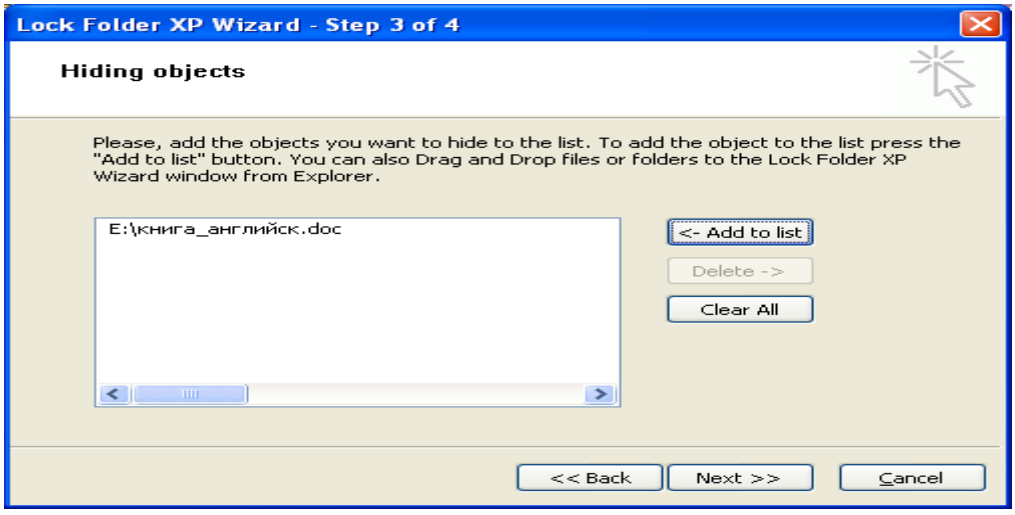


Рис. 4.17. Вікно майстра

встановити і пізніше (якщо не встановлений при інсталяції програми). Введіть команду **Security** і **Change Password** та запишіть пароль. Встановіть **Options** і **Password Protection** для використання паролю програмою.

Рекомендується встановлювати буквенно цифрові паролі (не менш шести символів) з використанням символів: ! @ # $ % ^ & * ( ) _.

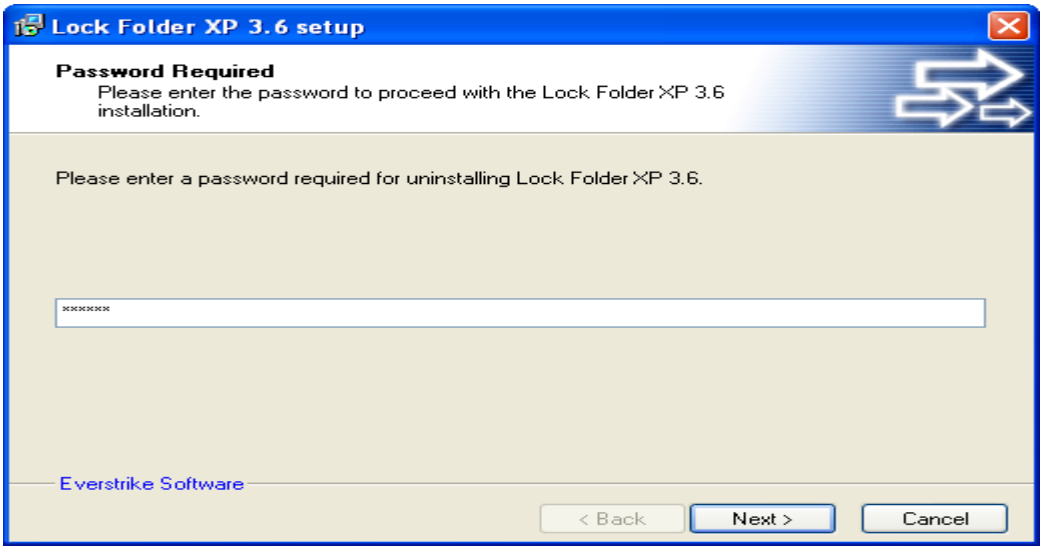


Рис. 4.18. Вікно деінсталяції програми

КОНТРОЛЬНІ ПИТАННЯ

1. Принцип роботи шифрувального устрою скитала.
2. Принцип дешифрування шифру скитала.
3. Принцип шифрування в древніх іудейських текстах.
4. Принцип шифрування Цезаря.
5. Два напрямки криптології.
6. Поняття криптоаналізу.
7. Особливості програмної криптології.
8. Особливості апаратної криптології.
9. Загальна схема захищеного зв'язку.
10. Призначення рандомізатора в загальній схемі захищеного зв'язку.
11. Призначення ключів.
12. Загальні поняття шифрування підстановкою.
13. Метод підстановки з використанням квадрату Полібія.
14. Загальні поняття методу простої перестановки.
15. Класифікація криптоалгоритмів.
16. Симетричні криптосистеми.
17. Криптосистеми з вікритим ключем.
18. Призначення устрою шифрування та дешифрування в загальній схемі захищеного зв'язку.
19. Правило Огюста Керкхоффа.
20. Поняття крипостійкості.
21. Призначення програми Super File Encryption .
22. Порядок шифрування файлів в програмі Super File Encryption.
23. Порядок дешифрування файлів в програмі Super File Encryption.
24. Порядок підбору параметрів шифрування та дешифрування файлів.
25. Призначення утиліти (T-CEC Pro).
26. Порядок шифрування дешифрування файлів утилітою (T-CEC Pro).
27. Призначення системи шифрування даних BestCrypt.
28. Які алгоритми шифрування підтримує BestCrypt?

29. Короткі характеристики алгоритмів шифрування, які підтримує BestCrypt?
30. Поняття контейнера в системі шифрування даних BestCrypt.
31. Призначення генератора ключів в системі BestCrypt.
32. Особливості роботи зі Схованим і Оригінальним контейнерами.
33. Два методи кодування інформації за допомогою утиліти DISKREET.
34. Пункти підменю FILES утиліти DISKREET.
35. Послідовність зміни пароля в DISKREET.
36. Поняття Ndisk в утиліті DISKREET.
37. Послідовність видалення NDisk в утиліті DISKREET.
38. Послідовність кодування файлів в утиліті DISKREET.
39. Блокування клавіатури та екрану в утиліті DISKREET.
40. Зміна основного паролю в утиліті DISKREET.
41. Захист інформації за допомогою програми Lock Folder XP.

Розділ 5.

ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СИСТЕМ РЕЗЕРВУВАННЯ.

ВСТУП.

Система безпеки господарюючого суб'єкта - це методологія теоретичних підходів і практичних дій, що забезпечують максимально повний захист від всіх видів загроз і ризиків діяльності підприємства. Широке поняття “безпеки” як категорії стану захищеності розвитку, дозволяє розуміти функціональну сутність системи безпеки, як моніторинг захищеності функції розвитку організації від всіх видів погроз і ризиків діяльності.

При такому трактуванні, у центрі системи безпеки розташовані потреби й життєво важливі інтереси особистості, організації й держави з його широким шлейфом структур і органів. Ступінь усвідомлення важливості моніторингу потреб і інтересів, з всього поля його носіїв, є новою, ще не досить усвідомленою, проблемою менеджменту господарюючого суб'єкта, яку не можна не враховувати при виробленні й реалізації політики й стратегії забезпечення організаційної безпеки (див. додаток 4).

Одним із ключових моментів, що забезпечують відновлення системи в разі аварії, є резервне копіювання систем, робочих програм і даних. Незважаючи на очевидність цієї процедури і її відносну нескладність, у деяких організаціях її виконують недостатньо часто або ігнорують взагалі. Резервне копіювання має, супроводжуватися цілим комплексом не менш очевидних організаційних заходів. Носії - стрічки або магніто-оптичні диски - повинні зберігатися за межами серверної кімнати. Оскільки носій використовується багаторазово, потрібно знати стандарти на число припустимих перезаписів і тести, що дозволяють визначити ступінь його зношеності. Широкий вибір пристроїв для копіювання також може зіграти злий жарт із користувачами: про сумісність цих пристроїв варто подбати до того, як один з них вийде з ладу.

Особливу роль у резервному копіюванні належить програмним засобам, їх можливостям, що забезпечують отримання резервних копій.

Резервування даних за допомогою архіваторів та пошук паролів

Програми-архіватори, як правило, мають опцію шифрування. Нею можна користатися для не занадто важливої інформації.

По-перше, використовувані там методи шифрування не занадто надійні (підкоряються офіційним експортним обмеженням).

По-друге, детально не описані.

Усе це не дозволяє всерйоз розраховувати на такий захист. Архіви з паролем можна використовувати тільки для непрофесіоналів (інформація не конфіденційна).

Системи шифрування можуть здійснювати криптографічні перетворення даних на рівні файлів або на рівні дисків.

До програм першого типу можна віднести архіватори типу ARJ і RAR та інші, які дозволяють використовувати криптографічні методи для захисту архівних файлів.

Прикладом систем другого типу може служити програма шифрування Diskreet, що входить до складу популярного програмного пакета Norton Utilities і т.п.

Архів ARJ:

Захист архіву паролем 123: arj a -g123 name - створення архіву.

Витяг з архіву з паролем 123: arj e -g123 name.arj

Архів ZIP:

Захист архіву паролем 45: pkzip a-s45 name - створення архіву.

Витяг з архіву з паролем 45: pkunzip a-s45 name.zip

Архів WinRar:

Protect Archive from Damages (Захистити архів від ушкоджень) – дана команда вносить до архівів додаткові дані, що будуть запобігати від ушкоджень.

Lock Archive (Заблокувати архів) – після того, як дана команда була обрана, архів стає заблокованим від внесення в нього яких-небудь змін.

Архів WinZip:

Захист архіву паролем. З підменю **Options** уводиться команда **Password**. У діалоговому вікні вводитися та підтверджується пароль.

При відкритті архіву необхідно підтвердити пароль.

На деяких сайтах в Інтернеті можна знайти "програми-ломалки" для зашифрованих архівів. Наприклад, архів типу ZIP “зламується” на потужному комп'ютері за кілька хвилин, при цьому від користувача не потрібно особливої високої кваліфікації.

Додаткова інформація:

Ultra Zip Password Cracker 1.00 -- швидкодіюча програма для підбору паролів до зашифрованих архівів. Російсько/англійський інтерфейс. Win'95/98/NT. (Розроблювач – "m53group")

Advanced ZIP Password Recovery 2.2 – потужна програма для підбора паролів до ZIP-архівів. Висока швидкість роботи, графічний інтерфейс, додаткові функції. ОС: Windows 95/98/NT. (Розроблювач – "Elcom Ltd."), shareware.

Для визначення паролю архіву типу ZIP необхідно провести запуск програми Advanced ZIP Password Recovery (AZPR), використавши пусковий файл AZPR.exe, після чого на екрані з'явиться діалогове вікно (рис. 5.1) в якому необхідно вибрати захищений архів та підібрати необхідні параметри пошуку і подати команду почати перебір (кнопка старт). Якщо в архіві знаходяться файли, які мають різні паролі захисту, то необхідно створити копію архіву та визначати паролі окремо для груп файлів, які мають однаковий пароль.

В програмі можна використовувати “гарячі кнопки” : F1 - Help, F2 - Save setup, F3 - Open ZIP file, F4 - Edit charset, F9 - Start, F10 – Stop.

Можливі три режими переборів паролів:

Прямий перебір. Цей режим включає використання для порівняння готових паролів, які знаходяться в додатковому словнику, а також режими використання визначених символів, масок і т.п.

Перебір за маскою. Використовується в тому випадку коли відомий один або декілька символів паролю. Цей режим включає використання для порівняння паро-

лів символів масок у якості яких використовується символ „?”. В тих випадках, коли відомо, що в самому паролі мається символ „?” в масці необхідно змінити його на символ „*” , або „#”.

Атака за словником. Цей режим включає використання для порівняння готових паролів, які знаходяться в додатковому словнику. Використовується в тому випадку коли необхідно використати нейменше часу на знаходження паролю, але не завжди приводить до необхідного результату.

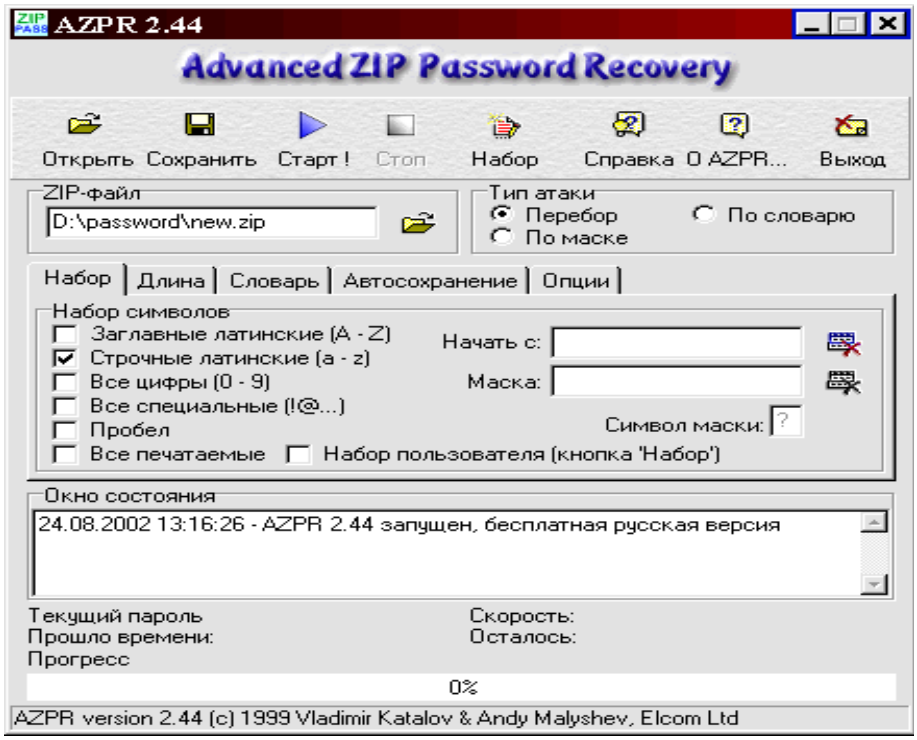


Рис. 5.1. Діалогове вікно програми Advanced ZIP Password Recovery

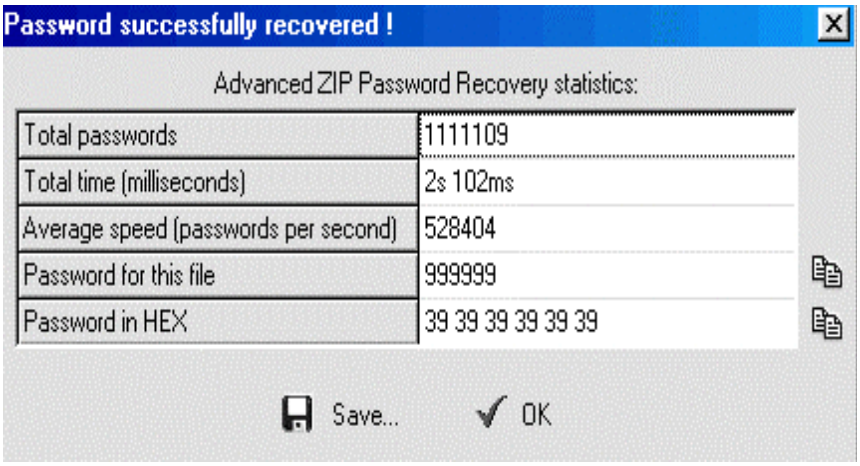


Рис. 5.2. Діалогове вікно результатів пошуку

Резервування систем інформації в Norton Ghost

Створення копій дисків, каталогів та файлів

Для запуску програми треба помістити Norton Ghost, який знаходиться на компакт-диску, у відповідний CD і перезапустити комп'ютер. Можливо також запустити Norton Ghost із панелі завдань за допомогою контекстного меню (рис. 5.3) або головного меню Windows.

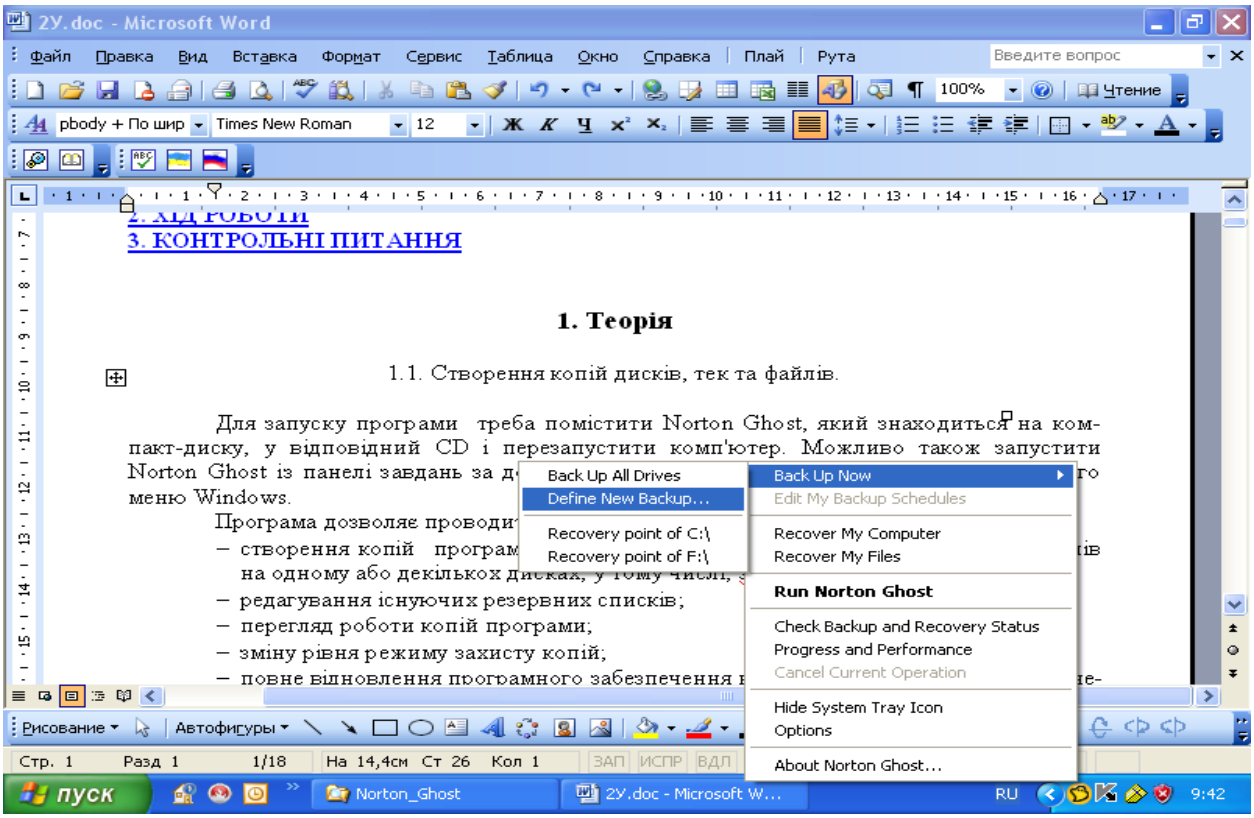


Рис. 5.3. Вікно виклику команд програми

Програма дозволяє проводити:

- створення копій програмного забезпечення комп'ютера, дисків, каталогів та файлів на одному або декількох дисках, зокрема, з'ємних;
- редагування існуючих резервних списків;
- перегляд роботи копій програми;
- зміну рівня режиму захисту копій;
- повне відновлення програмного забезпечення комп'ютера, зокрема, якщо непрацездатна операційна система;
- відновлення програмного забезпечення дисків;
- відновлення каталогів та файлів.

Початкове вікно програми (рис. 5.4-5.6) дозволяє мати доступ до:

Backup-резервна група: надає доступ до всіх ключових резервних особливостей програми, потрібного для конфігурування, планування й підтримки параметрів комп'ютера.

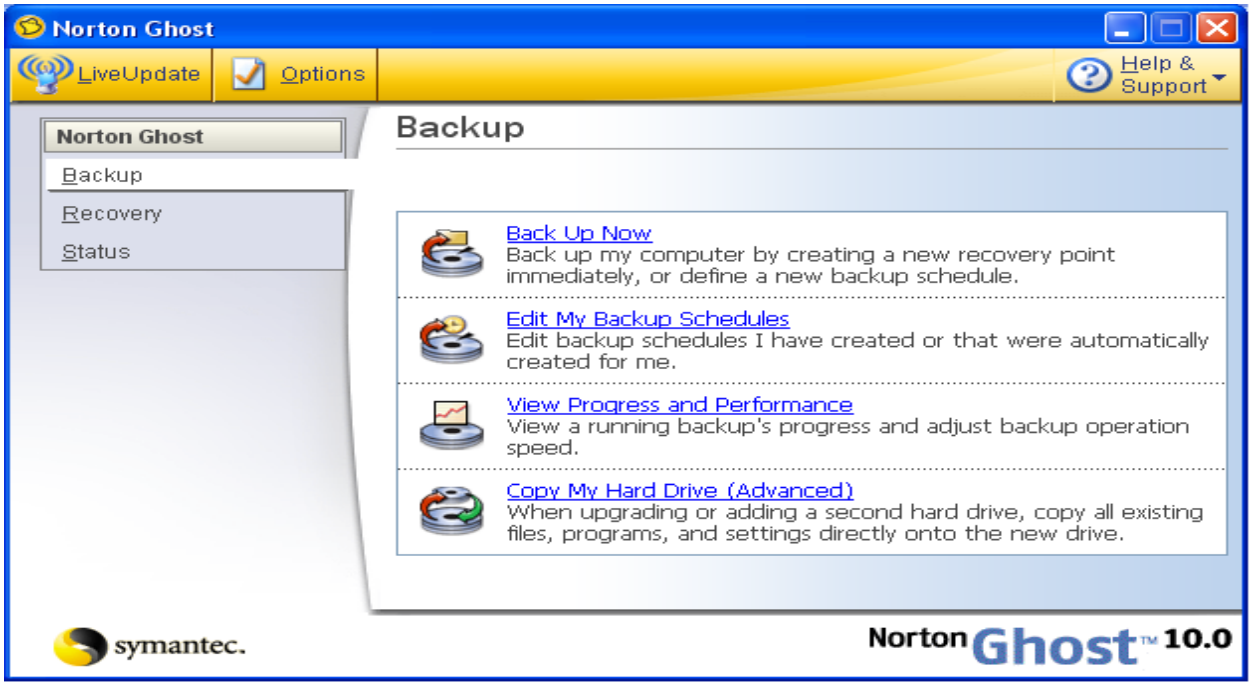


Рис. 5.4. Вікно резервної групи

Рис. 5.5. Вікно відновлення

Recovery-група оновлення: дозволяє відновити комп'ютер повністю до того стану (дати й часу, коли він працював нормально), відновити файли й каталоги, досліджувати, управляти, і оптимізувати пункти оновлення.

Status -група статусу: надає інформацію про копії вашого комп'ютера і статус захисту оновлення.

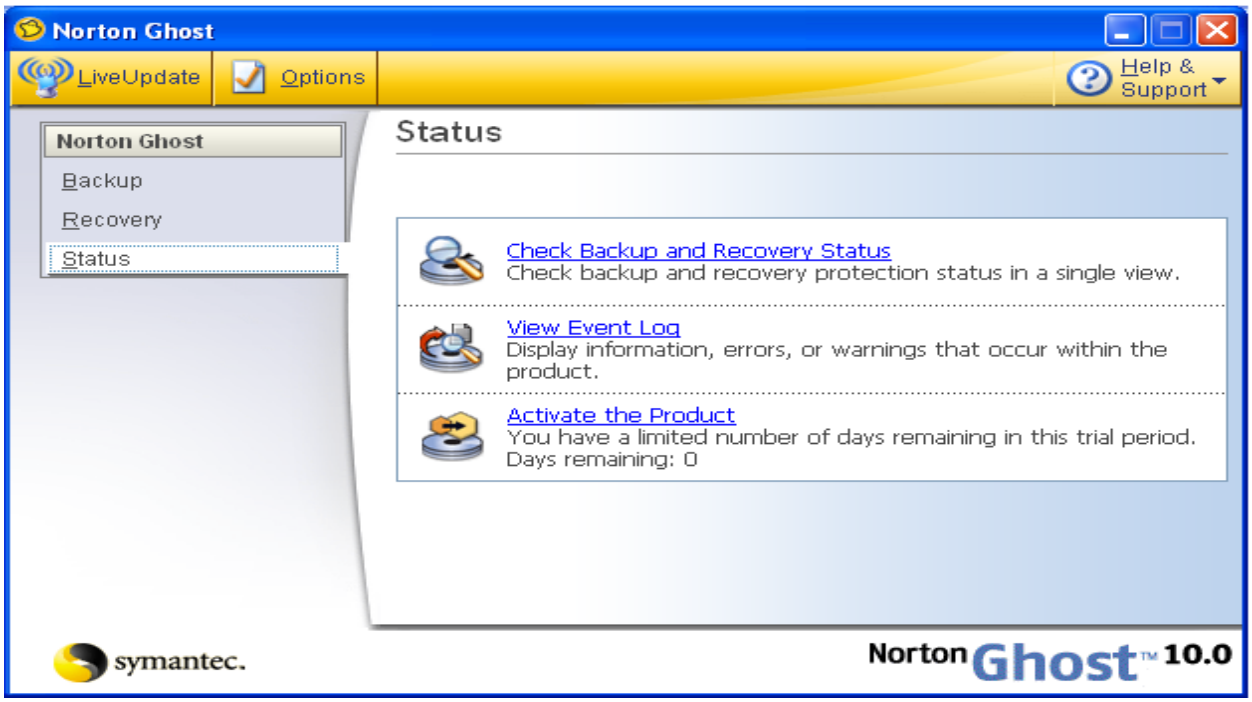


Рис. 5.6. Вікно статусу

Група Backup (рис. 5.2) надає доступ до наступних ключових резервних особливостей (табл. 5.1).

Таблиця 5.1

Короткий опис команд групи Backup.

Back Up Now	Відкриває список визначених в певний час копій.
Edit My Backup Schedules	Відкриває списки копій, де можна редагувати списки, які були автоматично визначені протягом початкової установки Norton Ghost.
View Progress and Performance	Показує параметри будь-якої копії,

	яка в зараз працює, й дозволяє регулювати виконавську швидкість створення копії. Якщо ви працюєте зі своїм комп'ютером і не хочете, щоб процес копіювання впливав на швидкість роботи комп'ютера, можна встановити резервну швидкість повільною, звільняючи більшість ресурсів комп'ютера.
Copy My Hard Drive (Advanced)	Коли потрібно встановити новий жорсткий диск (або другий жорсткий диск), ця команда копіює всі існуючі файли, програми, і параметри налагодження безпосередньо на новий диск.

Група Recovery надає доступ до наступних ключових резервних особливостей (табл. 5.2).

Таблиця 5.2

Короткий опис команд групи Recovery.

Recover My Computer	Відновлює комп'ютер до того дня і часу, коли він працював правильно.
Recover My Files	Відновлює файли або каталоги, які були втрачені, пошкоджені, замінені, або випадково видалені.
Explore Recovery Points (Advanced)	Дозволяє досліджувати файли і каталоги, що були запам'ятовані в існуючому пункті оновлення.
Optimize Recovery Point Storage	Оптимізує простір жорсткого диска, який використовується для зберігання пунктів оновлення комп'ютера.

Група Status надає доступ до наступних ключових резервних особливостей (табл. 5.3).

Таблиця 5.3

Короткий опис команд групи Status.

Check Backup and Recovery Status	Копія показів статусу захисту оновлення в єдиному вигляді.
View Event Log	Інформація показів, помилки, і попередження, які відбуваються в межах програми.
Purchase the Product	Указує, скільки залишилося днів протягом випробувального терміну, а також забезпечує легко інтерактивно доступ для придбання ліцензійної копії програми.

Діалогове вікно Options (рис. 5.7) включає чотири вкладки табл. 5.4, які дозволяють, налагодити параметри програми, що встановлюються за умовчанням:

Для оновлення програми достатньо подати команду **LiveUpdate** та за допомогою майстра оновлення отримати її через мережу Internet рис. 5.8. Адреса оновлення програми: http://www.symantec.com/partitionmagic.

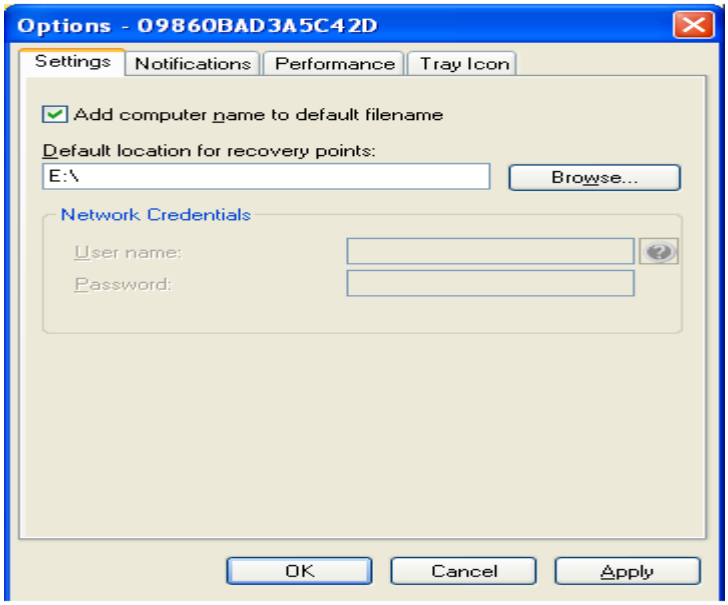


Рис. 5.7. Вікно налагодження

Таблиця 5.4

Короткий опис вкладок.

Таблиця	Опис
Settings	Указано де саме будуть створені копії.
Notifications	Показує історію дій Norton Ghost або повідомлень про помилки і попередження, можна вибрати збереження їх в реєстраційному файлі на комп'ютері, або, послати за електронною поштою.
Performance	Дозволяє конкретизувати задану за умовчанням швидкість для дублювання процесів оновлення.
Tray Icon	Можна встановити ярлик на панелі задач, або показати повідомлення про помилки, коли вони відбуваються, так і іншу інформацію, як, наприклад, завершення роботи програми.

Створення нової копії диска, каталоги або файлу

1. У групі Backup, увести команду **Back Up Now**.

2. У вікні **Back Up Now** введіть команду **Define New Backup** (рис. 5.9). З'явиться вікно майстра (рис. 5.10).

3. Клацніть кнопку **Next** у вікні майстра. У наступному вікні (рис. 5.11) виберіть диск, копія якого буде створюватися та клацніть кнопку **Next**. У наступному вікні (рис. 5.12) відберіть **Recovery point set** (набір пункту оновлення, він рекомендований за умовчанням, але не активний, якщо запущений один із процесів створен-

ня копії), або **Independent recovery point** (Незалежний пункт оновлення) та клацніть кнопку **Next**. У наступному вікні майстра (рис. 5.13)

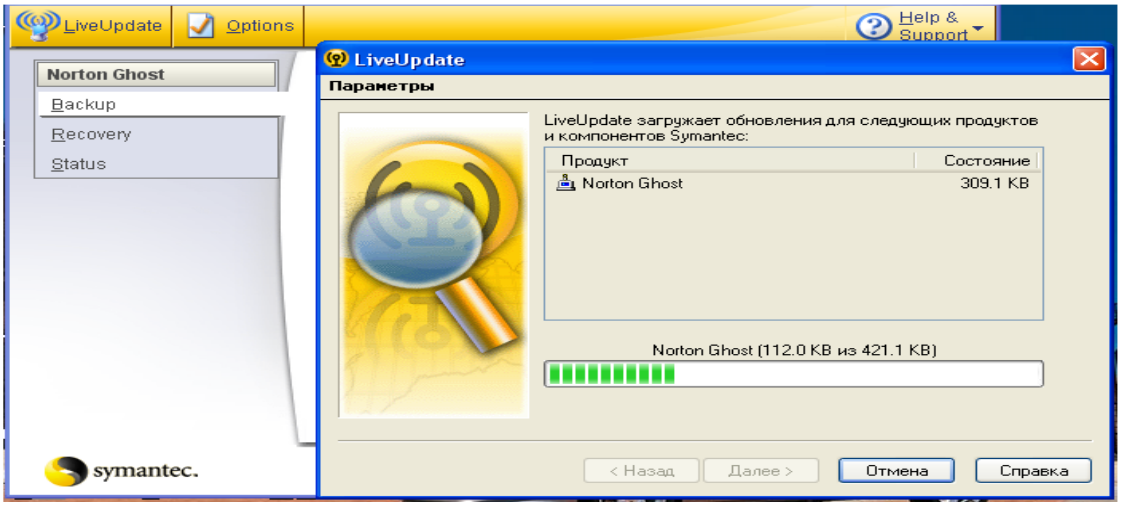


Рис. 5.8. Вікно оновлення програми

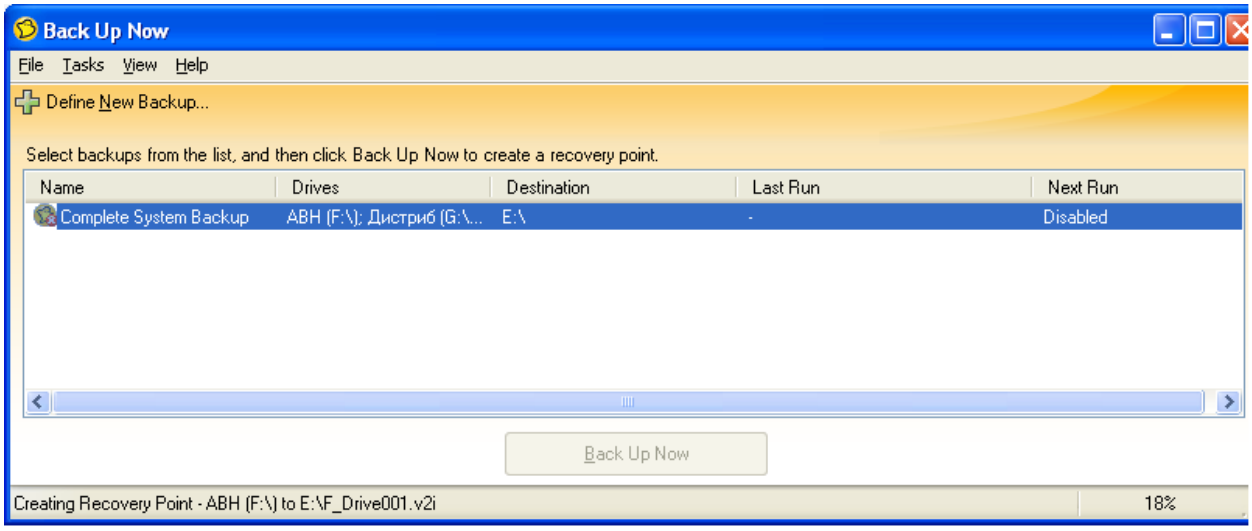


Рис. 5.9. Вікно Back Up Now

укажіть диск, каталог або файл із якого програма буде створювати копію (скористайтеся кнопкою **Browse**). Мається можливість перейменування диска (кнопка **Rename**), та вказання ступеня стиснення копії (без стиснення, низька степінь-стандартна, середня, висока)(вибір зі списка).

За допомогою кнопки **Advansed** можна встановити пароль (до 128 символів з ASCII) на копію (рис. 5.14). Має, можливість кодування пароля, та розбиття копії диска на декілька файлів з указанням їх розмірів, а також ігнорування несправних секторів на дисках.

Рис. 5.10 Вікно майстра створення копії

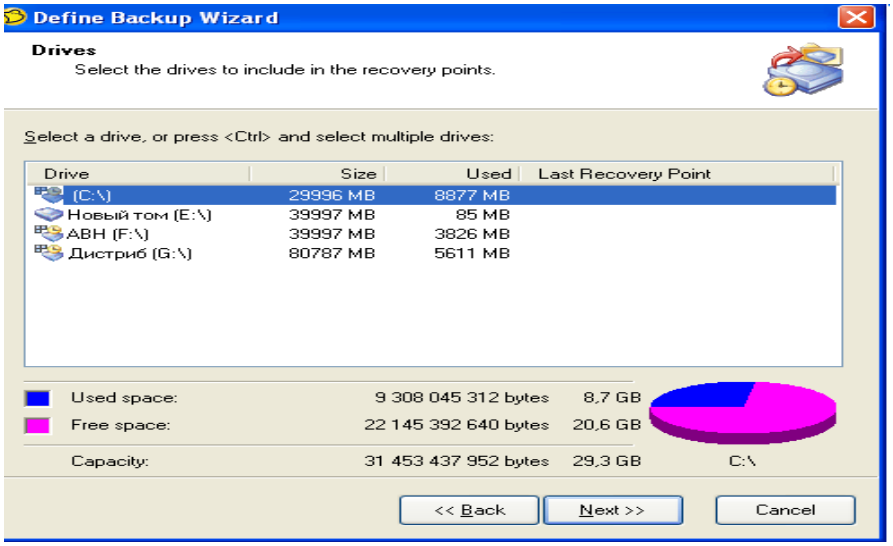


Рис. 5.11 Вікно відбору диска для створення копії

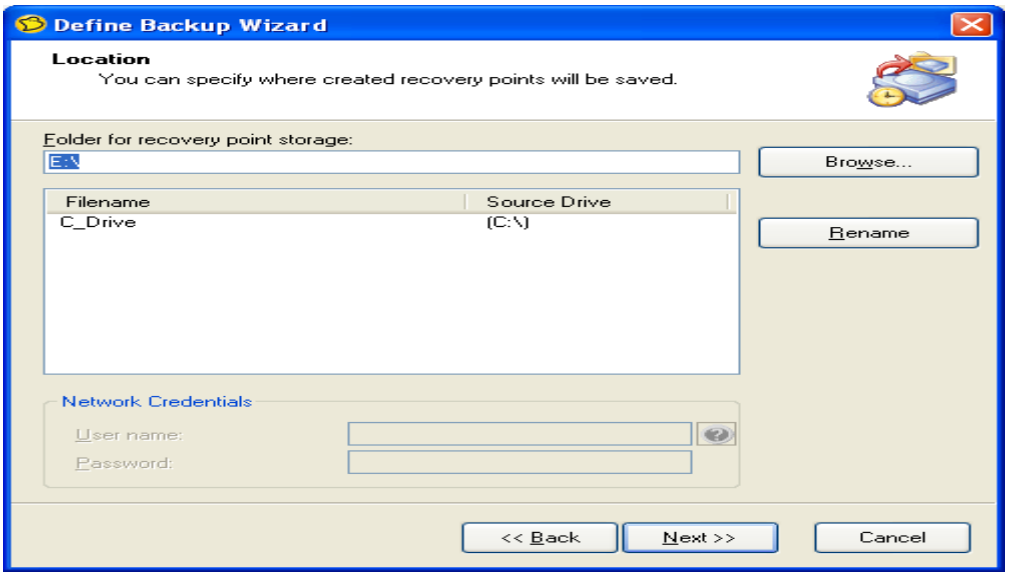


Рис. 5.12 Вікно відбору диска, каталогу або файлу для створення копії

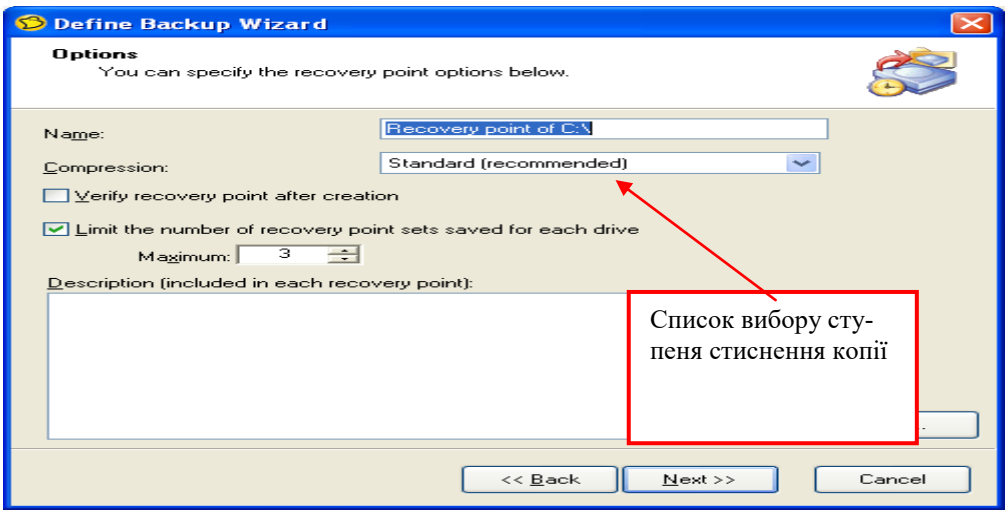


Рис. 5.13. Вікно відбору параметрів створення копії

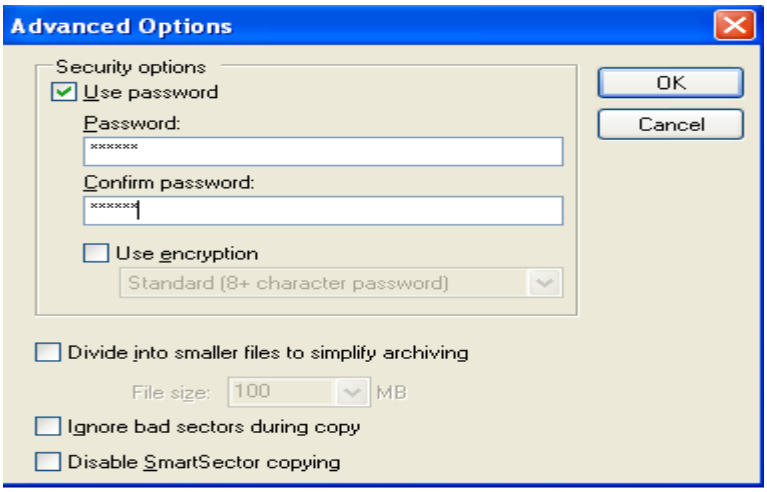


Рис. 5.14. Вікно встановлення пароля та відбору інших додаткових параметрів

Клацніть кнопку **Next**, після чого з'явиться нове діалогове вікно майстра (рис. 5.15) де можна відібрати режими **Manually** (one schedule) (уручну (не планується) або **scheduled** (планується). Якщо вибрати пункт **scheduled**, то можна вказати дату та час, коли буде проводитися створення копії. Клацніть кнопку **Next**, після чого з'явиться нове діалогове вікно майстра (рис. 5.16), де можна вказати **Create recovery point now** (Створіть пункт оновлення зараз) та натиснути кнопку **Finish**. Після закінчення процесу створення копій на вказаному диску з'являться нові файли-копії дисків (рис. 5.17).

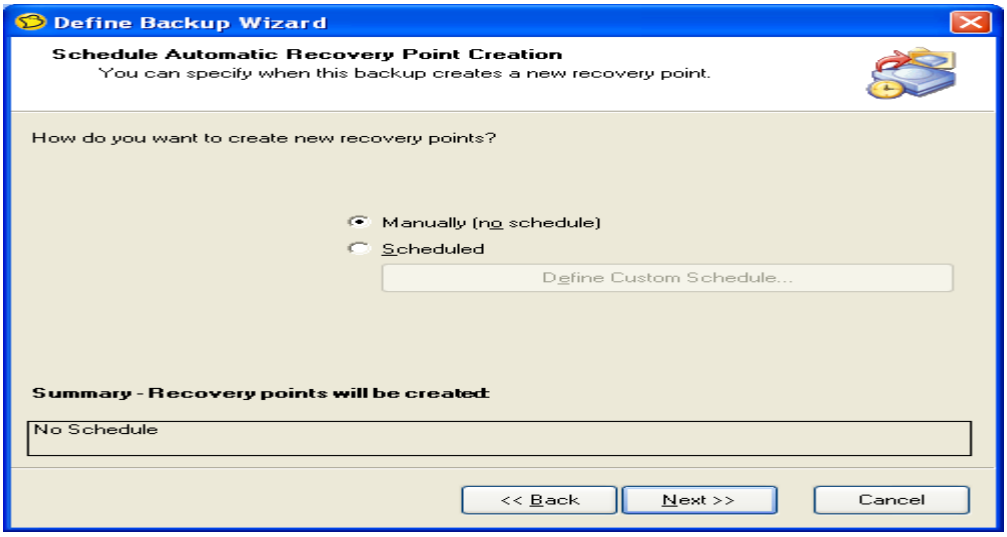


Рис. 5.15. Вікно відбору режиму копіювання

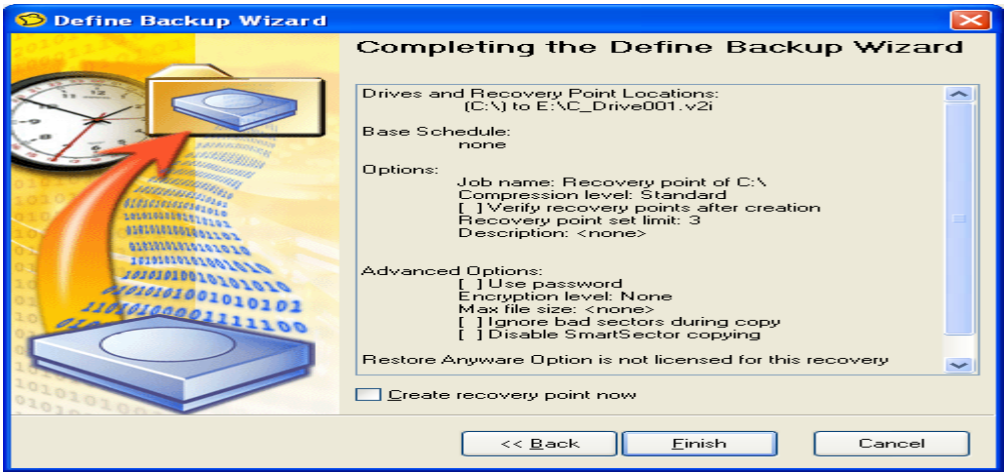


Рис. 5.16. Вікно перегляду параметрів копіювання

Під час створення копії іноді важливо задати швидкість роботи програми, якщо в цей час користувач працює з іншими програмами і т.п. Якщо встановити максимальну швидкість, то велика кількість ресурсів комп'ютера буде задіяна в процесі створення копії, що буде мішати нормальній роботі користувача. Для встановлення потрібної швидкості необхідно в групі Backup подати команду View Progress and Performance та перетягнути засувку на потрібне місце.

Перевірка копій під час збереження

У групі **Recovery** введіть команду **Recover My Files**. З'явиться діалогове вікно (рис. 5.18) Виділіть копію, яку треба перевірити та натис-

ніть кнопку **Browse Contents**

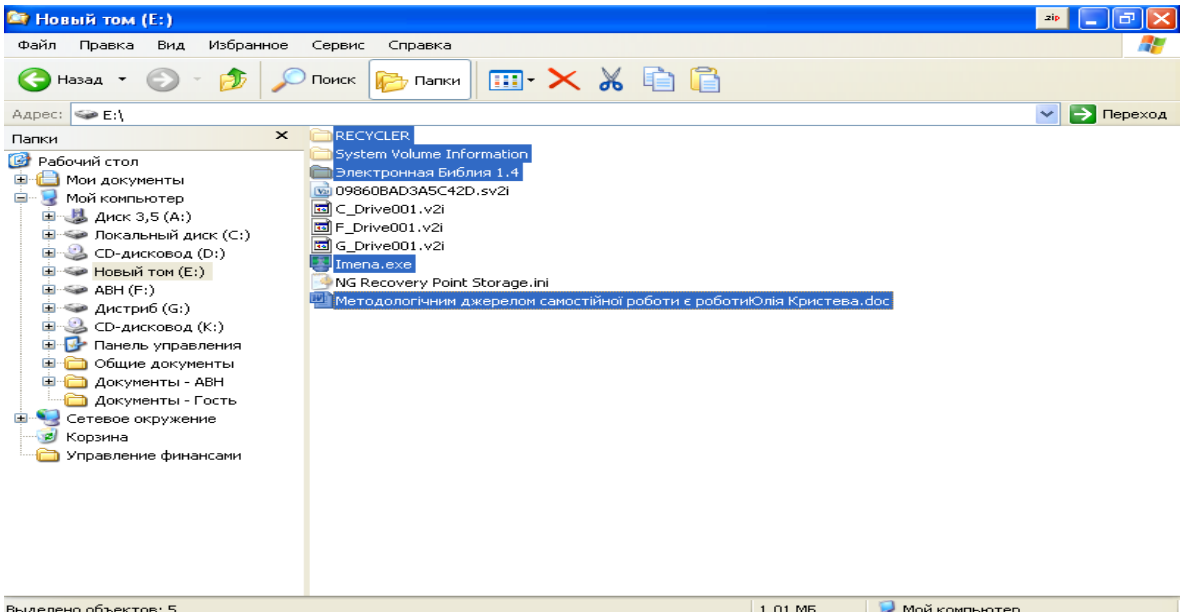


Рис. 5.17. Файли копії дисків

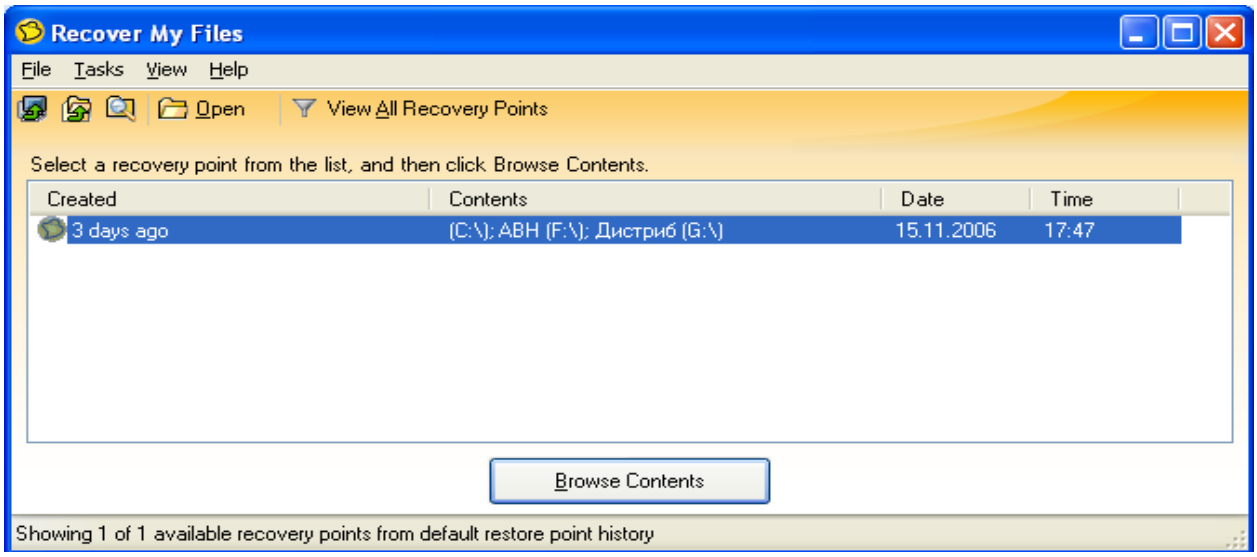


Рис. 5.18 Вікно перевірки копії диска

після чого можна перевірити дерево каталогів та файли (рис. 5.19), вибравши, наприклад, із контекстного меню відповідні команди (рис. 5.20).

Зміна рівня захисту копії

У групі **Status** введіть команду **Check Backup and Recovery Status** з'явиться діалогове вікно з копіями (рис. 5.21), відберіть потрібну копію та введіть команду **Add protection** для визову майстра (рис. 5.22), за допомогою якого на окремих кроках відбираються параметри захисту.

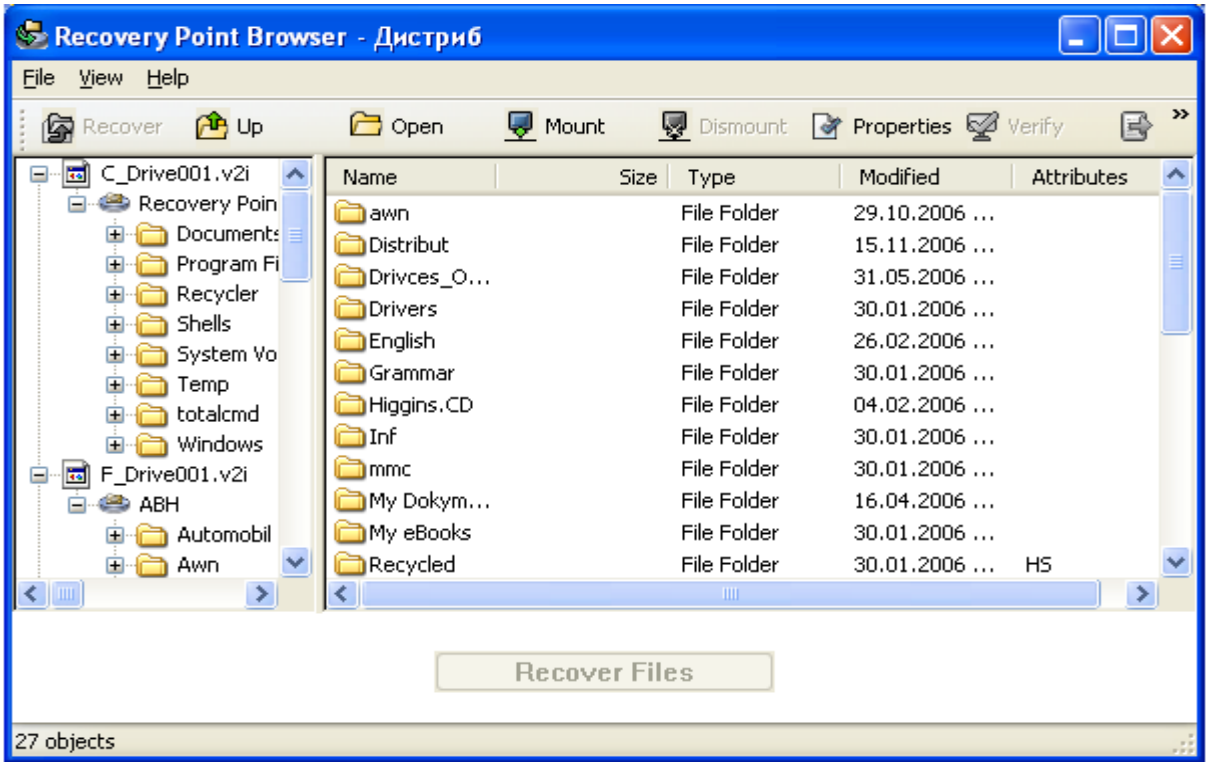


Рис. 5.19. Вікно дерева копії

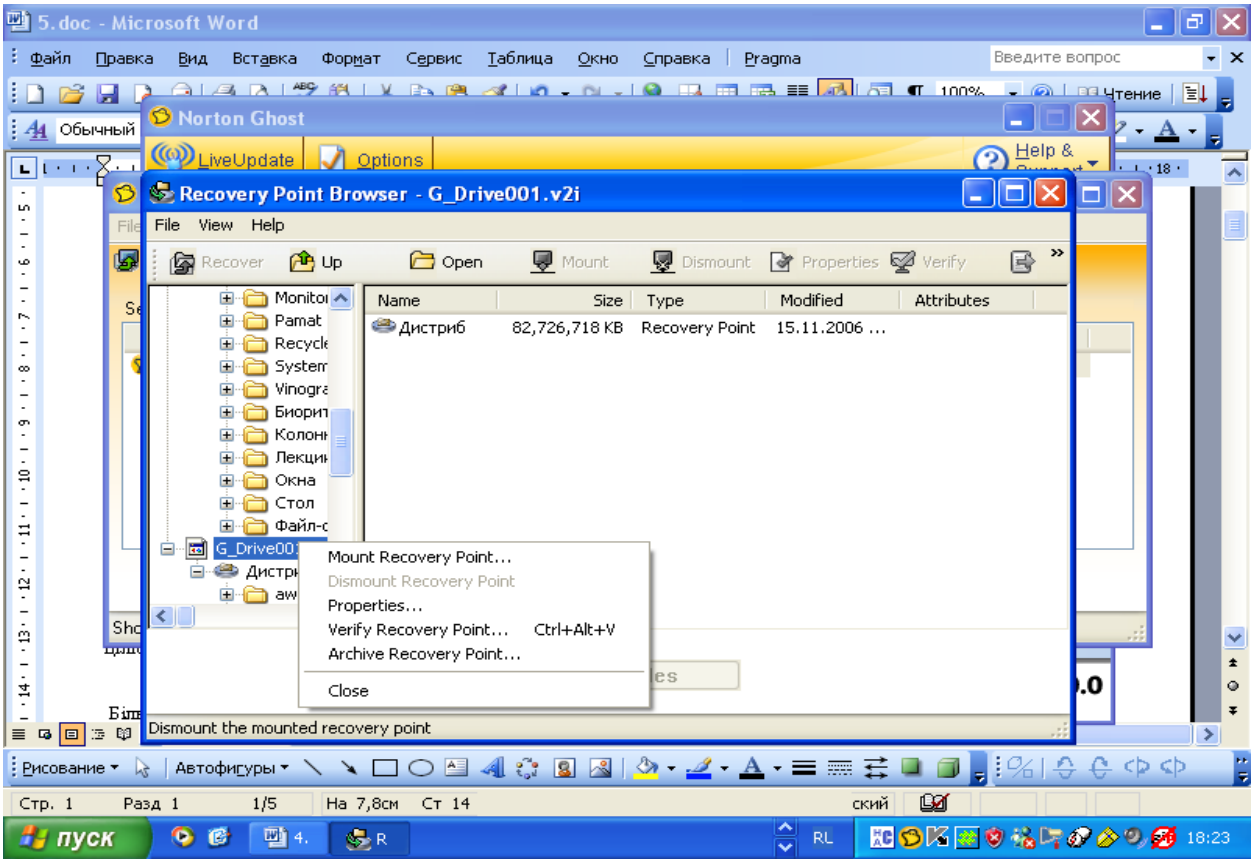


Рис. 5.20. Контекстне меню перевірки.

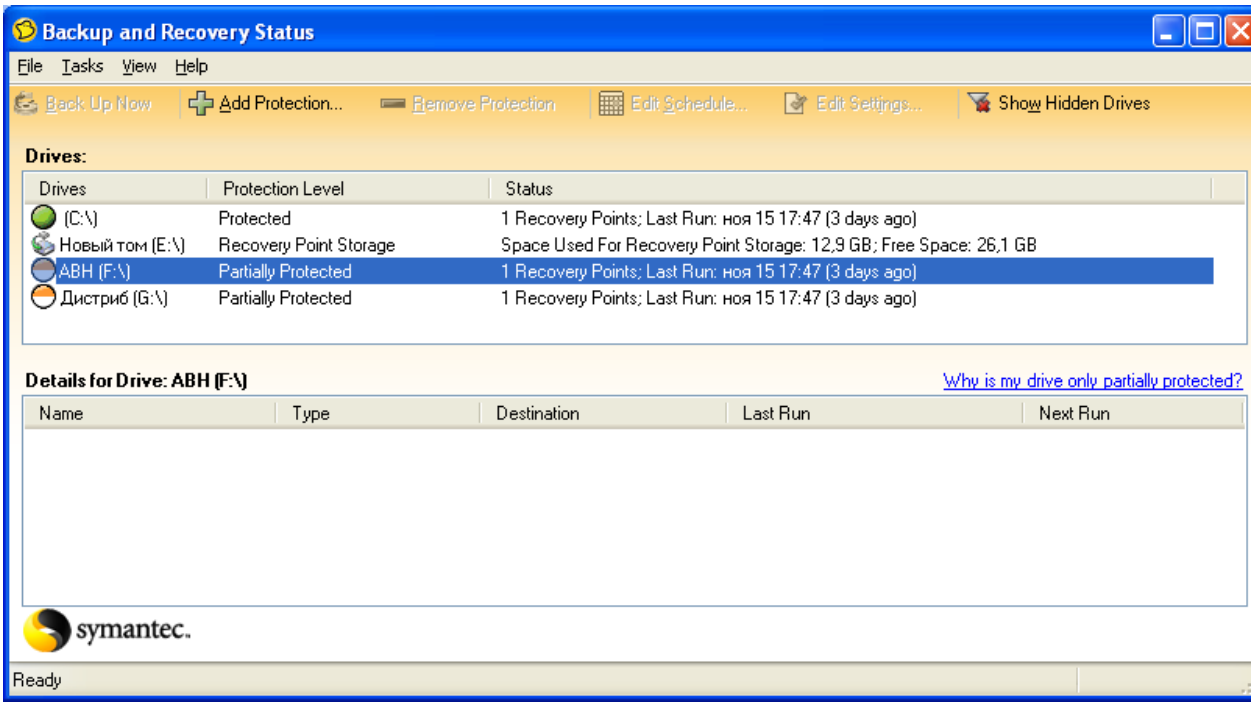


Рис. 5.21. Вікно відбору копії

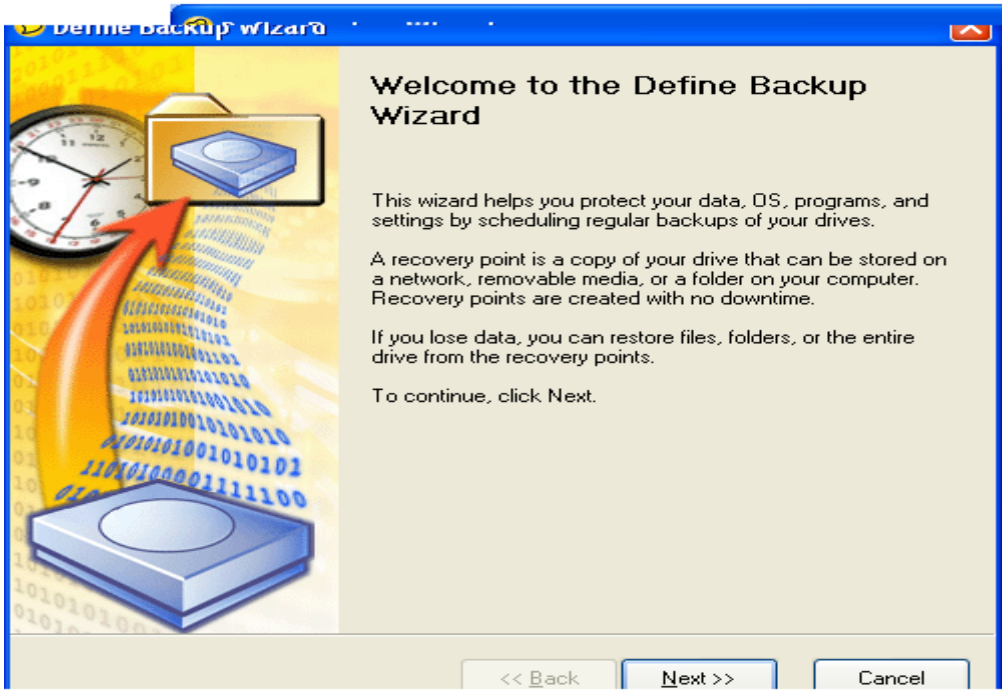


Рис. 5.22. Вікно майстра встановлення захисту

Визначення властивостей копії

У групі **Recovery** подайте команду **Explore Recovery Points** (Advanced) у вікні, що з'явиться (рис. 5.23) відберіть потрібну копію та в контекстному меню введіть команду **Properties** з'явиться вікно властивостей копії (рис. 5.24).

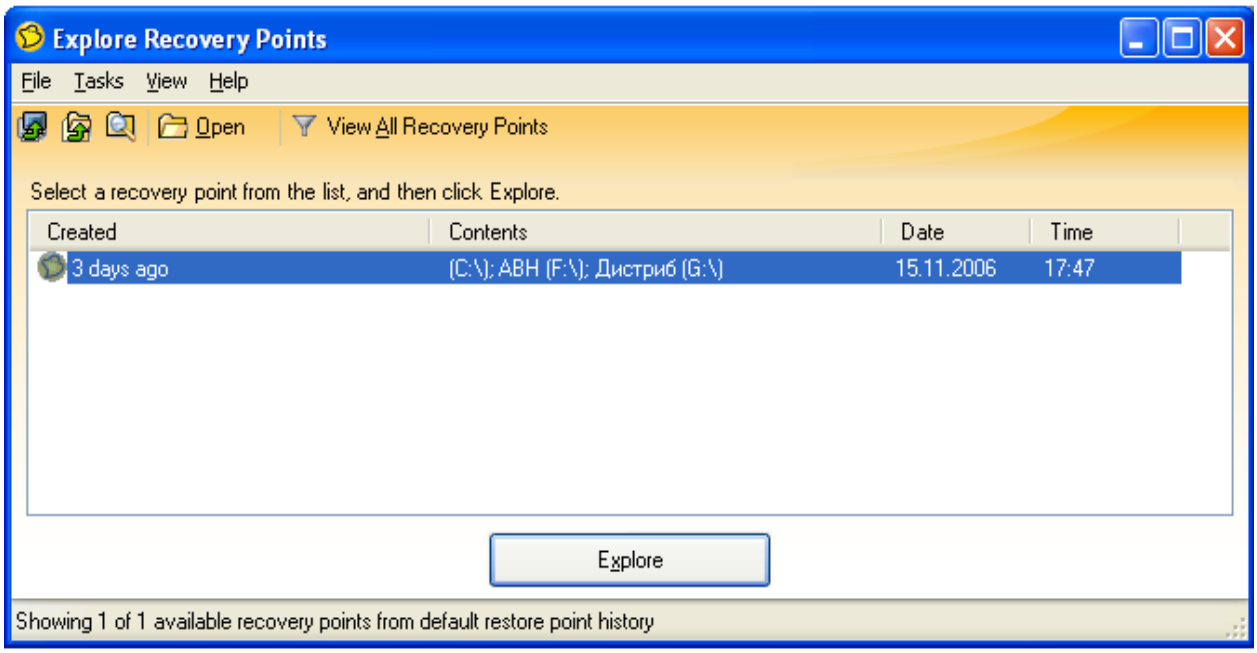


Рис. 5.23 Вікно відбору копії

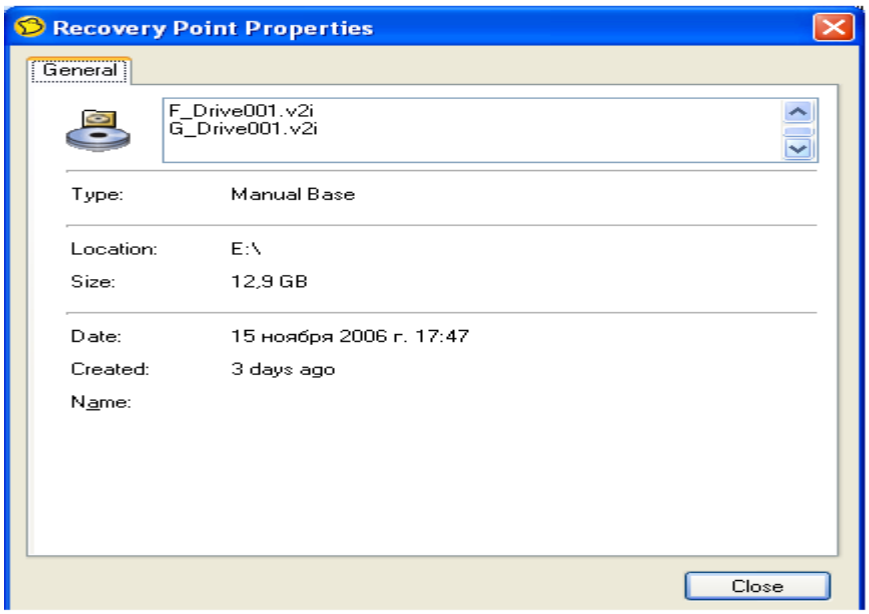


Рис. 5.24. Вікно властивостей копії

Видалення непотрібних копій

У групі **Recovery** ввести команду **Optimize Recovery Point Storage** з'явиться вікно (рис. 5.25),в якому необхідно відібрати копію для подальшого видалення та ввести команду **Delete Set** після чого необхідно підтвердити видалення копії (рис. 24),після чого програма виведе вікно остаточного видалення копії (рис. 5.26).

Оптимізація простору жорсткого диска, який використовується для зберігання пунктів оновлення комп'ютера

У групі **Recovery** введіть команду **Optimize Recovery Point Storage** з'явиться вікно (рис. 5.28) відберіть команду **Options** (правий нижній куток) та у

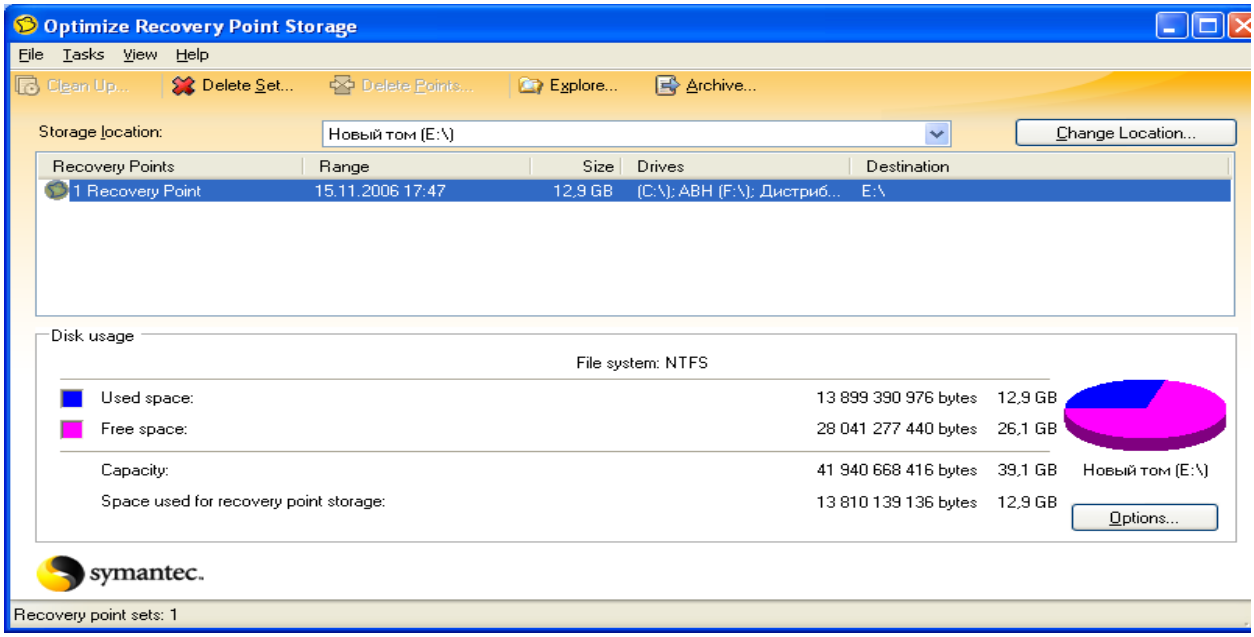


Рис. 5.25. Вікно відбору копії для видалення

Рис. 5.26. Вікно підтвердження видалення копії

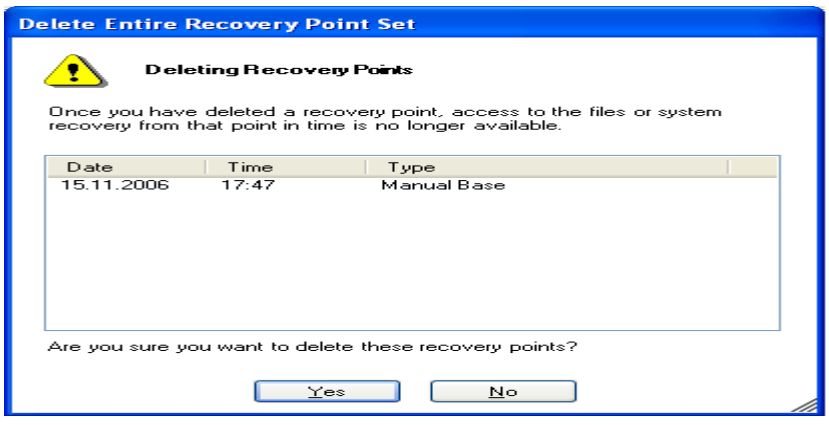


Рис. 5.27. Вікно остаточного видалення копії

вікні, що з'явиться (рис. 5.29) укажіть необхідні параметри. Якщо встановити автоматичне використання простору **Automaticaly optimise storade**, то при заповненні 90% вільного простору диску програма видасть попередження. Для ручного встановлення простору під копії на диску перетягніть у відповідне місце засувку.

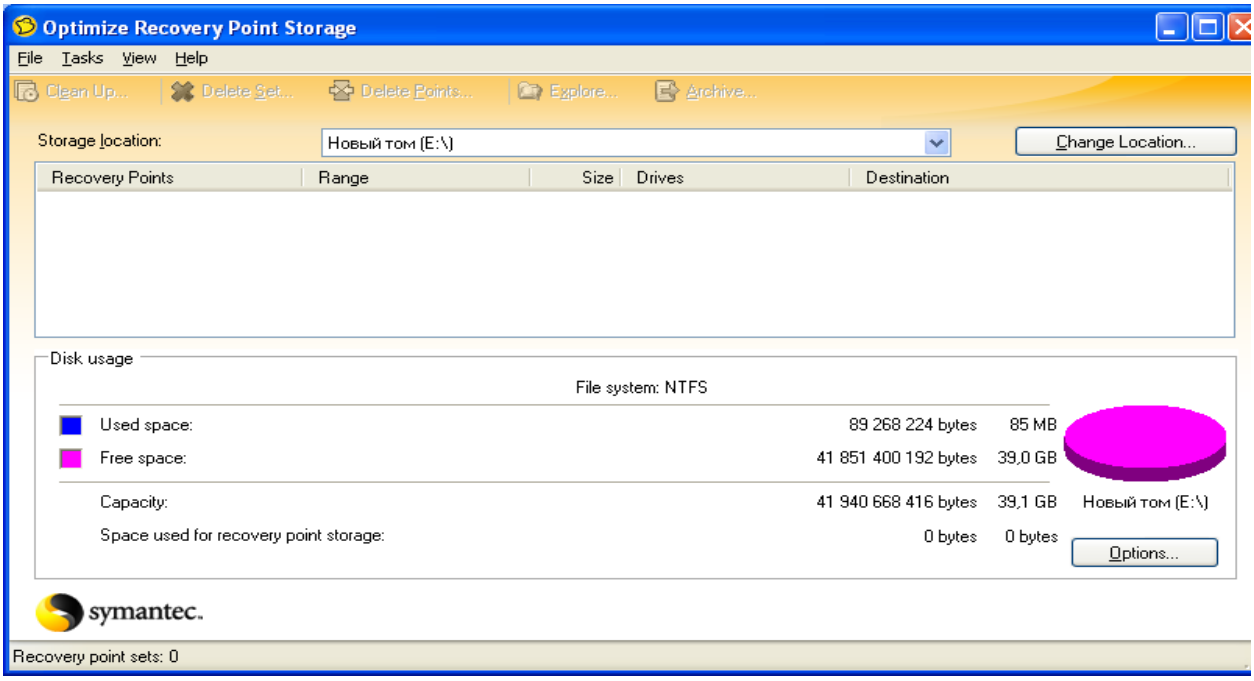


Рис. 5.28. Вікно Optimize Recovery Point Storage

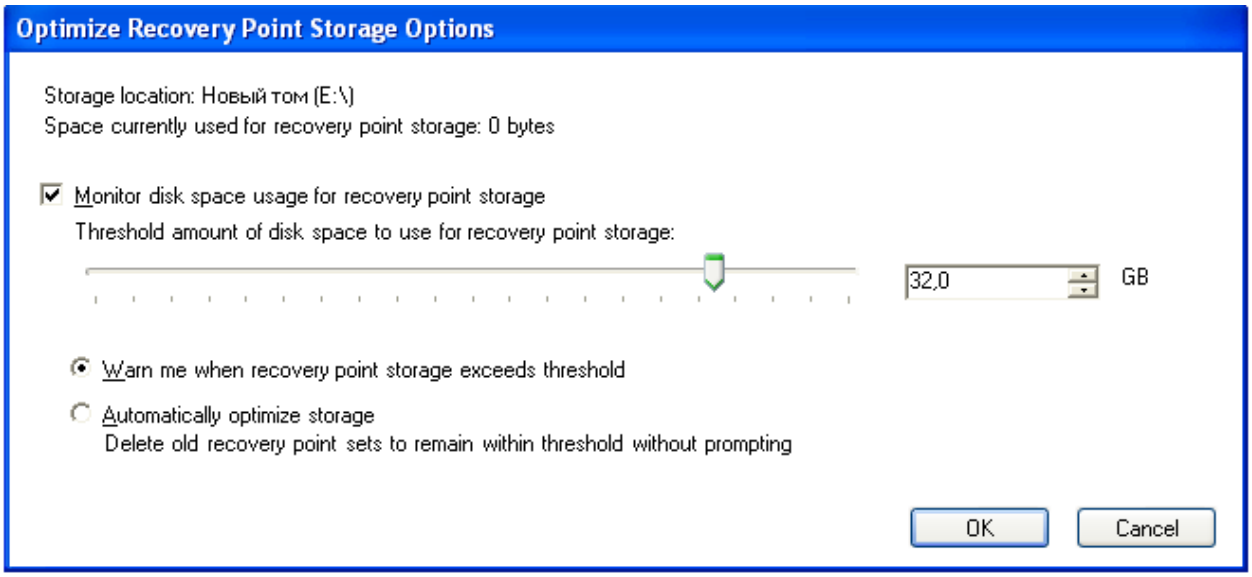


Рис. 5.29. Вікно відбору необхідних параметрів диска

Зміна місця розташування копій

У групі **Recovery** введіть команду **Optimize Recovery Point Storage** введіть команду **Change Location** у вікні, що з'явиться (рис. 5.30) необхідно вказати нове місце розташування копій (в тому числі змінні носії інформації та мережеві ресурси) і ввести команду **ОК**.

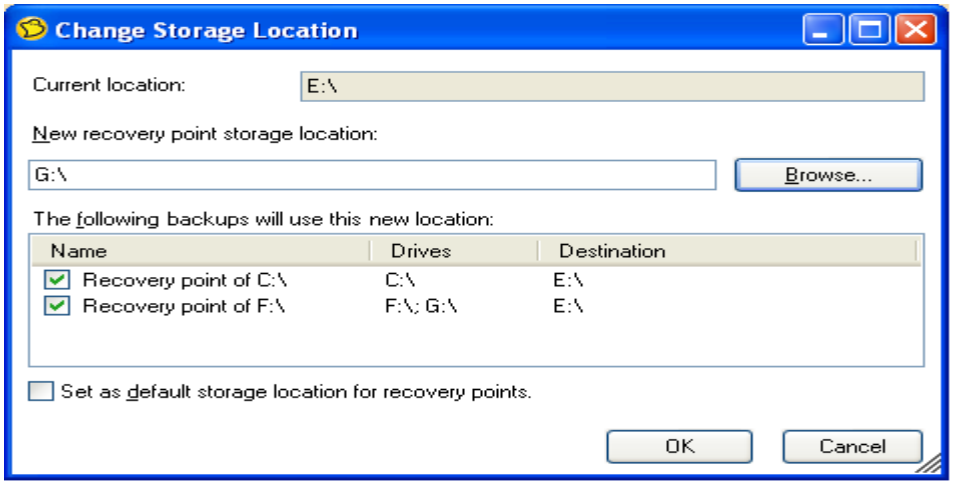


Рис. 5.30. Вікно відбору нового місця зберігання копій

Відновлення комп'ютера

Якщо відновлення системи відбувається з компакт-диска при неможливості запуску операційної системи, то необхідно мати щонайменше 256 МБ вільного простору в оперативній пам'яті комп'ютера. Установіть в BIOS завантаження з компакт-диск та встановіть диск із програмою в дисковод. Якщо причиною пошкодження системи комп'ютера був вірус, то програма надає можливість перевірки дисків на віруси та помилки (додаткова група **Аналіз програми**) перед відновленням системи. Відновлення системи можливе з мережевих дисків. Указану можливість широко використовують адміністратори мереж для відновлення. Для відновлення в групі **Recover** введіть команду **Recover My Computer** з'явиться діалогове вікно (рис. 5.31), відберіть у ньому потрібні копії та подайте команду **Recover My Computer**, у діалоговому вікні, що з'явиться (рис. 5.32) виберіть режими відновлення **Express** (автоматичне відновлення) та **Custom** (вибіркове відновлення). При виборі останнього з'явиться вікно майстра відновлення (рис. 5.33), за допомогою якого за кілька етапів його роботи можна відібрати потрібні параметри відновлення.

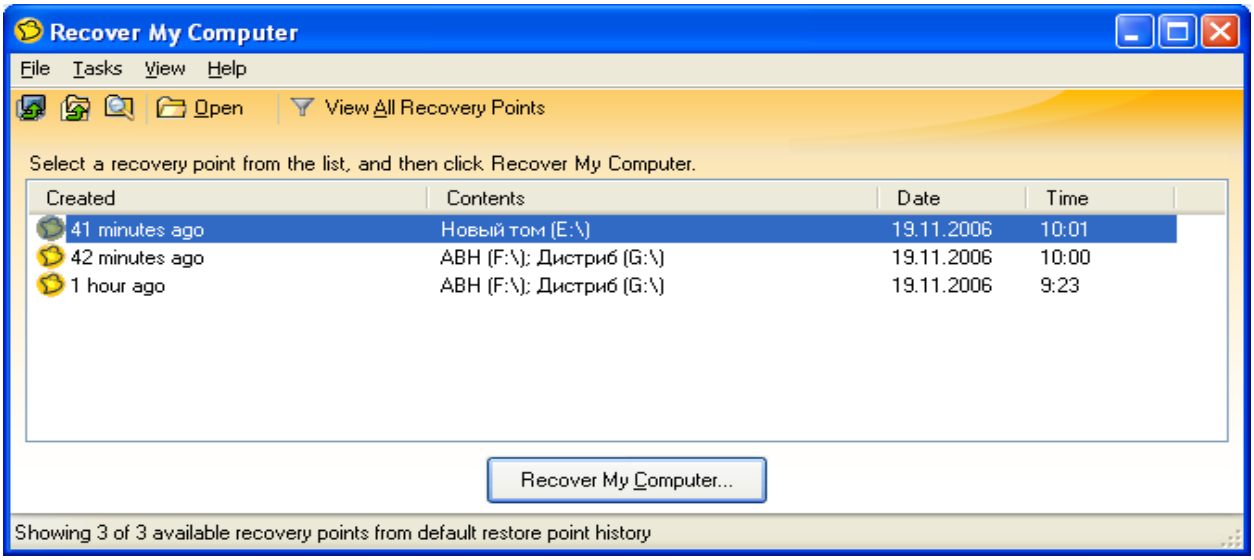


Рис. 5.31. Вікно відбору копій для відновлення комп'ютера

Рис. 5.32. Вікно відбору режимів відновлення комп'ютера

Рис. 5.33. Вікно майстра відновлення комп'ютера

Відновлення копій файлів та каталогів

У групі **Recover** введіть команду **Recover My Files** з'явиться діалогове вікно (рис. 5.34) виберіть пункт оновлення зі списку та введіть команду **Browse Contents**.

У вікні, що з'явиться (рис. 5.35) відберіть файли або каталоги, які треба оновити та введіть команду **Recover Files** та в наступному вікні (рис. 5.36) укажіть місце куди буде відновлювати програма файли та каталоги. Уведіть команду **Recover**.

Після введення команди програма почне процес відновлення (рис. 35) указаних файлів або каталогів на комп'ютері.

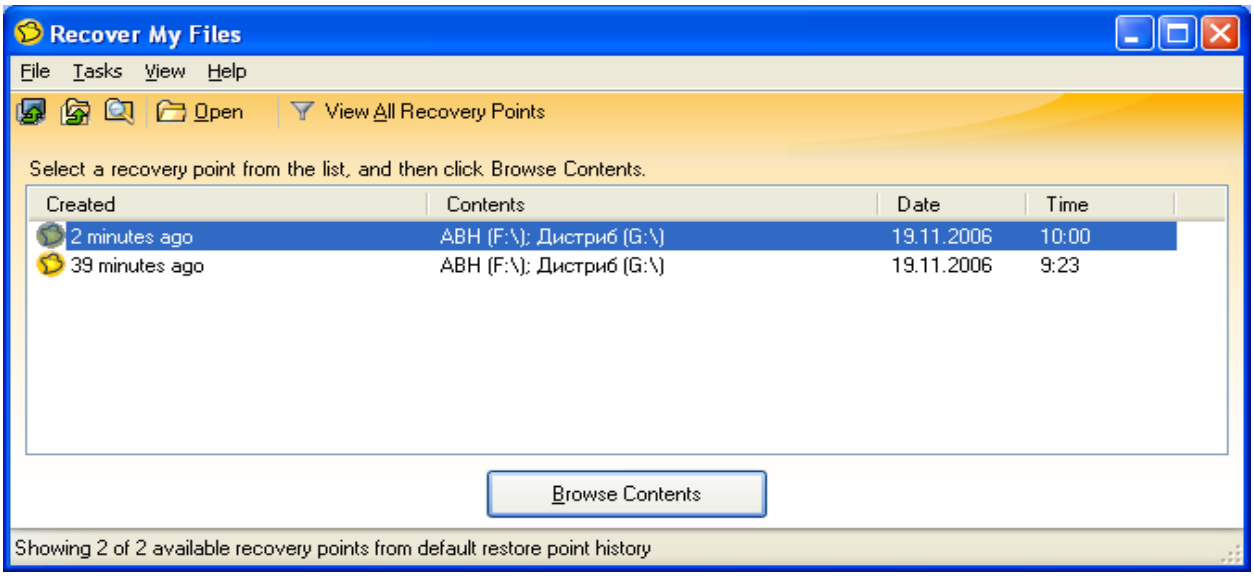


Рис. 5.34. Вікно Recover My Files

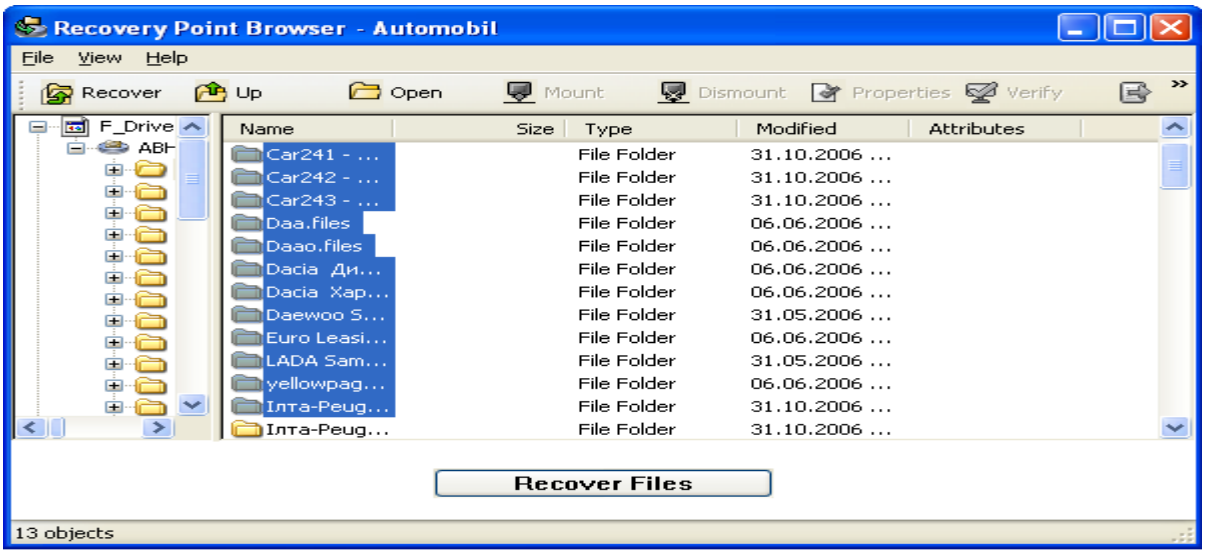


Рис. 5.35 Вікно відбору каталогів та файлів для оновлення

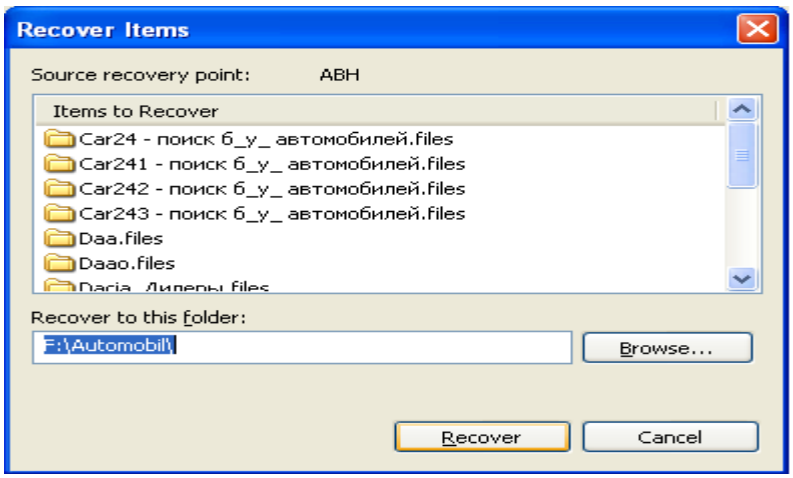


Рис. 5.36. Вікно указання місця відновлення файлів та каталогів

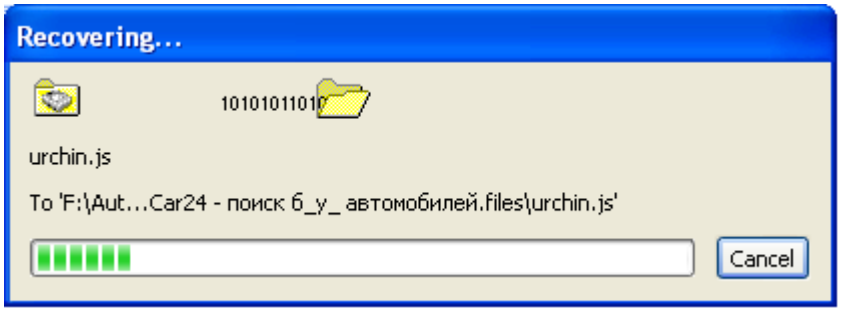


Рис. 5.37. Процес відновлення файлів та каталогів

Контрольні питання.

1. Порядок встановлення парольного захисту архівів.
2. Порядок пошуку паролів в архівах .
3. Порядок пошуку паролів в архівах із декількома файлами, які мають різні паролі.
4. Складові діалогово віконця програми Advanced ZIP Password Recovery.
5. Режими підбору паролів та їх характеристики.
6. Маски пошуку паролів.
7. Залежність часу пошуку паролю від його параметрів.
8. Призначення програми Norton Ghost.
9. Призначення команд групи Backup.
10. Призначення команд групи Recover.
11. Призначення команд групи Status.
12. Діалогове вікно Options.
13. Послідовність створення копії диска.

14.Послідовність створення копії каталоги.

15.Послідовність створення копії файлу.

16.Як провести перевірку копій під час збереження?

17.Як провести зміну рівня захисту копії?

18.Як переглянути властивості копії?

19.Як проводиться видалення непотрібних копій?

20.Як проводиться оптимізація простору жорсткого диска, який використовується для зберігання пунктів оновлення комп'ютера?

21.Як проводиться зміна місця розташування копій?

22.Як проводиться відновлення комп'ютера?

23.Як проводиться відновлення копій файлів та каталогів

Розділ 6.
ВІДНОВЛЕННЯ ТА ВИДАЛЕННЯ ІНФОРМАЦІЇ.

Тестування дисків та відновлення даних на дисках, які попередньо видалені, або видалені при форматуванні із використанням програми Easy Recovery Professional.

Тестування дисків

Ця програма дозволяє користувачеві робити діагностику дисків, відновлювати файли та каталоги, які були випадково видалені, або знищенні під час форматування дисків.

При запускові програми з'явиться діалогове вікно, яке має на панелі програми головні компоненти (див. рис. 6.1).

Рис. 6.1. Вікно запуску програми

Компонента Disk Diagnostics Contents

Забезпечує системою діагностичних інструментів (рис. 6.2). Інструменти, включені в цю категорію розроблені, для того, щоб швидко визначити, має система проблеми з апаратними засобами ЕОМ або на диску проблеми файлової структури. Усі інструменти в цій категорії роблять детальне повідомлення про систему.

Рис. 6.2. Вікно інструментів Діагностики Диска

Компоненти Діагностики Диска:

- DriveTests (тестування дисків);
- JumperViewer (перегляд джемпера);
- PartitionTests (випробовування розділу);
- SizeManager (менеджер розміру);
- SMARTTests (шикарні(сильні) випробовування);
- DataAdvisor (Радник Даних) ;

Інструмент (майстер) DriveTests дозволяє перевіряти фізичний стан диска. Є можливість вибрати для одночасного дослідження одразу декілька дисків.

Наступні випробовування, доступні в DriveTests інструменті (рис. 6.3).

У процесі вибору можливе встановлення:

- Швидкого Діагностичного Іспиту;
- Повного Діагностичного Іспиту.

Якщо диск не знайдений у списку, перевірте, що кабель нагромаджувача на твердих дисках зв'язаний належним чином, і призначення джемпера диска правильні. JumperViewer програмне забезпечення може допомогти із джемпером, для дисків ATA/IDE.

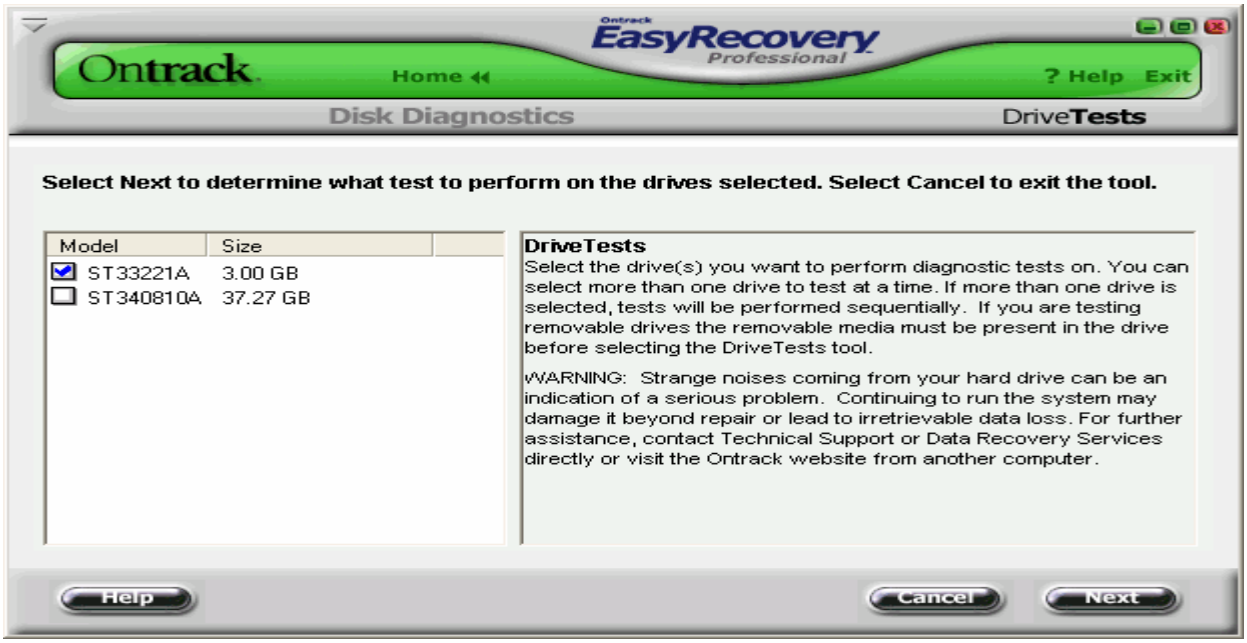
Мається можливість вибору, щоб керувати одним випробовуванням одночасно на кожному відібраному диску, швидко визначати, або має нагромаджувач на твердих дисках, серйозні фізичні проблеми. Для цього вибиріть -- **Швидкі Діагностичні випробовування**. Щоб виконувати великий, детальний перегляд вашого нагромаджувача на твердих дисках, виберіть **Повний Діагностичний Іспит**.

Приклад результатів швидкого дослідження диска наведений на рис. 6.4.

Швидкий Діагностичний Іспит визначить, з 90-процентною впевненістю, у 90 секунд, чи має ваш твердий диск фізичну проблему.

Повний Діагностичний іспит перевірить нагромаджувач на твердих дисках, що має фізичні проблеми типу нечитабельних секторів. Якщо немає впевненості щодо фізичної стабільності твердого диска, виберіть -- Повний **Діагностичний іспит.**

SMARTTests– іспит для самоконтролю, аналізу і Reporting Технологія. SMARTTests запобігає втраті даних, пророкуючи можливі відмови диска, використовуючи спеціальні алгоритми, убудовані в програмувальне устаткування нагромаджувача на твердих дисках. Самі нові IDE і SCSI нагромаджувачі на твердих дисках підтримують SMARTTests технологію.



РРис. 6.3. Вікно майстра вибору дисків та режимів дослідження дисків.

Компонента SMARTTests

Включає три, окремі діагностичні іспити:

- **SMARTTests іспит** -- виконає швидку перевірку статусу нагромаджувача на твердих дисках, за кілька секунд;
- **короткий SMARTTests іспит** – проводить швидку перевірку (приблизно 90 секунд) диска. Цей іспит, убудований у програмне устаткування диска і розроблений (призначений) для того, щоб швидко ідентифікувати головні внутрішні пошкодження диску;
- **розширений SMARTTests іспит** – проведе всебічну перевірку твердого диска. Цей іспит також убудований у програмне устаткування нагромаджувачів на твердих дисках і розроблений, щоб знайти незначні внутрішні проблеми або непогодженості з вашим диском.

Для перевірки дисків необхідно:

1. Вибрати диск, на якому потрібно виконати SMARTTests іспит. Іспитові результати будуть показані, коли іспити повні. Мається можливість вибору більше ніж одного диска одночасно. Якщо більше ніж один диск відібраний, іспити будуть виконані послідовно.

2. Вибрати тип SMARTTests іспиту на відібраних дисках.

Компонента PartitionTests

У деяких випадках, у той час як диск не може мати ніяких фізичних проблем, він може мати на диску проблеми файлової структури. PartitionTests інструмент розроблений, щоб аналізувати на диску структуру файлової системи. При перевіці файлової системи перевіряють цілісність даних розділів NTFS і FAT. Час іспитів залежить від розміру розділу та числа файлів у розділі.

Для перевірки диска виберіть розділ, який буде перевірятися (рис. 6.5). Про будь-які знайдені помилки файлової структури будуть повідомлення на екрані.

Компонента DataAdvisor

Це діагностичний інструмент розроблений для оцінки стану комп'ютерної системи. **Радник Даних** швидко оцінює “здоров'я” диска, структуру файлової систе-

ми, і комп'ютерної пам'яті, вказуючі на проблеми, які можуть привести до втрати даних. Цей усебічний діагностичний інструмент може використовуватися,

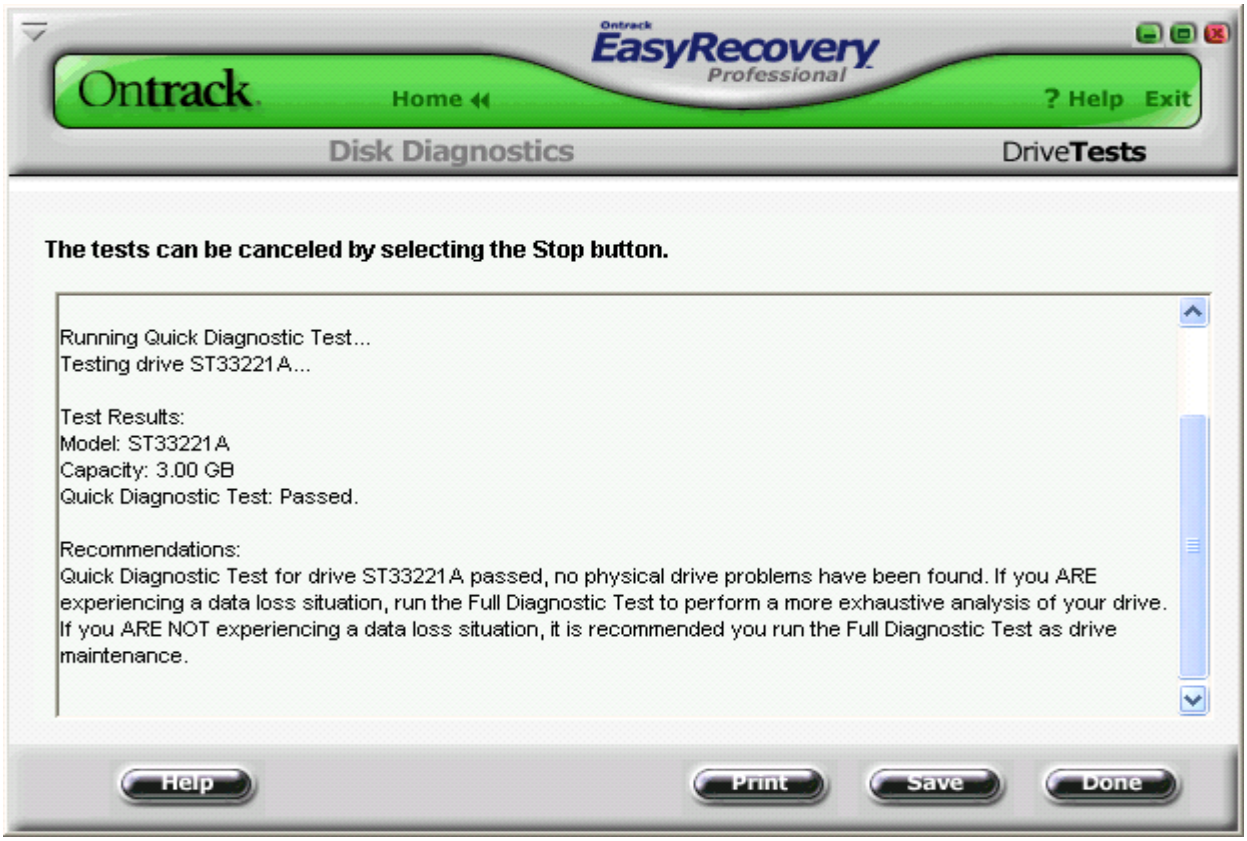


Рис. 6.4. Вікно результатів дослідження диска

щоб діагностувати поточні проблеми і як частина правильної програми обслуговування, для ідентифікування потенційних проблем, які могли вести до втрати даних. Якщо потенційні проблеми ідентифіковані, буде надано програмою час для того, щоб зробити виправлення та уникнути майбутніх втрат.

При виборі **DataAdvisor** , програма дозволить проводити:

- **Швидкий функціональний іспит** - читає й прагне на твердому диску перевіряти катастрофічні фізичні проблеми;
- **SMARTTests перевірку** - повідомляє щодо будь-яких пошкоджень;
- **Іспит структури файлу** - читає й перевіряє цілісність файлової структури, наприклад, таблиць FAT, визначає критичні сектори;
- **Іспит пам'яті системи** - здійснює і перевіряє цілісність пам'яті в комп'ютерній системі і виявляє дефекти й помилки.

Компонента Ontrack JumperViewer

Це графічний, діалоговий апплет для того, щоб швидко знайти розміщення джемпера для IDE/ATA нагромаджувачів на твердих дисках. База даних включає останні версії головних виготовлювачів дисків та може оновлюватися.

Оновлення програми відбувається за адресою:

http://www.ontrack.com/jumperviewer/jumperviewerhelp.asp

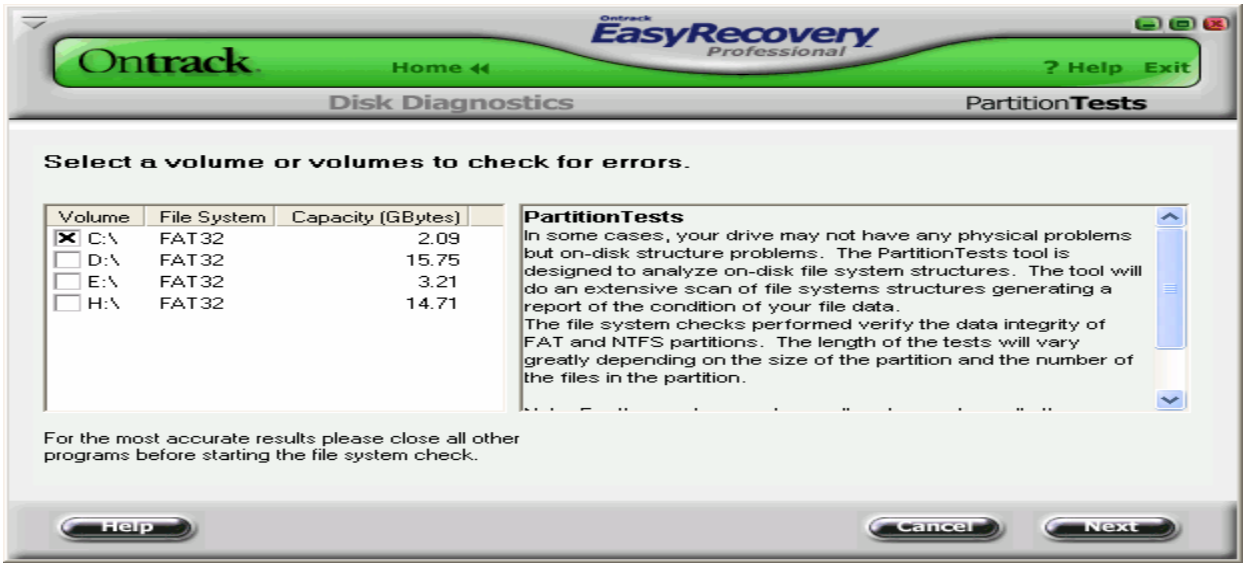


Рис. 6.5. Вікно майстра діагностики

Компонента SizeManager

Показує степінь використання диска в комп'ютерній системі. SizeManager надає миттєве графічне представлення того, де і як використовується місце на комп'ютері (рис. 6.6), полегшує визначення місцезнаходження негабаритних каталогів і файлів. SizeManager допомагає визначати, які файли захаращують місце в системі.

Категорія Data Recovery

Включає інструменти відновлення (рис. 6.7), файлів та каталогів. Інструменти Відновлення даних повернуть файли FAT і розділів NTFS. Інструменти розроблені, щоб повернути і копіювати дані до іншого призначеного типу змінного диска, іншого нагромаджувача на твердих дисках, гнучкої дискети, або диску мережі.

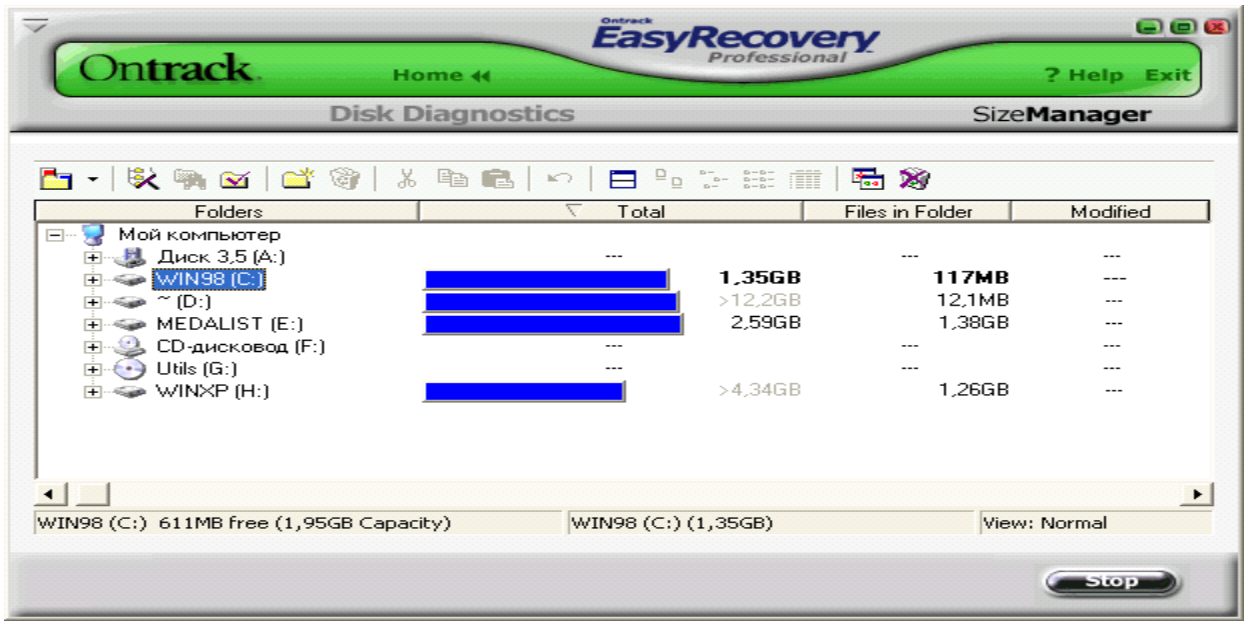


Рис. 6.6. Вікно SizeManager

Рис. 6.7. Вікно відновлення файлів, каталогів

Кожен інструмент – це майстер, який веде користувача через три простих кроки та дозволяє:

1. **Оцінити** - інструмент ідентифікує всі пристрої або розділи в системі і показує графічне представлення того, що було знайдено.

2. **Відтворити** - інструмент досліджує структури файлу, що залишаються у розділі, і будує дійсну (віртуальну) файлову систему в пам'яті.

3. **Відновити** – файли та каталоги, створити їх копії до безпечного місця розташування.

Інструменти Відновлення Даних:

- AdvancedRecovery (Просунуте відновлення);
- DeletedRecovery (Вилучене відновлення);
- FormatRecovery (Відновлення формату);
- RawRecovery (Попереднє відновлення);
- ResumeRecovery (Відновлення резюме);
- EmergencyDiskette (Надзвичайна дискета).

Основні Кроки Відновлення

Усі інструменти в категорії Відновлення даних мають подібні кроки в процесі відновлення:

- Вибір розділу;
- Перегляд файлової структури;
- Відбір файлів та каталогів для відновлення;
- Вибір параметрів відновлення;
- Створення копій на вказаному розділі;
- Резюме відновлення.

Компонента AdvancedRecovery

Для самого важкого відновлення призначена компонента , AdvancedRecovery інструмент (рис.6.8), яка забезпечує просунутими варіантами відновлення, включаючи, проблеми повернення файлів та каталогів при помилковому вилученні з розділу, вірусні напади, і інших помилок та пошкоджень файлової системи. Інструмент забезпечує детальне графічне представлення дисків, зв'язаних із системою, включаючи розділи, зв'язані з кожним пристроєм.

Список видалених файлів представлений на рис. 6.9. Вікно вибору диска, куди будуть записані відновлені файли, представлене на рис. 6.10. Вікно результатів відновлення файлів представлене на рис. 6.11.

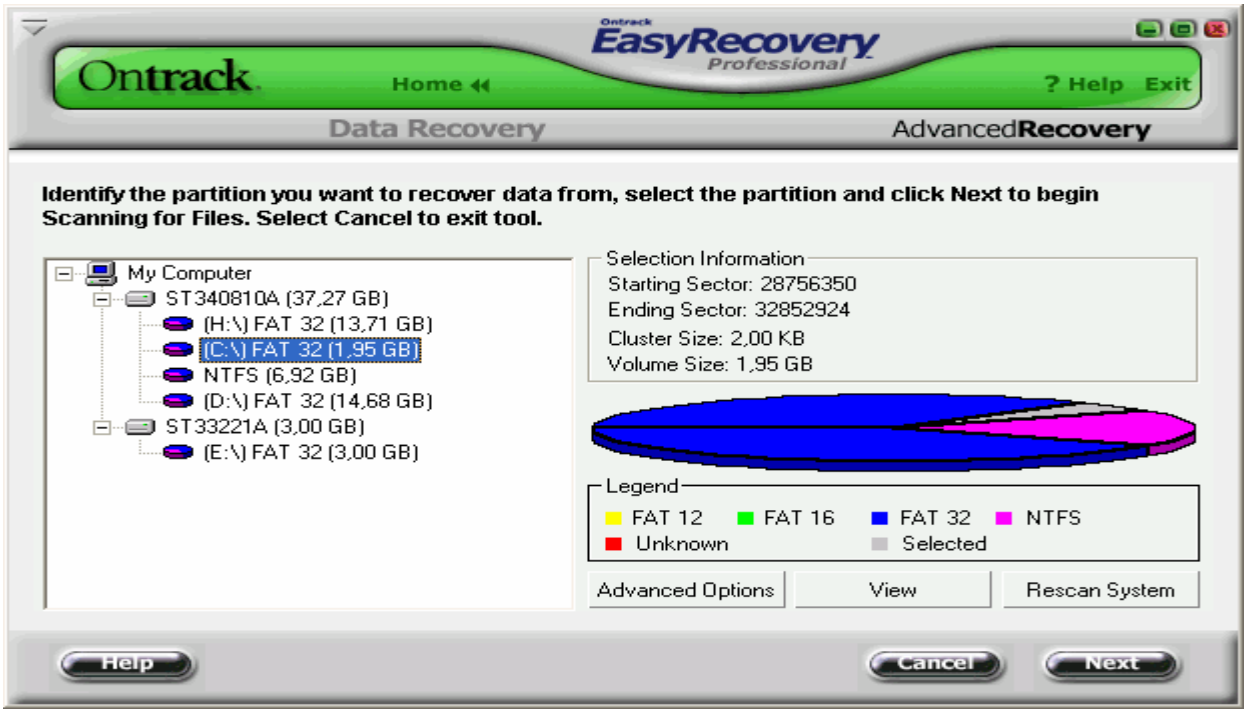


Рис. 6.8. Вікно майстра AdvancedRecovery

Компонента DeletedRecovery.

Помилкове видалення файлів - один із самих загальних сценаріїв відновлення даних. DeletedRecovery інструмент дасть швидкий доступ до вилучених файлів, і має різні варіанти щоб переглянути розділ. Можливо виконати швидкий перегляд, або повний перегляд для вилучених файлів. Є також можливість встановлення Фільтру для Файлів (рис. 6.12) для цього можливе використання групових імен аналогічних груповим іменам у DOS.

DeletedRecovery інструмент який перегляне існуючий розділ, та покаже довідники й файли, що були відзначені вилученими (рис. 6.13).

Як правило, якщо видалені один або два файли і не скопіювали ніяких даних до розділу, то мається дуже гарний шанс на відновлення вилучених файлів. У цій ситуації, інформація файлу може звичайно бути знайдена, при використанні швидкого перегляду. Якщо видалений каталог з декількома підкаталогами й файлами, треба буде виконати повний перегляд.

Імовірність відновлення файлу цілком неушкодженим зменшується, коли файл фрагментовано.

Компонента FormatRecovery

Інша загальна ситуація відновлення даних настає при випадковому форматуванні розділу. FormatRecovery інструмент дозволить відновити файли від розділу, який випадково відформатований. Цей тип відновлення буде ігнорувати існуючі структури системи файлу і шукати структури, зв'язані з попередньою системою файлу.

Дані файлу, у розділі , який відформатовано, усе ще присутні і можуть бути відновлені, із використанням даного інструменту.

Перший екран на FormatRecovery інструменті покаже список розділів знайденого на дисках, у вашій системі. Щоб починати форматоване відновлення, виберіть розділ, а потім файли, які треба відновлювати (рис. 6.13).

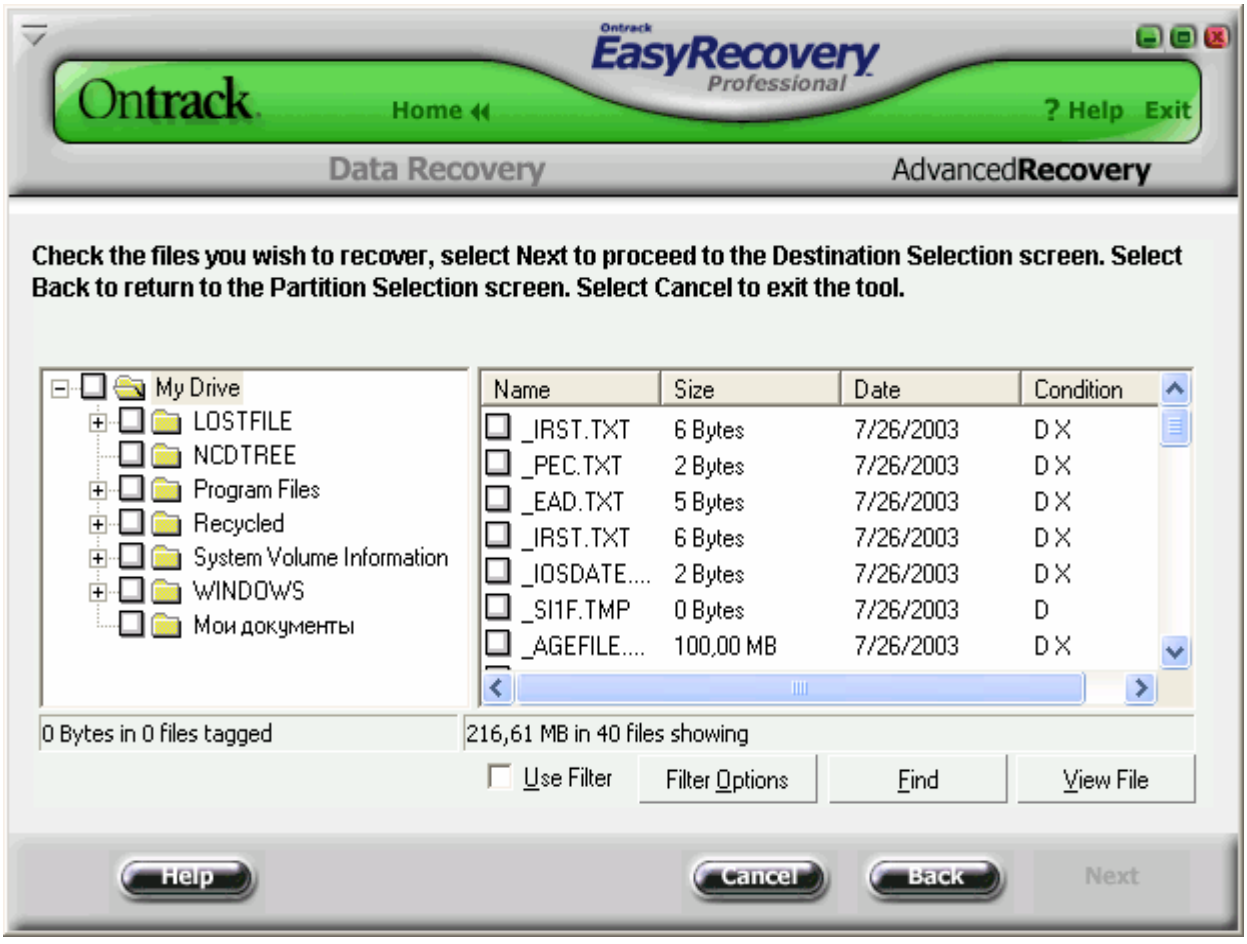


Рис. 6.9. Вікно зі списком видалених файлів

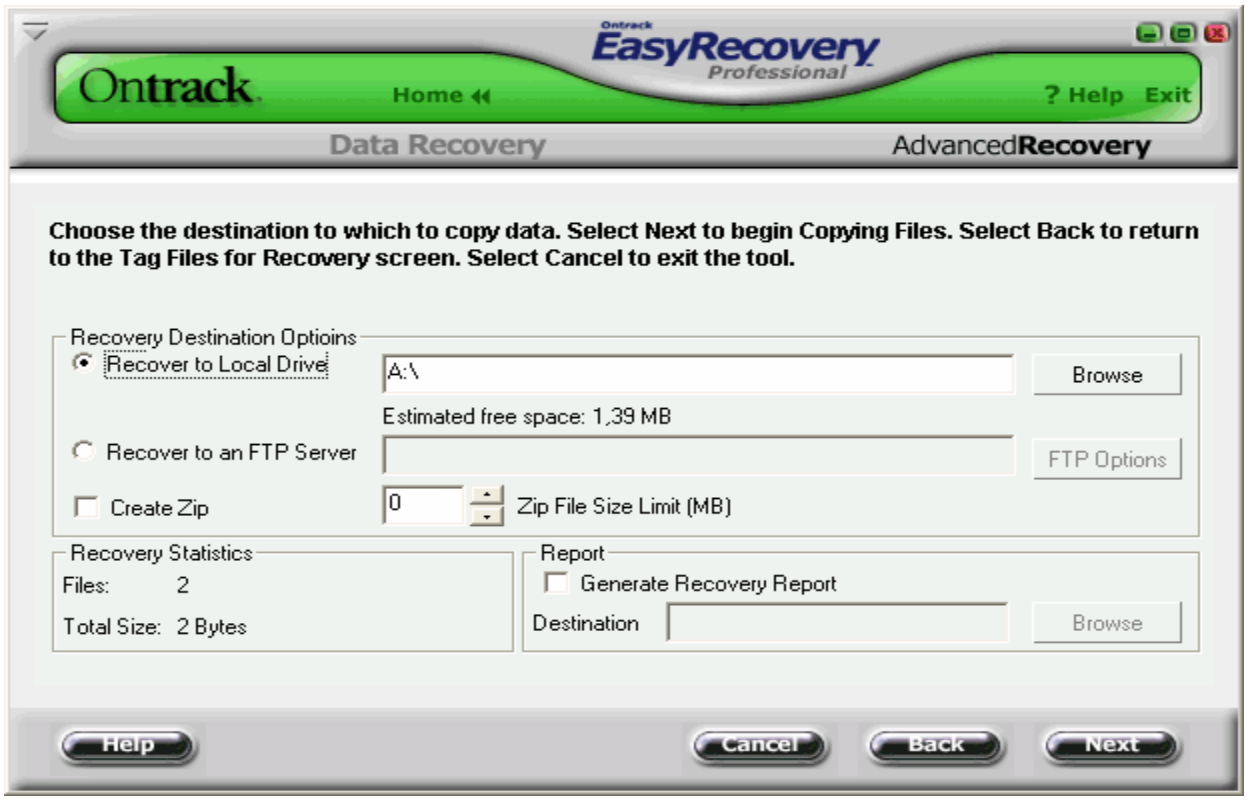


Рис. 6.10. Вікно вибору диска, куди будуть записані відновлені файли

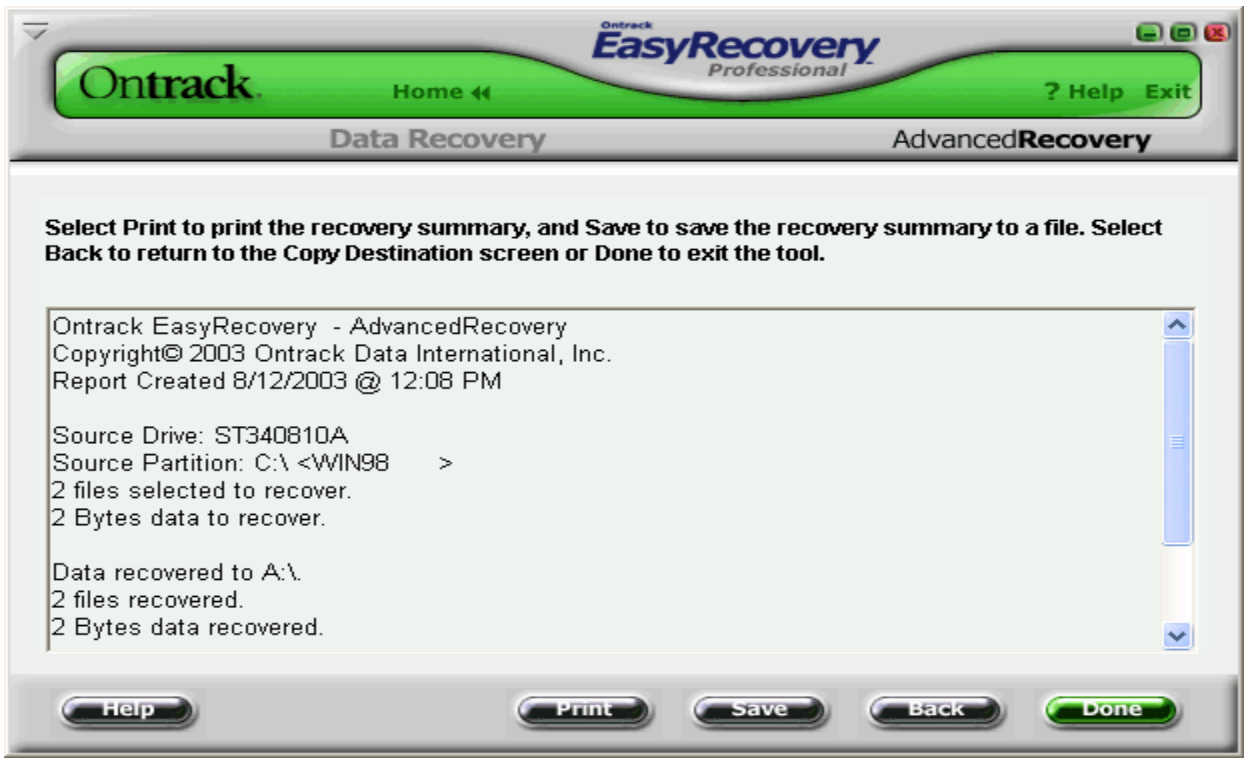


Рис. 6.11. Вікно результатів (резюме) відновлення файлів

Рис. 6.12. Вікно встановлення фільтру

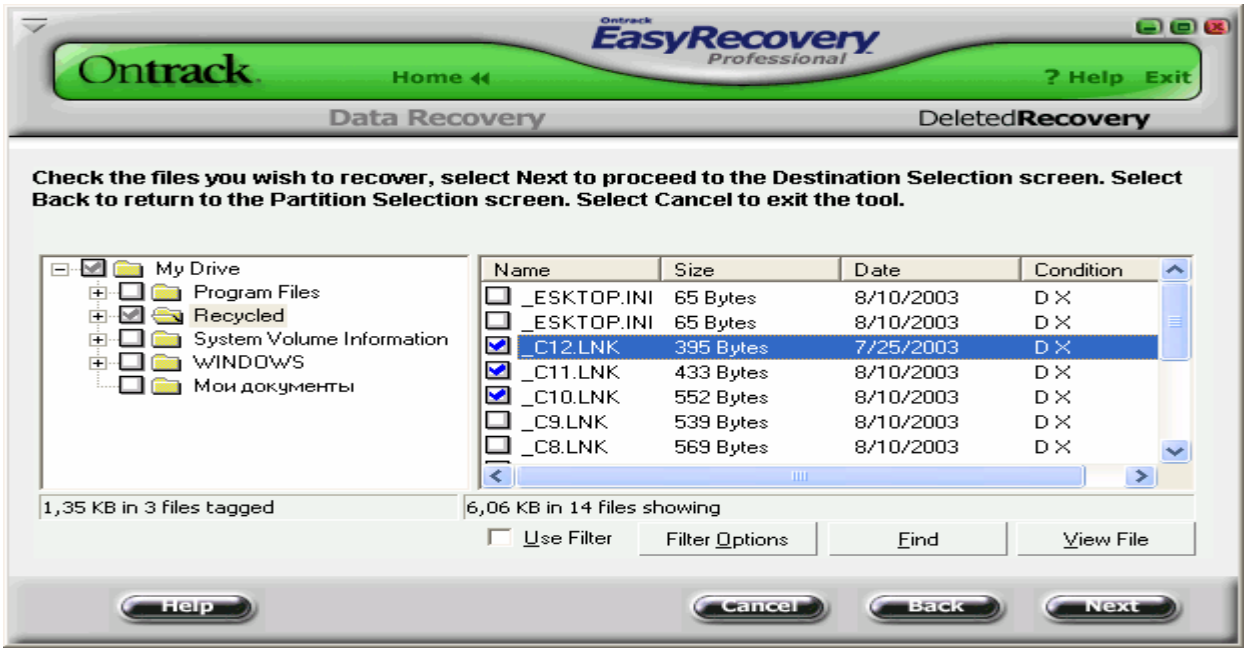


Рис. 6.13. Вікно перегляду видалених файлів

Цей інструмент допоможе відновити файли з розділів з ушкодженими файловими системами. Він буде читати всі сектори на диску послідовно (сектор за сектором), щоб визначити підписи удару головкою (заголовка) файлу. Якщо недавно про-

водилася робота з диском defragmenter, можливості відновлення будуть дуже поліпшені.

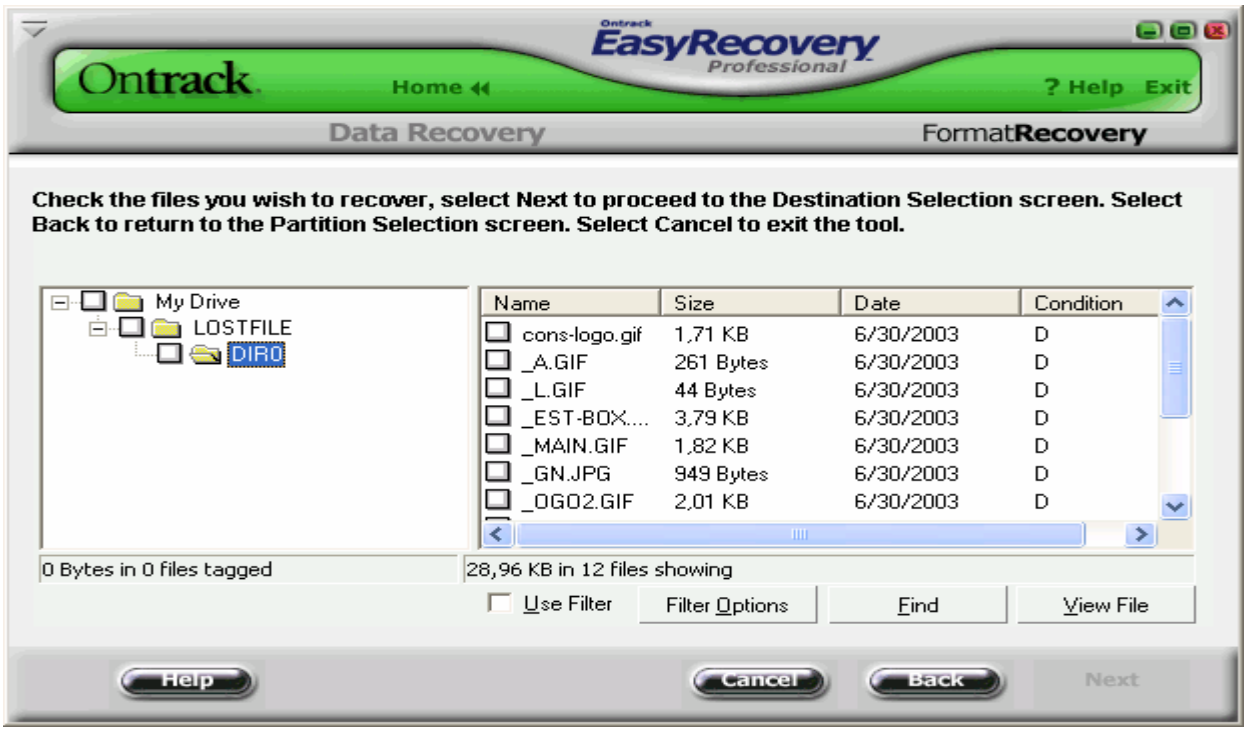


Рис. 6.14. Вікно зі списком видалених каталогів та файлів після форматування дискети

Утиліта UNFORMAT.

Unformat дозволяє відновлювати дані з відформатованого жорстокого диска. DOS-команда FORMAT видаляє системні області - **Завантажувальний запис** (Boot Record), **Таблицю розподілу файлів** (File Allocation Table), **Корневий каталог** (Root Directory), однак інформація з області даних на диску залишається недоторканою. Unformat спочатку шукає на диску системні дані і, якщо їх знаходить, реассемблерує їх, у противному випадку утиліта намагається реассемблерувати весь диск із самого початку.

Процес відновлення даних проходить швидше, якщо раніше була запущена утиліта Image для створення копії системних областей, і Unformat змогла знайти й скористатися інформацією з файлу Image.dat. Але і при відсутності Image.dat Unformat може повернути велику частину даних з диску.

Крім того, за допомогою цієї утиліти диск, зруйнований вірусами, також можна зробити працездатним.

Дискети за допомогою Unformat можна відновлювати тільки в тому випадку, якщо їх форматували утилітою Safe Format із попередньою обробкою дискет утилітою Image.

Як відновити відформатований диск?

1. Запустити утиліту Unformat; вибрати диск, який будемо відновлювати, ввести команду **View Map**...(Показати карту диска з виділеними кластерами відновлюваного файлу); ввести команду **Save**; відновити файл.

2. Якщо попередньо була використана утиліта **Image.exe** для створення копії системних областей диска або навіть якщо не зовсім упевнені в цьому, відповісти **Yes**, у противному випадку **No**.

З'явиться карта відновлення диска.

3. Якщо раніше використовувалась утиліту Image, Unformat повідомить про виявлення файлу Image.dat і запитає про відновлення даних відповідно до вмісту цього файлу (у противному випадку див. крок 4).

Якщо натиснути **ОК**, то буде запропоноване або повне, або часткове відновлення системної інформації з файлу Image.dat. Якщо важко вирішити, що ж вибрати використовуйте **FULL** - повне відновлення. Після вибору **Partial**- часткове відновлення, визначте, які системні області потрібно відновити: **Завантажувальний запис, Таблицю Розподілу Файлів, Кореневий каталог.** Після цього Unformat відновить диск і порадить запустити утиліту **NDD** (Norton Disk Doctor) для коректування даних, якщо були внесені зміни в структуру даних уже після створення файлу Image.dat, за яким створювалися системні області. На цьому, якщо Image.dat був знайдений, процес реассемблювання диска закінчений.

4. Після завершення Unformat підкаталоги у кореневому каталозі будуть мати імена DIR0, DIR1 і т.д. Засобами DOS їх можна перейменувати.

Для всіх файлів кореневого каталогу видалених командою Format, запустіть утиліту **UnErase** (процес відновлення файлової структури принципово не відрізняється від процесу відновлення файлової структури утилітою Unformat).

Видалення даних за допомогою програми Disk Wiper.

Реальне видалення файлів на накопичувачах жорстких дисків виконується загальноприйнятими засобами (провідник Windows, Norton Commander і т.п.) таким чином, що вони стають недоступними для використання прикладними програмами, наприклад, Microsoft Word, Excel і т.п., але можуть бути відновлені з використанням спеціальних програм. Для неможливості подальшого використання даних при їх видаленні використовують спеціальні програми, однією з яких і являється програма Disk Wiper.

Версія Windows Disk Wiper має розвинений інтерфейс і більше функціональних можливостей в порівнянні з версією для DOS. Інтерфейс вікон майстра дає більше можливостей (рис. 6.15).

Щоб створити новий розділ (логічний диск) необхідно маніпулятором типу „миш" в подальшому для зручності просто миш, виділити вільне місце на диску (Primary, free) та подати команду **Greate** (створити) із під меню **Partition** (розділ) (рис.6.15). Після введення команди з'явиться вікно (рис.6.16). Необхідно вибрати потрібні параметри та ввести команду **OK**.

Примітка:

- Align to beginning block (вирівняти за початком блоку);
- Greate on extended partition (створити додатковий розділ).

В результаті вказаних дій буде створено неформатований розділ (Primary Unformatted, або Extended Unformatted (рис. 6.17).

При виборі команди **Format** із під меню **Partition** з'явиться вікно роис. 6.18.

У даному вікні позначено: Volume Name (мітка диску), Surface test (перевірка поверхні диска), System type (тип файлової системи). Після введення команди **OK** пройде процес форматування диску (рис. 6.19).

Після форматування диску необхідно перезавантажити комп'ютер.

Розділ може бути видалений, якщо ввести команду **Delete** із під меню **Partition** (рис. 6.20).

При введенні команди **Wipe partition** із під меню **Partition** буде проведено повне очищення диску від усіх даних і подалі використання їх стане неможливим.

Щоб витерти тільки вільне місце в розділі, виберіть об'єкт і потім виберіть “**Clear free space**””, клацаючи правою кнопкою миші.

Параметри очищення вільного простору на диску вибирають за діалоговим вікном (рис. 6.21)

Примітка:

Де позначено **Hex mask** – маска (число яке заповнить всі кластери);

- **Wipe** – Витерти;
- **Pass** count—кількість проходів;
- **Check**—перевірка;
- **Percentage to Check**— процент перевірки.

Для приховування диску необхідно ввести команду **Hide** із під меню **Partition**. Після виконання вимог майстра та перезавантаження комп'ютера диск буде приховано. Для відображення диску необхідно ввести команду **Unhide** із під меню **Partition**.

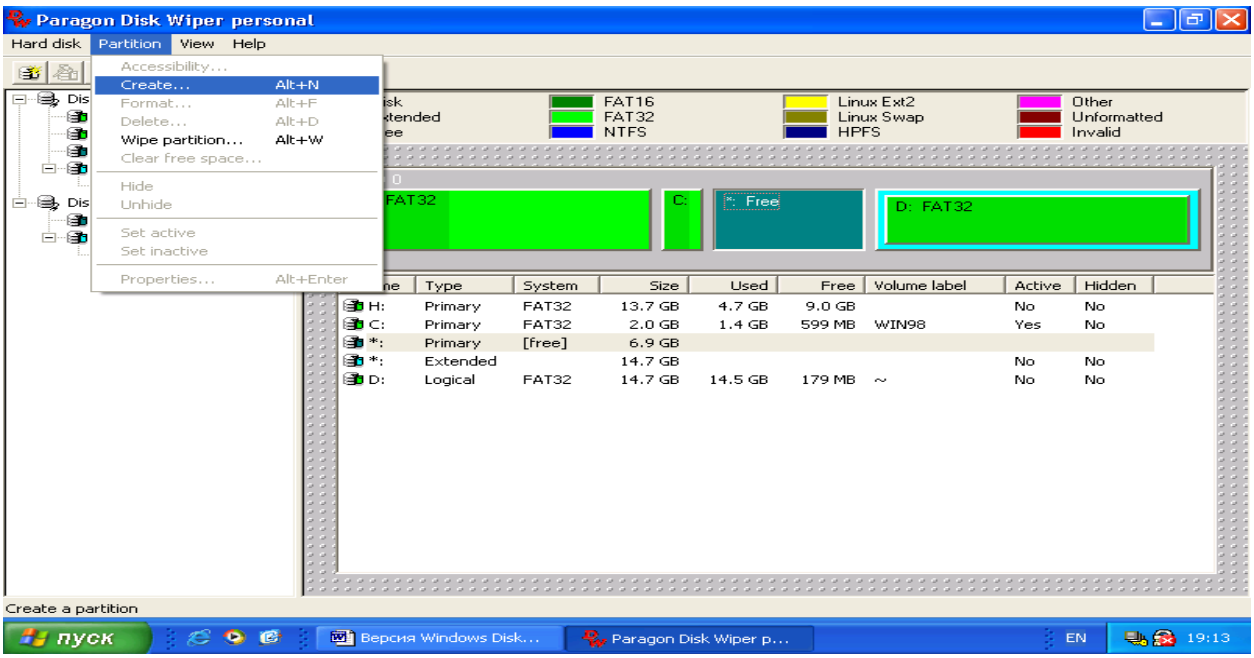


Рис. 6.15 Вікно майстра програми

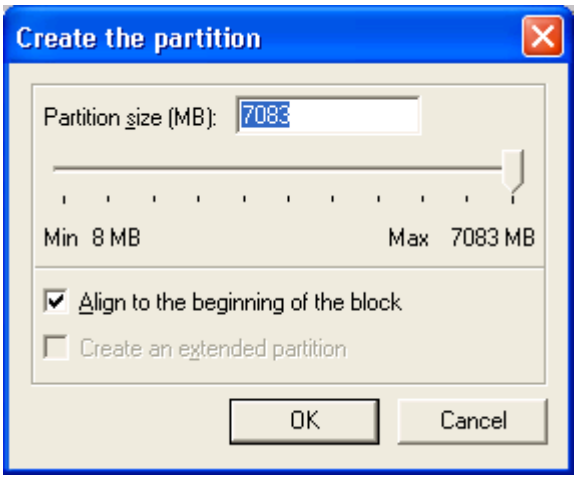


Рис. 6.16. Вікно вибору параметрів диска, який буде створено

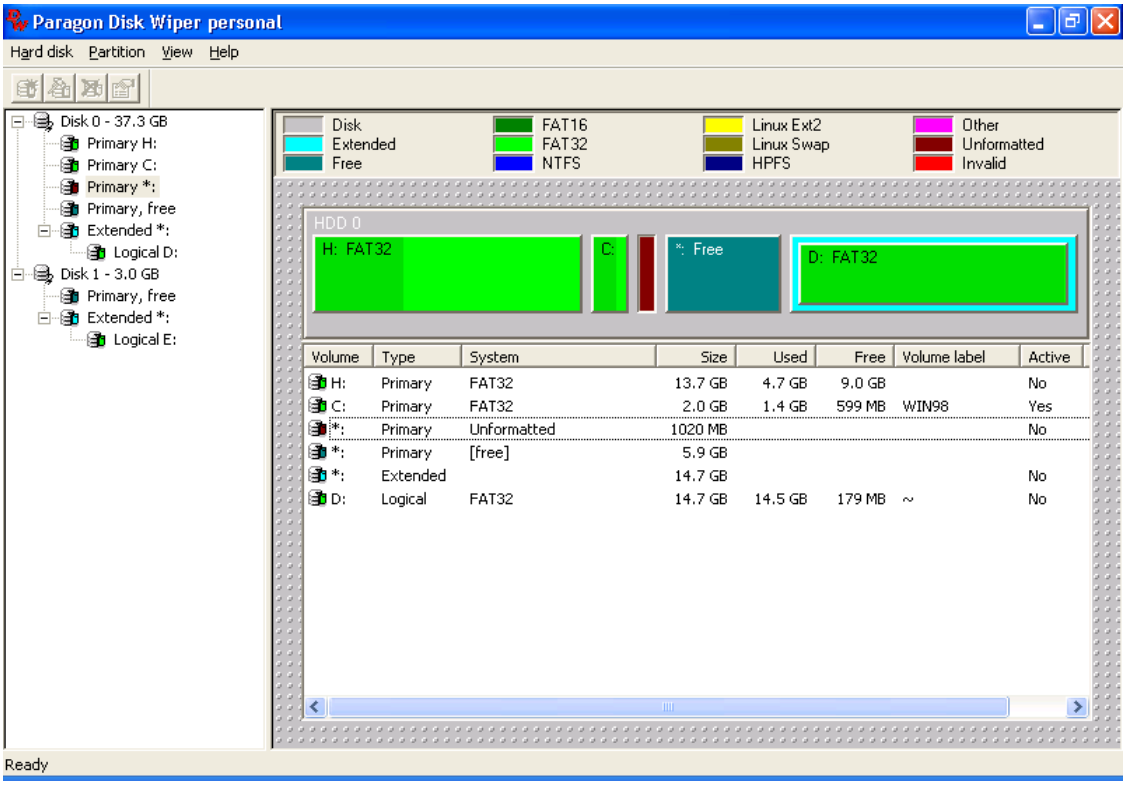


Рис. 6.17. Вікно з створеним неформатованим розділом

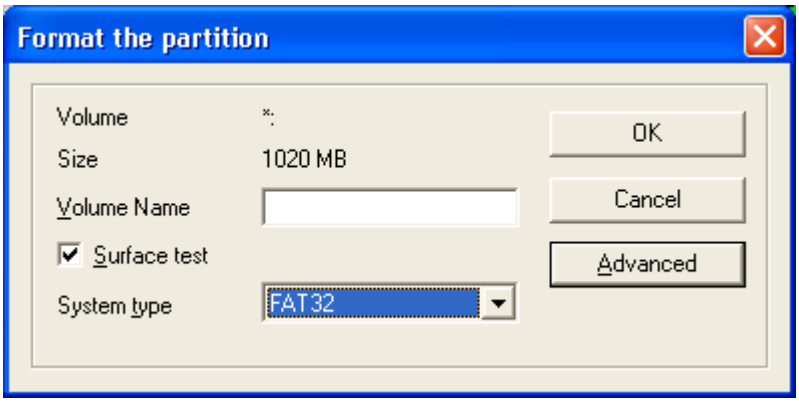


Рис. 6.18. Вікно вибору параметрів форматування

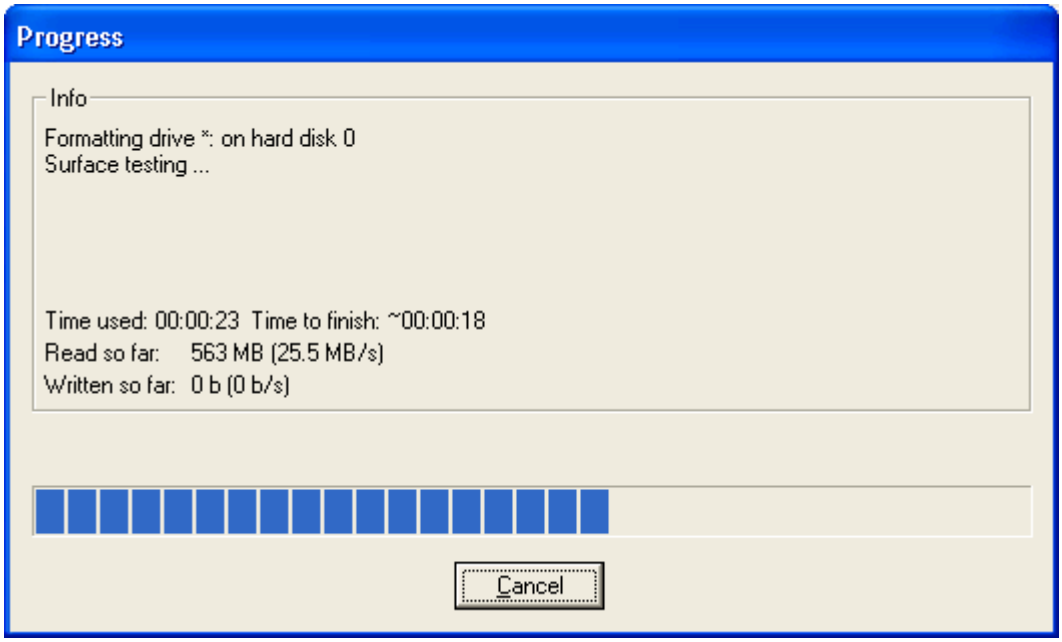


Рис. 6.19. Форматування диску

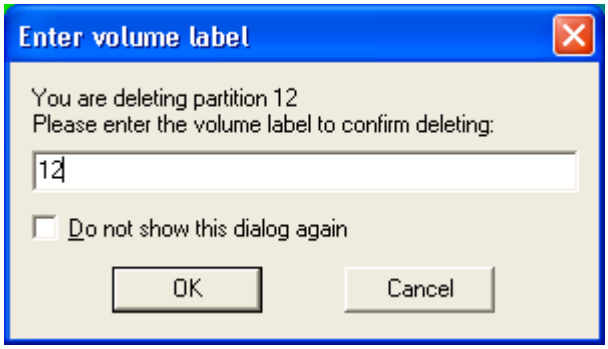


Рис. 6.20 Вікно видалення розділу

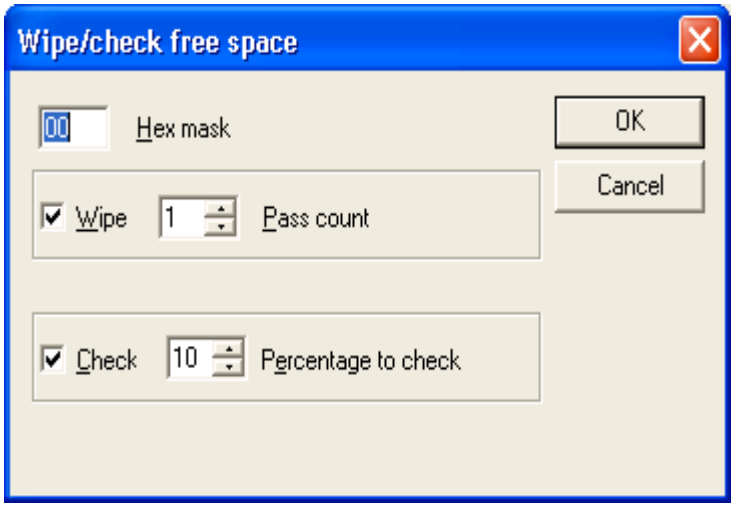


Рис.6.21. Вибір параметрів очищення вільного простору на диску

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть основні компоненти вікна програми.
2. Призначення компоненти Disk Diagnostics Contents.
3. Компоненти Діагностики Диска.
4. Основна відмінність тестування дисків у швидкому та повному режимі тестування.
5. Особливість та різновиди тестування дисків.
6. Призначення компоненти PartitionTests.
7. Призначення компоненти DataAdvisor.
8. Призначення компоненти Ontrack JumperViewer.
9. Призначення компоненти SizeManager.
10. Призначення компоненти Data Recovery.
11. Основні кроки відновлення даних.
12. Призначення компоненти AdvancedRecovery.
13. Призначення компоненти DeletedRecovery.
14. Призначення компоненти FormatRecovery.
15. Призначення програми Disk Wiper.
16. Особливості програми Windows Disk Wiper.
17. Як створити новий логічний диск за допомогою програми Windows Disk Wiper?
18. Як провести форматування створеного диску?
19. Як перевірити правильність позначення створеного диску?
20. Послідовність очистки вільного простору на диску.
21. Послідовність повної очистки диску.
22. Послідовність видалення логічного диску.
23. Як проводиться приховування диску та його відображення?

Розділ 7.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ.

Захист даних в комп'ютерних мережах стає однією з самих гострих проблем в сучасних інформаційно-обчислювальних системах. На сьогоднішній день сформульовано три базові принципи інформаційної безпеки, завданням якої є забезпечення:

- цілісності даних - захист від збоїв, ведучих до втрати інформації або її знищення;
- конфіденційності інформації;
- доступності інформації для авторизованих користувачів.

Важливу роль в захисті мереж сьогодні відіграє незалежне тестування на проникнення (тести на подолання захисту, penetration testing, pentest,) є популярною у всьому світі послугою в області інформаційної безпеки. Суть таких робіт полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту інформаційної системи. В ході тестування аудитор грає роль зловмисника, мотивованого на порушення інформаційної безпеки мережі замовника.

Мережеві компоненти, що атакуються

Згідно закону «Про захист інформації в автоматизованих системах» захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.

Захист інформації в АС забезпечується шляхом:

- дотримання суб'єктами правових відносин норм, вимог та правил організаційного і технічного характеру щодо захисту оброблюваної інформації;
- використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту інформації (мають відповідний сертифікат);
- перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому встановленим вимогам щодо

захисту інформації (сертифікація засобів обчислювальної техніки, засобів зв'язку і АС);

- здійснення контролю щодо захисту інформації.

Право власності на інформацію, створену як вторинну в процесі обробки в АС, встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем АС. Якщо такої угоди немає, то така інформація належить користувачу АС, який здійснив цю обробку. Користувач АС може проводити обробку інформації лише за наявності згоди на те її власника або уповноваженої ним особи, якщо ця інформація не віднесена до категорії загальнодоступної. Фізичні та юридичні особи в Україні на підставі Закону України "Про інформацію" (2657-12) можуть встановлювати взаємозв'язки з АС інших держав з метою обробки, обміну, продажу, купівлі відкритої інформації.

Такі взаємозв'язки повинні виключати можливість несанкціонованого доступу з боку інших держав або їх представників-резидентів України чи осіб без громадянства до інформації, що є в АС України, незалежно від форм власності і підпорядкування, стосовно якої встановлено вимоги нерозповсюдження її за межі України без спеціального дозволу.

Сервери

Призначені для зберігання інформації або надання певних видів послуг. Унаслідок цього, основними класами атак проти серверів є "відмова в сервісі" і спроби розкриття конфіденційної інформації. Специфічними атаками є атаки, що полягають у фальсифікації службових сервізів.

Всі можливі цілі зловмисників можна класифікувати як:

- отримання доступу до інформації;
- отримання несанкціонованого доступу до послуг;
- спроба виводу з робочого режиму певного класу послуг;
- спроба зміни інформації або послуг, як допоміжний етап якої-небудь більшої атаки.

Доступ до WEB-серверу має п'ять рівнів:

1. Загальнодоступний з можливістю тільки читання всіх URL за винятком тих, що поміщені в каталогах /private.
2. Доступ співробітників фірми або організації, якій належить сервер. Тут також допустимо тільки читання, але доступні і секції каталога /private.
3. Розробники WEB-сервера. Мають можливість модифікувати вміст сервера, інсталювати CGI-скрипты, переривати роботу сервера.
4. Адміністратори вузла (сервера). Мають ті ж привілеї, що і розробники, але можуть також реконфігурувати сервер і визначати категорію доступу.
5. Системні адміністратори. Мають ідентичні привілеї з адміністраторами сервера.

Сучасні WEB-сервери досить широко використовують java-аплети. При цьому повинні суворо виконуватися певні правила:

- Аплети не можуть читатися з або писатися на локальний диск;
- Аплети не повинні мати доступу до локальних зовнішніх фізичних пристроїв;
- Аплети не повинні мати доступу до конфігураційної інформації системи, включаючи ту, яка дозволила б їм дізнатися з якою ОС вони мають справу;
- Аплети не повинні виконувати системних команд або запускати зовнішні програми;
- Аплети не повинні встановлювати мережеві з'єднання з машинами, окрім тієї, з якої вони завантажені

Спроби отримання доступу до інформації, що знаходиться на сервері, у принципі нічим не відрізняються від подібних спроб для робочих станцій, і ми розглянемо їх пізніше. Проблема отримання несанкціонованого доступу до послуг приймає надзвичайно різноманітні форми і грунтується в основному на помилках або недокументованих можливостях самого програмного забезпечення. А ось проблема виводу з ладу (порушення нормального функціонування) сервізів досить актуальна в сучасному комп'ютерному світі. Клас подібних атак одержав назву атака "відмову в сервісі" (англ. deny of service – DOS). Атака "відмова в сервісі" може бути реалізована

на цілому діапазоні рівнів моделі OSI : фізичному, канальному, мережевому, сеансовому.

Зміна інформації або послуг як частина великомасштабної атаки є також дуже важливою проблемою в захисті серверів. Якщо на сервері зберігаються паролі користувачів або які-небудь дані, які можуть дозволити зловмиснику, зламавши їх, увійти до системи (наприклад, сертифікати ключів), то природно, сама атака на систему почнеться з атаки на подібний сервер. Як сервери послуг, що найбільш часто піддається модифікації, слід назвати DNS-сервери.

Річ у тому, що, якщо зловмиснику вдасться дістати права доступу до DNS-сервера, обслуговуючого дану ділянку мережі, то він цілком може зламати програму DNS-сервісу. Звичайно зміна робиться так, щоб за деякими видами запитів замість правильної IP-адреси клієнту видавалася IP-адреса якої-небудь машини зловмисника, а вся решта запитів оброблялася коректно. Це дає можливість змінювати шлях проходження трафіку, який можливо містить конфіденційну інформацію, і робити так, що весь потік інформації, який у нормальному режимі пройшов би поза досяжністю від прослуховування, тепер поступав прямо в руки зловмисника. Для боротьби з указаними видами атак створено відповідні системи захисту, наприклад, **система виявлення атак на мережевому рівні (Network IDS, NIDS**) контролює пакети в мережевому оточенні і виявляє спроби зловмисника проникнути всередину системи, що захищається (або реалізувати атаку типу "відмова в обслуговуванні"). Типовий приклад - система, яка контролює велике число TCP-запитів на з'єднання (SYN) з багатьма портам на вибраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP-портів. Система виявлення атак на мережевому рівні (NIDS) може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, що прозоро проглядає весь трафік в мережі (концентратор, маршрутизатор, зонд). Відзначимо, що "мережеві" IDS контролюють багато комп'ютерів, тоді як інші системи виявлення атак контролюють тільки один (той, на якому вони встановлені); с**истема контролю цілісності (System integrity verifiers, SIV**) перевіряють системні файли для того, щоб визначити, коли зловмисник вніс до них зміни. Найбільш відомою з таких систем є "Tripwire"; м**оні-**

тори реєстраційних файлів (Log-file monitors, LFM) контролюють реєстраційні файли, що створюються мережевими сервісами і службами. Аналогічно NIDS, ці системи шукають відомі сигнатури, тільки у файлах реєстрації, а не в мережевому трафіку, які указують на те, що зловмисник здійснив атаку. Типовим прикладом є синтаксичний аналізатор для log-файлів HTTP-сервера, який шукає хакерів, що намагаються використовувати добре відомі уразливості, наприклад, використовуючи атаку типу "phf"; о**бманні системи (deception systems**), які працюють з псевдосервісами, мета яких полягає у відтворенні добре відомих уязвимостей для того, щоб обдурити зловмисників. Як приклад можна назвати систему The Deception Tool Kit.

Робочі станції

Основним завданням зловмисника відносно робочих станцій є отримання інформації, що зберігається локально на їх жорстких дисках, або отримання паролів, що вводяться оператором, шляхом копіювання буфера клавіатури.

Однією з поширених технологій захисту від копіювання, є створення особливо визначуваних носіїв інфориації. Їх особливість полягає в тому, що на носії створюється спеціально організована мітка, яка використовується як ознака її дистрибутивності. Функцію контролю мітки виконує спеціальна частина програми, що захищається. Після копіювання засобами ОС диска, що захищається, буде скопійована вся інформація, за винятком мітки. При виконанні програми її контролююча частина встановить, що диск не дистрибутивний, і перерве виконання програми.

Інший спосіб запобігання незаконному використанню програм і даних полягає в зберіганні інформації в кодованому, зашифрованому вигляді. В цьому випадку без знання ключа робота з інформацією неможлива.

Третій спосіб використовувати ключі що підключаються до COM, LPT або USB портам.

Основною метою атаки на робочу станцію є, звичайно, отримання даних, що обробляються, або, що локально зберігаються на ній. А основним засобом подібних атак дотепер залишаються "троянські" програми. Ці програми за своєю структурою

нічим не відрізняються від комп'ютерних вірусів, проте при попаданні на ЕОМ прагнуть поводитися якомога непомітніше. При цьому вони дозволяють будь-якій сторонній особі, що знає протокол роботи з даною троянською програмою, проводити віддалено з ЕОМ будь-які дії. Тобто основною метою роботи подібних програм є руйнування системи мережевого захисту станції зсередини – пробиття в ній величезного пролому.

Для боротьби з троянськими програмами використовується як звичайне антивірусне ПЗ, так і декілька специфічних методів, орієнтованих виключно на них. Відносно першого методу як і з комп'ютерними вірусами необхідно пам'ятати, що антивірусне ПЗ виявляє величезну кількість вірусів, але тільки таких, які широко розійшлися по країні і мали численні прецеденти зараження. У тих же випадках, коли вірус або троянська програма пишеться з метою отримання доступу саме до Вашої ЕОМ або корпоративної мережі, то вона практично з вірогідністю 90% не буде виявлена стандартним антивірусним ПЗ.

Ті троянські програми, які постійно забезпечують доступ до зараженої ЕОМ, а, отже, тримають на ній відкритий порт якого-небудь транспортного протоколу, можна виявляти за допомогою утиліт контролю за мережевими портами. Наприклад, для операційних систем клона Microsoft Windows такою утилітою є програма NetStat. Запуск її з ключем "netstat -a" виведе на екран усі активні порти ЕОМ. Від оператора в цьому випадку потрібно знати порти стандартних сервізів, які постійно відкриті на ЕОМ, і тоді, будь-який новий запис на моніторі повинен привернути його увагу. На сьогодні існує вже декілька програмних продуктів, що проводять подібний контроль автоматично.

Відносно троянських програм, які не тримають постійно відкритих транспортних портів, а просто методично пересилають на сервер зловмисника яку-небудь інформацію (наприклад, файли паролів або повну копію тексту, що набирає з клавіатури), можливий тільки мережевий моніторинг. Це достатньо складне завдання, що вимагає або участі кваліфікованого співробітника, або громіздкої системи ухвалення рішень.

Тому найбільш простий шлях, що надійно захищає як від комп'ютерних вірусів, так і від троянських програм, – це установка на кожній робочій станції програм контролю за змінами в системних файлах і службових областях даних (реєстрі, завантажувальних областях дисків і т.п.) – так званих адвизорів (англ. adviser – повідомлювач).

Джереламі електромагнітних випромінювань в локальній мережі є, безумовно, робочі станції (комп'ютери) і активне мережеве устаткування.

Для захисту від витоку інформації за каналами побічних випромінювань і наведень застосовується екранування цього устаткування та дотримання європейської директиви з електромагнітної сумісності (European EMS Directive 89/336/EEC). На рівень випромінювання істотно впливає якість всіх елементів, що встановлюються в комп'ютер, а не тільки якість його корпусу. Вимоги з електромагнітної сумісності набагато менш жорсткі, ніж вимоги з технічного захисту інформації. Сучасні корпуси дозволяють значно ослабити випромінювання елементів комп'ютера.

Середовище передачі інформації

Різні середовища передачі даних (ефірна, кабельна) вимагають від зловмисника різних витрат для їх прослуховування.

Природно, основним видом атак на середовище передачі інформації є її прослуховування. Відносно можливості прослуховування всі лінії зв'язку діляться на :

- широкомовні з необмеженим доступом;
- широкомовні з обмеженим доступом ;
- канали "крапка-крапка" .

До першої категорії відносяться схеми передачі інформації, можливість прочитування інформації, в яких нічим не контролюється. Такими схемами, наприклад, є інфрачервоні і радіохвильові мережі. До другої і третьої категорій відносяться вже тільки дротяні лінії : читання інформації з них можливо або всіма станціями, підключеними до даного дроту (широкомовна категорія), або тільки тими станціями і вузлами комутації через які йде пакет від пункту відправки до пункту призначення (категорія "крапка-крапка").

До широкомовної категорії мереж відносяться мережа TokenRing, мережа EtherNet на коаксіальному кабелі і на повторювачах (хабах – англ. hub). Цілеспрямовану (захищену від прослуховування іншими робочими станціями) передачу даних у мережах EtherNet проводять мережеві комутатори типу свіч (англ. switch) і різного роду маршрутизатори (роутери – англ. router). Мережа, побудована із захистом трафіку від прослуховування суміжними робочими станціями, майже завжди коштуватиме дорожче, ніж широкомовна топологія, але за безпеку потрібно платити.

Відносно прослуховування мережевого трафіку пристроями, що підключаються ззовні, існує наступний список кабельних з'єднань за збільшенням складнощі їх прослуховування :

- невита пара – сигнал може прослуховуватися на відстані в декілька сантиметрів без безпосереднього контакту;
- вита пара – сигнал дещо слабкіше, але прослуховування без безпосереднього контакту також можливе;
- коаксіальний дріт – центральна жила надійно екранована обплетенням : необхідний спеціальний контакт, що розсовує або ріже частину обплетення, і проникає до центральної жили;
- оптичне волокно – для прослуховування інформації необхідне уклинення в кабель і дороге устаткування, сам процес під'єднування до кабелю супроводжується перериванням зв'язку і може бути виявлений, якщо по кабелю постійно передає який-небудь контрольний блок даних.

Виведення систем передачі інформації з ладу (атака "відмова в сервісі") на рівні середовища передачі інформації можливе, але звичайно, він розцінюється вже як зовнішня механічна або електронна (а не програмна) дія. Можливі фізичне руйнування кабелів, постановка шумів в кабелі і в інфра- і радіо- трактах.

Вузли комутації мереж

Атаки на вузли комутації переслідують звичайно дві мети : або порушення цілісності мережі ("відмова в сервісі"), або перенаправлення трафіку за невірним шляхом, яким-небудь чином вигідному зловмиснику.

Вузли комутації мереж представляють для зловмисників:

- як інструмент маршрутизації мережевого трафіку;
- як необхідний компонент працездатності мережі.

Відносно першої мети отримання доступу до таблиці маршрутизації, її реалізація дозволяє змінити шлях потоку можливо конфіденційної інформації у сторону, що цікавить зловмисника. Подальші його дії можуть бути подібні атаці на DNS-сервер. Досягти цього можна або безпосереднім адмініструванням, якщо зловмисник як-небудь отримав права адміністратора (найчастіше дізнався пароль адміністратора або скористався незміненим паролем за умовчанням). У цьому плані можливість видаленого управління пристроями комутації не завжди благо : дістати фізичний доступ до пристрою, керованого тільки через фізичний порт, набагато складніше.

Або ж можливий другий шлях атаки з метою зміни таблиці маршрутизації – він заснований на динамічній маршрутизації пакетів, включеної на багатьох вузлах комутації. У такому режимі пристрій визначає найбільш вигідний шлях відправки конкретного пакета, грунтуючись на історії приходу певних службових пакетів мережі – повідомлень маршрутизації (протоколи ARP, RIP та інші). В цьому випадку при фальсифікації за певними законами декількох подібних службових пакетів можна добитися того, що пристрій почне відправляти пакети за шляхом, що цікавить зловмисника, думаючи, що це і є найшвидший шлях до пункту призначення.

При атаці класу "відмова в сервісі" зловмисник, звичайно, примушує вузол комутації або передавати повідомлення за невірним "тупиковим" шляхом, або взагалі перестати передавати повідомлення. Для досягнення другої мети звичайно, використовують помилки в програмному забезпеченні, запущеному на самому маршрутизаторі, із метою його "зависання". Так, наприклад, зовсім недавно було виявлено, що цілий модельний ряд маршрутизаторів однієї відомої фірми під час надходження на його IP-адресу досить невеликого потоку неправильних пакетів протоко-

лу TCP або перестає передавати всю решту пакетів до тих пір, поки атака не припинитися, або взагалі зациклюється.

Системи аутентифікації електронних даних

При обміні даними за мережами виникає проблема аутентифікації автора документа і самого документа, тобто встановлення достовірності автора і перевірка відсутності змін в одержаному документі. Для аутентифікації даних застосовують код аутентифікації повідомлення (імітовставку) або електронний підпис.

Імітовставка виробляється з відкритих даних за допомогою спеціального перетворення (шифрування) з використанням секретного ключа і передається за каналами зв'язку в кінці зашифрованих даних. Імітовставка перевіряється одержувачем, з секретним ключем, шляхом повторення процедури, виконаної раніше відправником, над одержаними відкритими даними.

Електронний цифровий підпис є відносно невеликою кількістю додаткової аутентифікуючої інформації, передаваної разом з підписуваним текстом. Відправник формує цифровий підпис, використовуючи секретний ключ відправника. Одержувач перевіряє підпис, використовуючи відкритий ключ відправника.

Таким чином, для реалізації імітовставки використовуються принципи симетричного шифрування, а для реалізації електронного підпису - асиметричного.

Захист інформації при застосуванні особистої системи мережевого захисту

McAfee Personal Firewall Plus

Призначення програми.

Особиста Система мережевого захисту встановлює бар'єр між комп'ютером і Інтернетом, за умовчанням проводить моніторинг інтернетівського трафіку на предмет підозрілих дій. Вона може виконувати наступні функції:

- Захищати проти потенційних досліджень хакера і нападів;
- Захищати від вірусних вторгнень;
- Контролювати інтернетівську й мережеву діяльність;
- Попереджувати про потенційно ворожі події;

- Забезпечувати детальну інформацію щодо підозрілого інтернетівського трафіку;
- Забезпечувати розширену інтелектуальну обробку доступу. Особиста Система мережевого захисту спочатку відзначає, або розпізнає спробу доступу, як дозволену або недозволену. Якщо спробу доступу, визначено, як дозволену система автоматично дозволяє цей доступ до Інтернету;
- Об'єднувати функціональність Hackerwatch.org, зокрема перевіряє повідомлення, події, одночасно перевіряючи інструменти і здатність поштових повідомлень до подій і інших діалогових повноважень;
- Забезпечувати поліпшене запобігання входженню в мережу або надійне виявлення троянців, закладок і т.п. Блокує потенційну можливість передачі особистих даних;
- Забезпечує поліпшений візуальний розгляд (візуальний слід, який включає легкі для читання графічні карти, що показують джерело ворожих нападів і трафік, перелік Ip адрес від вашого комп'ютера до нападника) вторгнення від Інтернету;

Примітка:

Використання Firewall дозволяє деякою мірою вникнути загроз, із використанням евристично-подібної функціональності. Звести "на нівець" ризик від несанкціонованого сканування портів. Ця програма не дає можливості одержати з портів, що не входять у список дозволених, яку-небудь відповідь, тому що взагалі не пропускає до них подібного роду запити. Але Firewall не зможе допомогти, якщо атака ведеться за допомогою цілком законного доступу - скажімо, у вашій пошті виявиться лист, що містить вірус.

Системні вимоги

- Microsoft Windows 98, Мене, 2000, або XP;
- Персональний комп'ютер з 486 або вищий процесор (Рекомендований Pentium);

- 8 МБ вільної пам'яті жорсткого диска для інсталяції Microsoft Internet Explorer 5.01 або вище .

Примітка:

Щоб відновити найпізнішу версію Internet Explorer, відвідайте сайт Microsoft Web у http://www.microsoft.com/.

Установка програми

Скопіюйте каталог McAfee Personal Firewall Plus на жорсткий диск свого комп'ютера (місцезнаходження каталогу визначити за вказівкою викладача).

Для установки запустіть на виконання файл McAfeePersonalFirewallPlus.exe, який знаходиться в указаному каталозі, та відберіть потрібні параметри в процесі роботи майстра установки. Після установки запустіть файл mpf.reg і погодьтеся на внесення змін до реєстру Windows.

Запуск McAfee SecurityCenter

McAfee SecurityCenter - універсальний обчислювальний центр захисту. Він забезпечує консолідоване представлення стану захисту комп'ютера, і наявність вірусних тривог. Можливий запуск Security Center від значка McAfee у панелі задач (кнопка червоного кольору) використавши допоміжну клавішу маніпулятора типу

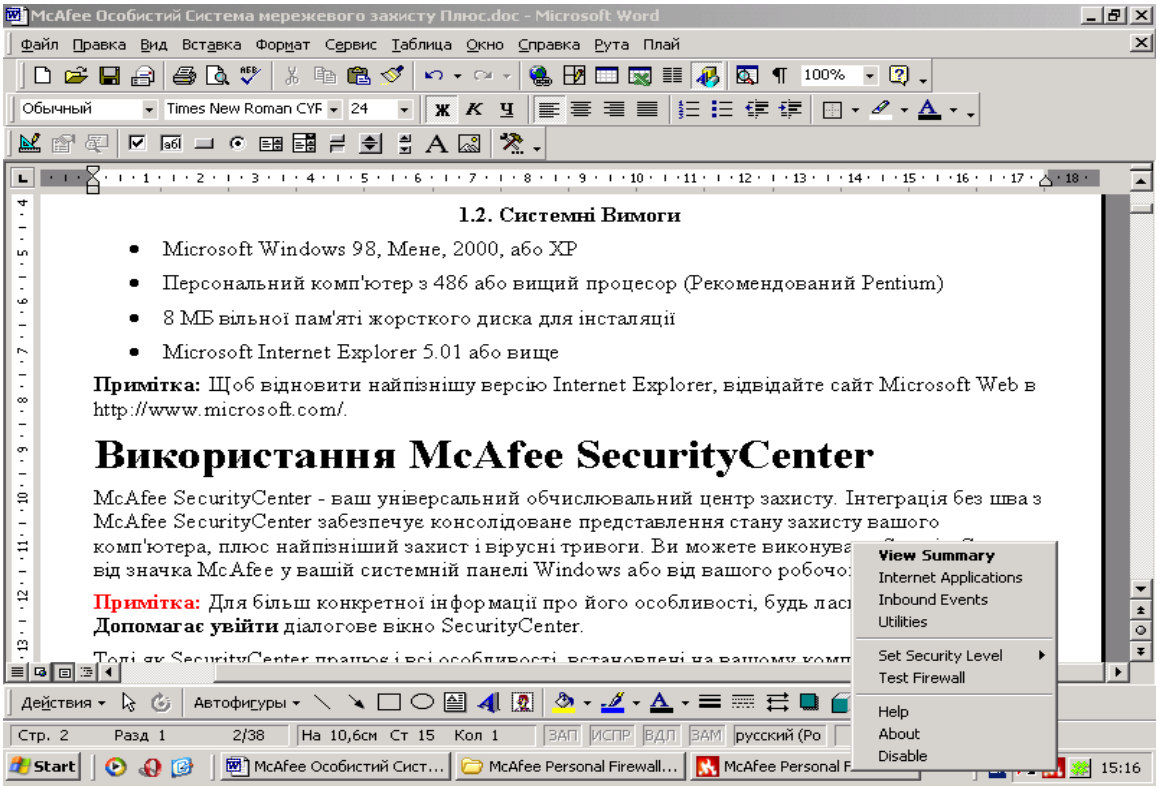


Рис. 7.1. Вікно запуску програми

“миш” (рис. 7.1), або з робочого столу Windows.

Якщо один або більше застосувань, встановлених на вашому комп'ютері, McAfee відключені, то колір кнопки змінюється на чорний. Для запуску програми введіть команду **View Summary**. З'явиться діалогове вікно програми (рис. 7. 2).

Конфігурування елементів системи мережевого захисту

Не потрібно, як правило, формувати параметри мережевого захисту, тому що значення, які встановлені за умовчанням забезпечують адекватну безпеку проти вторгнення. Можна змінити параметри налагодження, за допомогою помічника установлення програми.

Помічник установлення дозволяє налагодити:

- вид тривог, які потрібно одержувати;
- захист від вірусів;
- мережевий тип підключення;
- прикладні рекомендаційні параметри налагодження.

Рис. 7.2. Вікно програми

Щоб звернутися до Помічника, клацніть значок **Security Settings**. Виконуйте команди діалогових вікон.

Установки:

Клацніть правою кнопкою миші кнопку (рис. 7.1) **Утиліти**.

Налагодження параметрів проводиться у діалоговому вікні **Utilities** (рис. 7.3). Установіть рівень захисту, переміщаючи засувку на бажаний рівень. Якщо користувач системи новачок мережевого захисту, треба прийняти задане за умовчанням врегулювання **Стандарту**. Діапазони рівня захисту міняються від низького рівня (відкритий) до максимального (сувора ізоляція):

Табл. 7.1.

Рівні захисту

Діапазон рівня захисту	Опис
Сувора ізоляція High (Lockdow)	Весь трафік зупинений. Це по суті такий само режим, як відключення вашого інтернет-з'єднання. Можна використовувати це врегулювання, щоб блокувати порти.
Щільний Tight	Через прикладні запити забезпечується тільки вид доступу до Інтернету, який потрібен. Блокується будь-який недозволений доступ.
Стандарт Standard	Рекомендований рівень доступу. Надається прикладний повний доступ. Повний доступ дозволяє посилати дані, і одержувати непрошені дані на несистемних портах.
Довіра Trusting	Усім підключенням автоматично довірено, коли вони початково намагаються звертатися до Інтернету. Проте, можна вибрати параметри, щоб одержати повідомлення про нові підключення на вашому комп'ютері з тривогами.
Низька фільтрація Open/No)	Ваша система мережевого захисту фактично відключена. Це врегулювання дозволяє весь трафік пропускати без фільтрації.

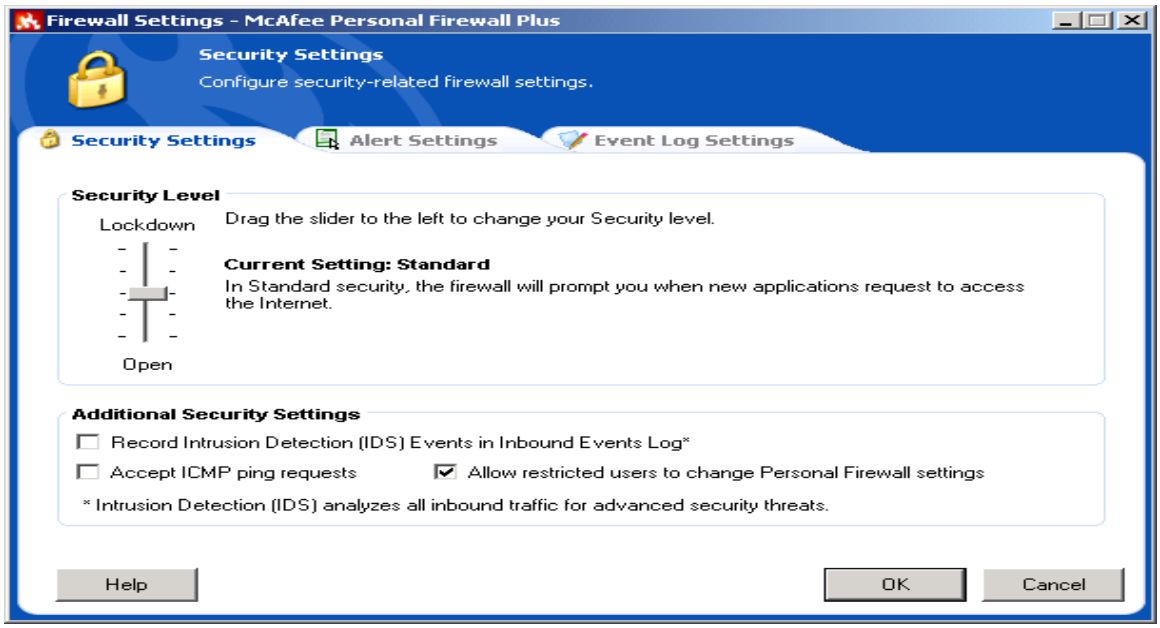


Рис. 7.3. Вікно утиліт

Примітка:

Налагодження параметрів можливе, якщо користувач володіє правами адміністратора системи.

Record Intrusion Detection (IDS) Events in Inbound Events Log (система візуального зображення інформації). Якщо вибрати цей налагоджувальний елемент, події візуального зображення інформації, з'являться у файлі Подій реєстрації, що прибувають.

Accept ICMP ping requests (міжмережевий протокол управління повідомленнями використовується переважно для виконання команд pinging). Якщо вибрати цей налагоджувальний елемент, особиста система мережевого захисту дозволяє всі запити залишати без реєстрації у файлі Подій реєстрації.

Allow restricted users to change Personal Firewall settings. Якщо на комп'ютері операційна система Windows XP і багато користувачів, то необхідно вибрати вказаний параметр для, того щоб дозволити деяким користувачам змінювати параметри налагодження даної програми.

Вкладка Alert Settings.

Виберіть вид тривоги в полі ”Alert to Lisplay” для відображення:

Show Only Red Alerts (покажіть тільки червоні тривоги) — червоні тривоги містять важливу інформацію, яка вимагає вашої безпосередньої уваги. Наприклад, прикладний доступ запитів до Інтернету і треба надати або блокувати доступ.

Show Only Red and Green Alerts (покажіть тільки червоні й зелені тривоги) — зелені тривоги інформують про зміни, які були зроблені до особистої системи мережевого захисту. Наприклад, зелені тривоги можуть інформувати про підключення, які особиста система мережевого захисту автоматично надала, або про застосування будь-яких нових правил при доступі до Інтернету.

Show All Alerts (покажіть всі тривоги) — покази червоних, зелених, і блакитних тривог. Блакитні тривоги містять інформацію, яка не вимагає ніякої відповіді від .

Виберіть додаткові налагоджувальні елементи відповіді для тривог, що відображаються:

Flash the tray icon when alerts aren't displayed (спалахнути значку лотка, коли тривоги не відображаються)— при виборі вказаного параметра спалахує значок на панелі задач, коли подія, що відбувається;

Auto-hide non-critical alerts after 10 seconds (некритичні тривоги авто-укриття після 10 секунд) — виконується дія програми, яка вибрана за умовчанням на подію. Якщо не вибрати вказаного параметра, то сигнал тривоги буде на екрані до того часу доки користувач не відреагує на подію;

Animate slide-in alerts (активні включені тривоги) — вибирають цей перемикач (значення встановлюються за умовчанням), щоб активізувати включення ярлика на вашому робочому столі Windows. Інакше, очистіть перемикач, щоб одержати стандартні спливаючі тривоги.

Виберіть параметри в полі "Smart Recommendations ":

Use Smart Recommendations —особиста система мережевого захисту автоматично дозволяє підключення, що засновані на базі даних розпізнаних застосувань. Завжди буде виведено попередження про невизначені або потенційно небезпечні програми;

Display Smart Recommendations Only -- особиста система мережевого захисту не автоматично дозволяє або блокує підключення, але рекомендує курс дії;

Do not use Smart Recommendations — особиста система мережевого захисту не автоматично дозволяє або блокує підключення і не рекомендує курс дії.

Вкладка Event Log Settings

В полі Inbound Events Logging Settings, виберіть, чи повинна реєструвати особиста система мережевого захисту події. Якщо вибирається режим, щоб зареєструвати події, особиста система мережевого захисту відображає події на сторінці **Подій** основного вікна. За умовчанням, особиста система мережевого захисту реєструє всі типи подій. Можна змінитися типи події для реєстрації. Для цього необхідно ввести команду **Configure**... і у вікні, що з'явиться (рис. 7.4) відібрати необхідні типи події, а також вказати номери портів показу в представленні подій, щоб показати початкові і призначені порти події у файлі **Подій реєстрації.**

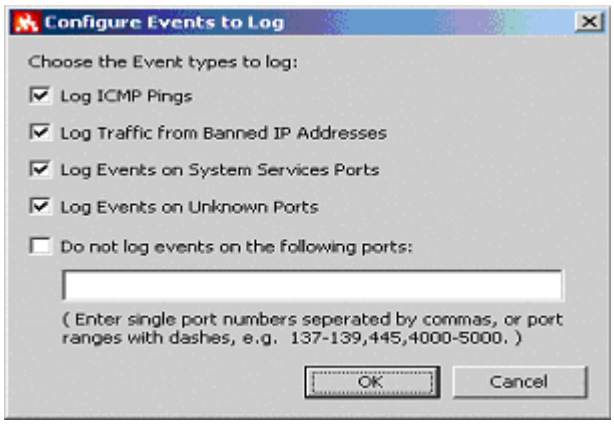


Рис. 7.4. Вікно вибору типів подій

Довірені IP адреси

Список довірених адрес Ip дозволяє отримувати весь трафік від певного комп'ютера, на будь-якому порту. Особиста система мережевого захисту не реєструє трафік або не генерує тривоги події від адрес Ip у списку довірених адрес Ip. Комп'ютер поводитиметься нібито немає ніякої системи мережевого захисту.

Щоб додати Ip адреси до списку "Довірених Адрес Ip" необхідно:

Виконати дії за рис. 7.1 на вкладці **Summary** ввести команду **Trusted this IP Addresses,** в діалоговому вікні (рис. 7.5) увести необхідні адреси.

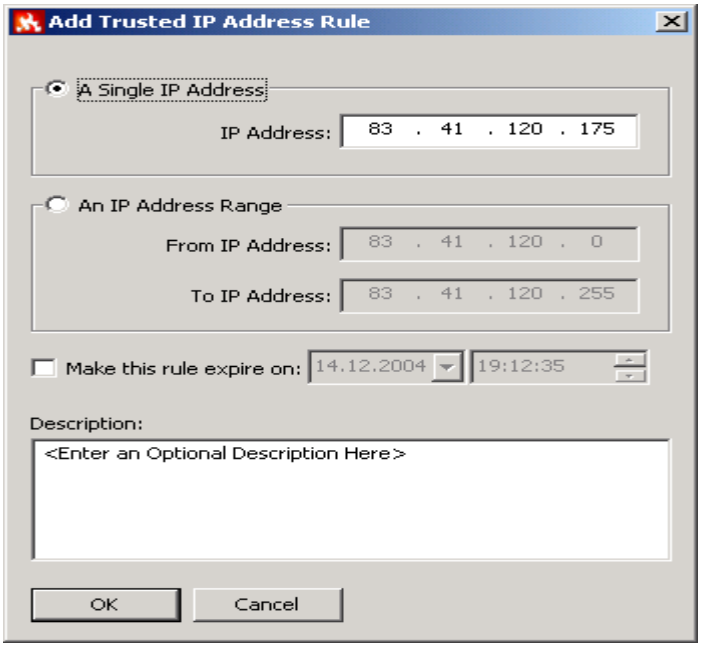


Рис. 7.5. Вікно введення Ip адреси

Примітка:

При введені адрес, яким довіряють тимчасово, необхідно вказати дату й час, закінчення довіри. Після введення команди **OK**. адреса Ip з'являється в списку "Довірених Адрес Ip".

Системні послуги

В деяких випадках обов'язково необхідно відкрити порти для забезпечення доступу інших комп'ютерів, наприклад, якщо комп'ютер працює в режимі веб-сервера і т.п. Для цього необхідно на вкладці **Утиліти** ввести команду **System Services** та в діалоговому вікні (рис. 7.6) відібрати потрібні порти доступу, або добавити їх, якщо таких немає в системному списку, ввівши команду **Add**.

Моніторинг трафіку

Моніторинг відображає числові й графічні представлення інтернетівського трафіку, трафіку доступу до Інтернету та доступу від Інтернету. Моніторинг трафіку також показує, які з'єднання зараз використовуються на вашому комп'ютері й адреси Ip, до яких є підключення. Моніторинг трафіку автоматично модифікує свої дані кожних декількох хвилин (рис. 7.7), але можливо уручну модифікувати екран, увівши команду **Refrech**. Для входу в указаний режим необхідно на вкладці **Утиліти** ввести команду **Traffic Monitor**.

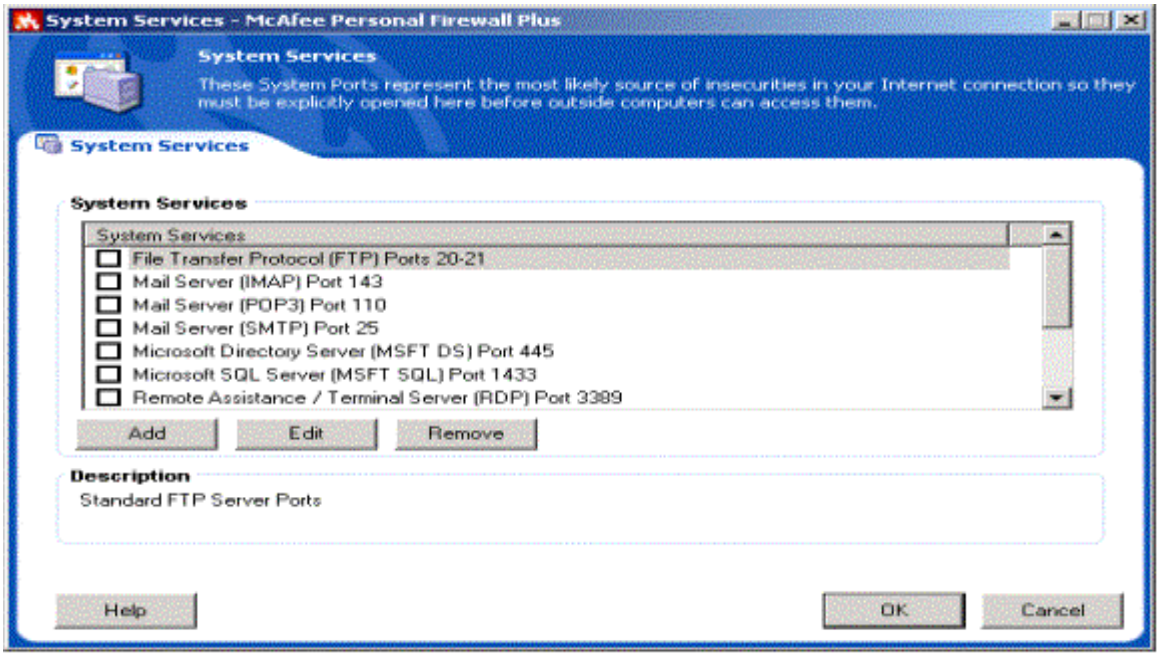


Рис. 7.6. Вікно вибору портів

Вкладка Applications (Аналіз трафіку) показує інтернетівську діяльність у реальному часі на комп'ютері, швидкості підключення, і кількість байтів, які перенесені через Інтернет. Traffic Analysis забезпечує візуальне представлення даних, показує норму кілобайт, перенесених на останніх 15 хвилинах. З правої сторони графіка нижче розташований перемикач представлення інформації. За його допомогою можна змінити представлення даних та отримати дані за останні 24 години, за поточний або минулий місяць.

Для трафіку, який надходить з Інтернету зелена лінія представляє поточну норму передачі даних, а пунктирна зелена лінія представляє середню норму передачі для вхідного трафіку. Якщо поточна норма передачі і середня норма передачі співпадають за величиною, то пунктирна лінія не з'являється. Для трафіку, який надходить до Інтернету червоний рядок представляє поточну норму передачі, червона пунктирна лінія представляє середню норму.

Перегляд короткого звіту.

Можна отримати різні сторінки звіту, вибравши потрібну зі списку (рис. 7.8).

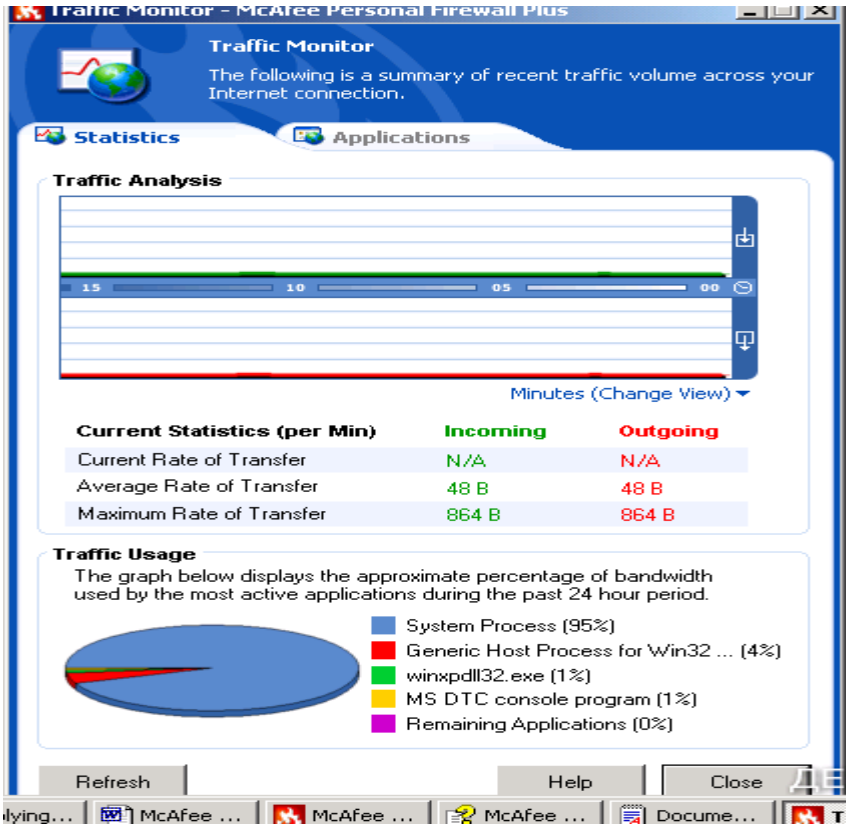


Рис. 7.7. Вікно моніторингу

Вкладка Internet Applications.

Вона використовується для того, щоб розглядати список дозволених і блокованих підключень, змінювати параметри підключень, добавляти нові, видаляти старі і т.п. Для дій з підключеннями використовується контекстно-залежне меню (рис. 7.9).

У списку Дозволів, клацніть правою кнопкою миші рівень дозволу для застосування, і виберіть інший рівень:

Allow Full Access, дозволяє підключення при посиланні й отримуванні даних.

Outbound Access Only, неможливе підключення ззовні.

Block This Application, не дозволяє підключення при посиланні й отримуванні даних.

Delete Application Rule, дозволяє видалити існуюче підключення.

Виберіть команду **New Allowed Application** для створення нового підключення й команду **New Blocked Application** для створення блокованого.

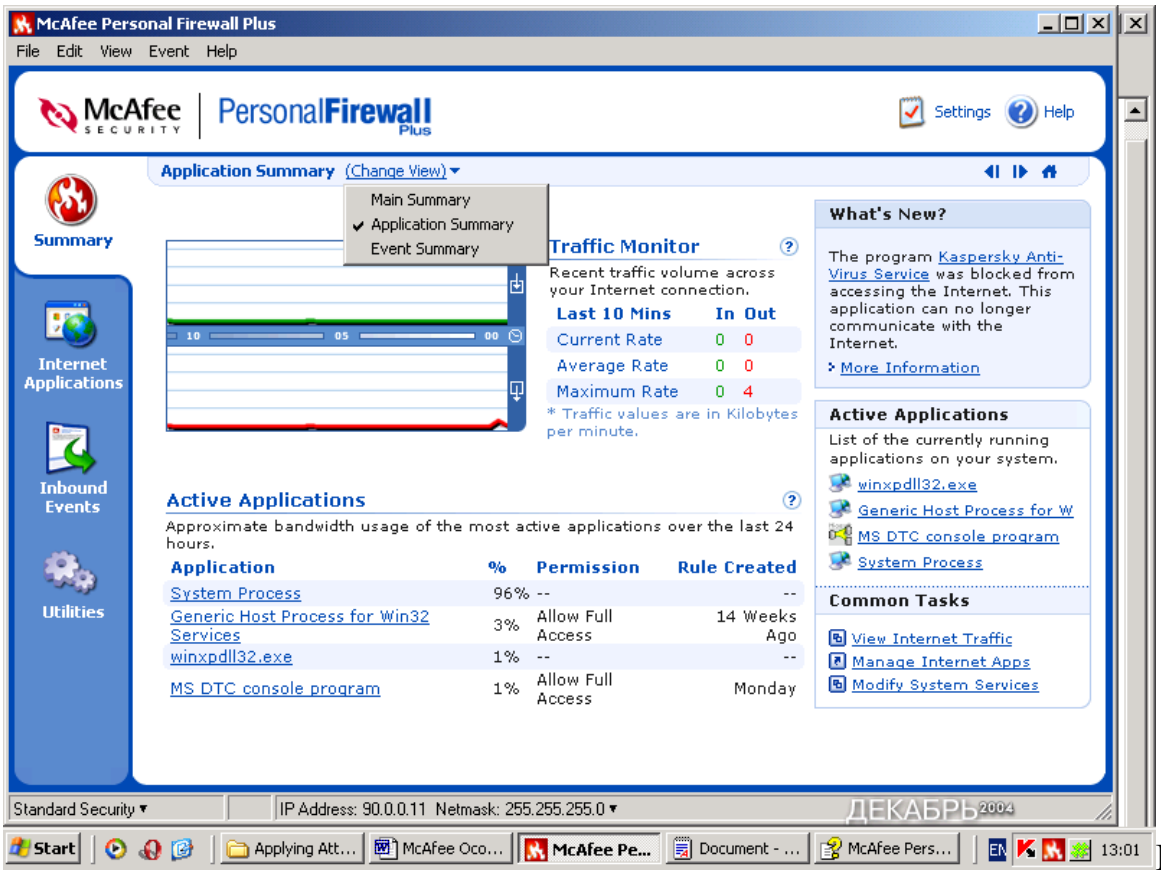


Рис. 7.8. Вікно відбору звітів.

Вкладка Inbound Events.

Використовуйте сторінку подій, що прибувають, щоб розглядати файл подій реєстрації. Він дозволяє створити архів подій та продивитися старі архіви. Можливий перегляд подій за поточний день, останній тиждень, перегляд повного файлу реєстрації, вибір події певних днів, від певних Ip адрес. Для отримання такої інформації необхідно виділити мишкою подію та вибрати відповідну команду з під меню **View**.

Можливо експортувати свій файл подій реєстрації, що прибувають, до текстового файлу. Для цього використовується команда **Exporting Displayed Events** із підменю **Файл**.

Про тривоги.

Для встановлення різних видів тривог необхідно перейти на вкладку **Утиліт** та ввести команду **Alert Settings**. В вікні **Smart Recommendations** відібрати зі списку потрібне значення тривог, за умовчанням установлюється команда **Use Smart**

Recommendations. Вона дозволяє отримувати червоні тривоги, які містять важливу інформацію, що вимагає безпосередньої уваги.

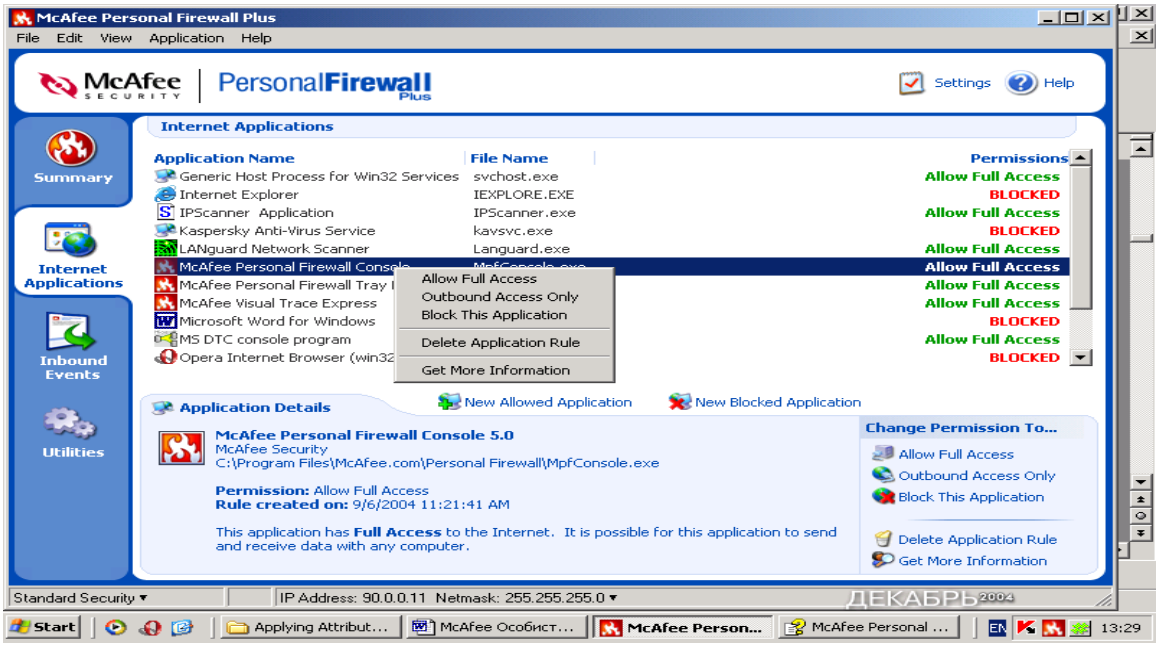


Рис. 7.9. Вікно роботи зі списком дозволів

Розрізняють наступні типи червоних тривог:

Internet Application Blocked - ця тривога з'являється, якщо особиста система мережевого захисту блокує спробу доступу до Інтернету. Наприклад, якщо з'являється тривога програми Trojan. McAfee автоматично блокує цей доступ програми до Інтернету і рекомендує переглянути свій комп'ютер на наявність вірусів.

Application Wants to Access the Internet - ця тривога з'являється, коли в результаті Інтернет пошуків мережа переходить до нової недозволеної Ip адреси. (Стандартний або щільний захист).

Application Has Been Modified - ця тривога з'являється, коли дозвіл доступу до Інтернету, що був наданий раніше, змінився. (Довіра, стандарт, або щільний захист)

Application Requests Server Access - ця тривога з'являється, коли доступ мережі наперед дозволений, а звертання іде як до сервера. (Щільний захист)

Зелені Тривоги

Зелені тривоги інформують про зміни, які були зроблені до особистої системи мережевого захисту. Наприклад, зелені тривоги можуть інформувати про нові надані доступи до Інтернету, або інформувати про будь-які нові правила застосування.

Program Allowed to Access the Internet - ця тривога з'являється, коли особиста система мережевого захисту автоматично надає інтернетівський доступ для всіх нових або змінених застосувань, а потім повідомляє (Довіра захисту), про нові правила застосування.

Блакитні Тривоги

Блакитні тривоги містять інформацію, але не вимагають ніякої відповіді.

Connection Attempt Blocked - ця тривога з'являється, коли особиста система мережевого захисту блокує небажаний інтернетівський або мережевий трафік. (Довіра, стандарт, або щільний захист)

Блокування спроби підключення до комп'ютера

Наприклад, після отримання сигналу тривоги розгляньте короткий опис події, далі виберіть із налагоджувальних елементів:

Уведіть команду, **Trace This Address**, щоб побачити візуальний слід адрес, для цієї події.

Уведіть команду **Ban This Address**, щоб блокувати цю адресу для доступу до комп'ютера. Адреса додається до списку "Заборонених Адрес Ip".

Уведіть команду **Trust This Address**, щоб дозволити цій адресі Ip звернутися до вашого комп'ютера.

Уведіть команду **Continue What I Was Doing**, якщо не треба обрати дію після того, як особиста система мережевого захисту вже виконала її.

КОНТРОЛЬНІ ПИТАННЯ

1. Особливості атак на сервери, робочі станції.
2. Особливості атак на середовище передачі даних.
3. Особливості атак на вузли комутації мереж.
4. Особливості захисту серверів, робочих станцій.
5. Особливості захисту середовища передачі даних.
6. Особливості захисту вузлів комутації мереж.
7. Системи аутентифікації електронних даних.
8. Призначення програми McAfee Personal Firewall Plus.

9. Системні вимоги при інсталяції програми.
10. Порядок запуску McAfee SecurityCenter.
11. Два підходи до конфігурування елементів системи мережевого захисту
12. Конфігурування елементів системи мережевого захисту за допомогою помічника установки.
13. Вибір елементів у вікні утиліт.
14. Типи тривог та їх вибір.
15. Червоні тривоги, їх призначення.
16. Зелені тривоги, їх призначення .
17. Блакитні тривоги, їх призначення .
18. Призначення вкладки Event Log Settings.
19. Установлення Ip адрес.
20. Системні послуги.
21. Порти та їх відкриття, закриття.
22. Моніторинг трафіку.
23. Робота зі звітами.
24. Призначення вкладки Internet Applications.
25. Призначення вкладки Inbound Events.
26. Порядок бокування спроби підключення до комп'ютера в різних випадках.

Розділ 8.

КОМП'ЮТЕРНІ ВІРУСИ ТА БОРОТЬБА З НИМИ.

ВСТУП.

Історично виникнення вірусів пов'язане з ідеєю створення програм, що самовідтворюються, - концепції, що йде своїм корінням в п'ятдесяті роки. Ідея механізмів, що самовідтворюються, досліджувалася ще Джоном фон Нейманом, який в 1951 р. запропонував метод створення таких механізмів. Таким чином, попередниками вірусів були різного роду програми (деякі з них у вигляді ігор), принцип роботи яких полягав в здатності самовідтворюватися.

Вже на початку 60-х з'явилася "Гра для опівнічників", в якій декілька асемблерних програм, названих "організмами", завантажувалися в пам'ять комп'ютера. Організми, створені одним гравцем (тобто що належать до одного вигляду), повинні були знищувати представників іншого вигляду і захоплювати життєвий простір. Переможцем вважався той гравець, чиї організми захоплювали всю пам'ять або набирали найбільшу кількість очок. І вже тоді в описі гри термін "вірус" застосовувався до одного з видів організмів.

Приблизно у 1970 р. була створена програма, що самовідтворюється, для однієї з перших комп'ютерних мереж - APRAnet. Програма Creeper подорожувала за мережею, виявляючи свою появу повідомленням: "I'M THE CREEPER ... CATCH ME IF YOU CAN".

Потім була написана програма Rabbit, яка розмножувалася на трьох сполучених між собою машинах IBM, причому появу нових підзадач викликало уповільнення роботи, а потім і повне зависання машин.

Другим прикладом вірусоподібних програм була досить відома гра Animal, розроблена для Univac 1108. Суть цієї гри полягала в тому, що людина замислювала деяку тварину, і програма, ставлячи питання, намагалася визначити, яку тварину загадав чоловік. Автор передбачив в ній можливість самовідтворення. Коли програма вгадувала неправильно, вона просила користувача запропонувати питання, яке дозволило б поліпшити її здібності до відгадування даної тварини. Запам'ятавши це

питання, програма не тільки модифікувала себе, але і намагалася переписати свою оновлену (покращену) копію в інший каталог. Якщо там вже була програма Animal, то вона стиралася. Інакше створювалася нова копія.

Найзнаменитішим вірусом того часу став мережевий вірус Морриса. Аспірант факультету інформатики Корнельського університету інфікував за допомогою написаної ним програми велику кількість комп'ютерів (близько 6000), підключених до американської національної мережі Internet. "Хропак Моріса" вражав тільки комп'ютери типу SUN 3 і VAX, які використовували варіанти ОС UNIX версії 4 BSD. Збитки від нього були оцінені в 96 мільйонів доларів.

Події 1985-86 рр. за часом співпали з швидким зростанням виробництва і різким зниженням цін на ПЕОМ серії IBM PC. Тому другий етап в розвитку вірусів пов'язаний з досягненням "критичної маси" виробництва цього наймасовішого комп'ютера в історії розвитку обчислювальної техніки. В 1987 р., одночасно в декількох країнах відбулися спалахи зараження комп'ютерів вірусами. Віруси почали бути загрозою для всіх користувачів персональних ЕОМ. На відміну від першого етапу, коли розробки вірусоподібних програм носили дослідницький характер, і автори, заручившись згодою користувачів, займалися чистим експериментатором на благо системного програмування, другий етап носить характер протистояння користувачів безвідповідальним або навіть кримінальним "елементам". До числа "першопроходців" на даному етапі відносять бутовий вірус "Brain", розроблений братами Алві. За неперевіреними (і, ймовірно, завищеним) даними, приведеними McAfee, він заразив тільки в США більше 18 тисяч комп'ютерів.

В кінці восьмидесятих паніку в США і західноєвропейських країнах викликала історія з так званою AIDS Information Trojan - троянською програмою, що розповсюджувалася у складі пакету з базою даних про захворювання синдромом придбаного імунодефіциту (СНІД). Як програма, так і база даних були записані на дискеті, яка була розіслана 20 тисячам замовників, включаючи ряд медичних і суспільних організацій США, Франції, Великобританії, ФРН, Данії, Норвегії, Швеції і багатьох інших країн.

На сьогоднішній день ніхто в світі не може вказати точну кількість таких програм, оскільки вони з'являються кожного дня все нові і нові. Але проблема боротьби з такими програмами вимагає щонайменше класифікації вказаних програм.

Класифікація вірусів

Віруси можна розділити на класи за наступними основними ознаками:

- місце існування;
- операційна система (ОС);
- особливості алгоритму роботи;
- деструктивні можливості.

За місцем існування віруси можна розділити на:

- файлові;
- завантажувальні;
- макро;
- мережеві.

Файлові віруси різними способами упроваджуються у виконавчі файли (найбільш поширений тип вірусів), або створюють файли-двійники (віруси компаньйона), або використовують особливості організації файлової системи (link-віруси).

Завантажувальні віруси записують себе в завантажувальний сектор диска (boot-сектор), або в сектор, системний завантажувач вінчестера (Master Boot Record).

Макро-віруси заражають файли-документи і електронні таблиці декількох популярних редакторів.

Мережеві віруси використовують для свого розповсюдження протоколи або команди комп'ютерних мереж і електронної пошти.

Існує велика кількість поєднань - наприклад, файлово-завантажувальні віруси, що заражають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи, часто застосовують оригінальні методи проникнення в систему, використовують стелс і поліморфик-технології. Інший приклад такого поєднання - мережевий макровірус, який не тільки заражає редаговані документи, але і розсилає свої копії за електронною поштою.

Серед особливостей алгоритму роботи вірусів виділяються наступні:

- резидентність;
- використання стелс-алгоритмів;
- самошифрування і поліморфізм;
- використання нестандартних прийомів.

Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення операційної системи до об'єктів зараження і упроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до виключення комп'ютера або перезавантаження операційної системи.

Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус. Такі віруси вважаються нерезидентними. Резидентними можна вважати макро-віруси, оскільки вони постійно присутні в пам'яті комп'ютера на весь час роботи зараженого редактора. При цьому роль операційної системи бере на себе редактор, а поняття "перезавантаження операційної системи" трактуючи як вихід з редактора.

Використання СТЕЛС-алгоритмів дозволяє вірусам повністю або частково приховати себе в системі. Найбільш поширеним стелс-алгоритмом є перехоплення запитів ОС на читання/запис заражених об'єктів. Стелс-віруси при цьому або тимчасово лікують їх, або "підставляють" замість себе незаражені ділянки інформації. У разі макро-вірусів найбільш популярний спосіб - заборона викликів меню проглядання макросів. Один з перших файлових стелс-вірусів - вірус "Frodo", перший завантажувальний стелс-вірус - "Brain".

Самошифрування і поліморфичність використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру детектування вірусу. Поліморфік-віруси (polymorphic) - це віруси, які складно знайти, що не мають сигнатур, тобто що не містять жодної постійної ділянки коду. В більшості випадків два зразки одного і того ж поліморфік-вірусу не матимуть жодного співпадання. Це до-

сягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровування.

Різні нестандартні прийоми часто використовуються у вірусах для того, щоб якомога глибше заховати себе в ядрі ОС (як це робить вірус "ЗАРАЗА"), захистити від виявлення свою резидентну копію (віруси "TPVO", "Trout2"), утруднити лікування від вірусу (наприклад, помістивши свою копію в FLASH-BIOS) і т.д.

За деструктивними можливостями віруси можна розділити на:

- нешкідливі, тобто що ніяк не впливають на роботу комп'ютера (окрім зменшення вільної пам'яті на диску в результаті свого розповсюдження);
- безпечні, вплив яких обмежується зменшенням вільної пам'яті на диску і графічними, звуковими і ін. ефектами;
- небезпечні віруси, які можуть привести до серйозних збоїв в роботі комп'ютера;
- дуже небезпечні, в алгоритм роботи яких свідомо закладені процедури, які можуть привести до втрати програм, знищення даних, стирання необхідної для роботи комп'ютера інформації, яка записана в системних областях пам'яті, і навіть, як свідчить одна з неперевірених комп'ютерних легенд, сприяння швидкому зносу рухомих частин механізмів - вводити в резонанс і руйнувати головки деяких типів вінчестерів.

Але навіть якщо в алгоритмі вірусу не знайдено можливостей, які завдають збитку системі, цей вірус не можна з повною упевненістю назвати нешкідливим, оскільки проникнення його в комп'ютер може викликати непередбачувані і деколи катастрофічні наслідки.

Цикл функціонування вірусів

У циклі існування будь-якого вірусу можна виділити три етапи. Спочатку вірус знаходиться в неактивному стані. У цьому стані він упроваджений в тіло вико-

нуваного файлу або знаходиться в завантажувальному секторі диска і "чекає" своєї години. Саме в неактивному стані віруси переносяться разом з програмами або дискетами від одного ПК до іншого. Зрозуміло, в неактивному стані вірус нічого не може зробити. Для того, щоб він почав свою роботу, необхідно запустити виконуваний файл або завантажитися із зараженої дискети. У цей момент активізується вірус, який або створює резидентну в пам'яті програму, здатну породжувати копії або проводити якісь руйнівні дії, або негайно приступає до роботи.

Якщо вірус створив резидентну програму, то її активізація здійснюється різними способами - все залежить від фантазії автора вірусу. Звичайно вірус перехоплює переривання 21, що є ключовим для доступу до будь-яких операцій з MS-DOS. Таким чином, будь-яка спроба читання або запису інформації на диск або звернення до клавіатури дисплея приводить до активізації резидентної програми вірусу. Після отримання управління (або активізації резидентної програми) вірус приступає до "розмноження": він відшукує відповідний виконавчий файл і упроваджує свій код в його тіло. Як правило, вірус заражає лише один виконавчий файл за раз, щоб користувач не звернув уваги на надмірне уповільнення в роботі програм: другий етап життєдіяльності вірусу - це етап активного розмноження, тому вірусна програма прагне максимально приховати від користувача ПК результати своєї діяльності.

Після того, як заражено достатньо багато файлів, може наступити третій етап, пов'язаний із зовнішніми проявами роботи вірусу. Ваш комп'ютер раптом почне поводитися дивно: чи зазвучить музична фраза, або почнуть "сипатися" символи на екрані дисплея не суть важливо, головне, що тільки у цей момент Ви з жахом пригадаєте, що на жорсткому диску знаходяться надзвичайно важливі дані або програми, які Ви не встигли або не змогли скопіювати на диски. На жаль! Деякі віруси до цього моменту можуть вже безповоротно порушити файлову структуру.

Завантажувальні віруси і боротьба з ними

У епоху розквіту макровірусів і троянців тема завантажувальних і файлово-завантажувальних (boot і multi) вірусів може показатися неактуальною. Дійсно, масовий перехід на Windows створив значні труднощі для виживання DOS-

орієнтованих програм, особливо якщо вони повинні піклується про це самі. Проте в списку WildList (http://www.wildlist.org/) в розділі вірусів, що часто зустрічаються, ще до недавнього часу були присутні AntiExe, ANTICMOS і OneHalf. Для виявлення завантажувальних вірусів в BIOS була введена перевірка запису в сектор головного завантажувального запису (MBR) диска (Virus Warning). За умовчанням ця опція відключена. Крім того, інструкція з установки Windows також вимагає її відключення, інакше нормальний хід установки припиняється без пояснень (насправді попередження про запис в завантажувальний сектор просто не виводиться на екран і необхідно натиснути клавішу "Y", щоб установка продовжилася). Таким чином прихований доступ до MBR і її зміни все ще можливі на комп'ютерах з Win95/98.

Макровіруси

Макровіруси (macro viruses) є програмами написаними на мовах (макромовах), вбудованих в деякі системи обробки даних (текстові редактори, електронні таблиці і т. д.). Для свого розмноження такі віруси використовують можливості макромов і при їх допомозі переносяться з одного зараженого файлу (документа або таблиці) в інші. Найбільшого поширення набули макровіруси для Microsoft Word, Excel із MS Office.

Для існування вірусів в конкретній системі (редакторі) необхідна наявність вбудованої в систему макромови з можливостями:

- прив'язки програми на макромові до конкретного файлу;
- копіювання макропрограм з одного файлу в інший;
- отримання управління макропрограмою без втручання користувача (автоматичні або стандартні макроси).

Описаним умовам задовольняють редактори MS Word, AmiPro, а також електронна таблиця MS Excel. Ці системи містять в собі макромови при цьому:

- макропрограми прив'язані до конкретного файлу (AmiPro) або знаходяться усередині файлу (MS Word/Excel);
- макромова дозволяє копіювати файли (AmiPro) або переміщати макропрограми в службові файли системи і редаговані файли (MSWord /Excel);

- при роботі з файлом за певних умов (відкриття, закриття і т. д.) викликаються макропрограми (якщо такі є), які визначені спеціальним чином (AmiPro) або мають стандартні імена (MS Word/Excel).

Остання особливість призначена для автоматичної обробки даних у великих організаціях або в глобальних мережах і дозволяє організувати так званий «автоматизований документообіг». З іншого боку, можливості макромов таких систем дозволяють вірусу переносити свій код в інші файли і таким чином заражати їх.

У вказаних вище програмних продуктах віруси одержують управління при відкритті або закритті зараженого файлу, перехоплюють стандартні файлові функції і потім заражають файли, до яких яким-небудь чином йде звернення. По аналогії з DOS можна сказати, що більшість макровірусів є резидентними вірусами: вони активні не тільки у момент відкриття або закриття файлу, але до тих пір, поки активний сам редактор.

Поштові віруси

Крім листів, що містять троянців і макровіруси, можуть бути небезпечні і електронні листи, що зовсім не містять ніяких вкладень, зате заражені так званими вірусами скрипта (поштовими вірусами-хропаками). Серед найбільш відомих, слід, зокрема, згадати KakWorm, Stages і ILOVEYOU (LoveLetter). Вони написані на Visual Basic for Applications (VBA), використовують Windows Scripting Host (машину для запуску програм скрипта) і украй небезпечні (наприклад, сумарні збитки від розповсюдження ILOVEYOU перевищили 12 мільярдів доларів). При цьому проти них часто безсилі традиційні антивірусні засоби, які не в силах виявити присутність вірусу, якщо він не звертається до жорсткого диска, а оперує виключно в оперативній пам'яті комп'ютера. Крім того, украй легко (за рахунок середовища розробки) створюються нові варіанти даних вірусів. У разі KakWorm, зараження взагалі відбувається просто при відкритті листа, і не вимагає здійснення яких-небудь ще додаткових дій.

Спам і боротьба з ним

Кого не діставали рекламні листи порно-сайтів або казино, онлайна, що завалюють у величезних кількостях електронні поштові скриньки? Причому спроби відписатися від розсилки ні до чого не привели - листи як приходили, так і продовжують приходити.

Для того, щоб уберегтися від спаму, слід, в першу чергу, не давати свої e-mail-адреси кому не потрібно. Окрім вищепереліченого, в боротьбі із спамом допоможуть спеціально призначені для цього утиліти. Так, наприклад, Telos 2.0 (800 кілобайт, сайт розробника) сканує вміст поштових скриньок на предмет виявлення заголовків спамовых листів (які листи віднести до спаму, визначає сам користувач) і видаляє їх. Програма може працювати в автоматичному режимі, скануючи поштові скриньки через певні проміжки часу. Telos можна налагодитиі для знищення листів, що приходять з певних адрес.

Можна рекомендувати також утиліту Spam Hater 2.09 (834 кілобайти), яка забезпечує найбільш ефективний і гнучкий захист від спаму.

Як боротися з вірусами (типи антивірусних програм)

Сьогодні можна виділити п'ять основних типів антивірусних програм: сканери, монітори, ревізори змін, імунізатори і поведінкові, які блокують.

Сканери — принцип їх роботи полягає в пошуку у файлах, пам'яті, завантажувальних секторах сигнатур вірусів, тобто унікального програмного коду вірусу. Описи відомих вірусів містяться в антивірусній базі даних, і якщо сканер зустрічає програмний код, співпадаючий з одним з цих описів, то він видає повідомлення про виявлення відповідного вірусу.

Монітори — ці резидентні програми є різновидом сканерів і здійснюють автоматичну перевірку всіх використовуваних файлів у реальному часі. Сучасні монітори проводять перевірку у момент відкриття і закриття файлу, виключаючи таким чином запуск раніше інфікованих файлів і зараження файлу резидентним вірусом.

Ревізори змін - принцип роботи ревізорів заснований на знятті оригінальних контрольних сум з можливих об'єктів зараження (файли, завантажувальні сектори,

системний реєстр) і збереженні їх в базі даних. Річ у тому, що, не дивлячись на всі способи маскування, віруси - звичайні комп'ютерні програми. Вони, звичайно ж, мають можливість таємно створювати нові копії або упроваджуватися у вже існуючі об'єкти, але все одно залишають сліди своєї діяльності в операційній системі. При наступному запуску ревізор порівнює контрольні суми з контрольними сумами своєї бази даних і повідомляє користувача про зміни, виділяючи вірусоподібні дії.

Імунізатори - такі програми діляться на два види: імунізатори, що повідомляють про зараження, і імунізатори, які блокують зараження яким-небудь типом вірусу. Перші звичайно записуються в кінець файлу, і кожного разу при запуску файлу проводиться перевірка на його на зміну. Другий тип імунізаторів захищає систему від зараження певним вірусом. Файли модифікуються таким чином, що віруси приймають їх за вже заражені. Зараз цей тип антивірусних програм майже не використовується із-за нездатності виявити зараження вірусами-невидимками.

Поведінкові які блокують – це резидентні програми, що перехоплюють різні події і у разі підозрілих дій (тобто дій, які може проводити вірус або інша шкідлива програма), забороняють вказану дію або запрошують дозвіл у користувача. Вони не здійснюють пошуку унікального програмного коду вірусу (як це роблять сканери і монітори) і не порівнюють файли з їх оригіналами (як ревізори змін), а відстежують і нейтралізують шкідливі програми за їх характерними діями. У перспективі саме такі програми мають реальну можливість з 100-процентною гарантією протистояти атакам нових вірусів. У кожного типу антивірусних програм є як свої переваги і недоліки і лише комплексне використання декількох типів антивірусних програм може привести до прийнятного результату.

Порівняння антивірусних програм

Компанія «Троянер-інфо» протестувала 20 антивірусних і антитроянських програм. Фахівці німецького сайту Троянер-інфо провели чергове тестування антивірусного програмного забезпечення.

Дослідження проводилося 9 листопада на базі AMD Athlon 700, 256 Мб Ram, Windows 2000 Professional. У дослідженні брало участь сто Троянів, як поширених,

так і достатньо рідкісних. Деякі з них були частково модифіковані, або архівуються EXE-архіваторами. В якості критерію перевірки виступала здатність до розпізнавання, але не видалення вірусів. Час сканування одержаний з усередненої швидкості движків, сканерів:

Таблиця 8.1

Деякі показники перевірки антивірусних програм.

Місце	Програма	%	Час сканування (сек)
1	Kaspersky Anti-Virus	99	9
1	AVK	99	23
2	McAfee	97	10
3	PC Door Guard	88	18
3	PC-Cillin	88	28
4	TDS	87	15
5	Dr. Web	86	6
6	ANTS	85	3
7	Norman	84	58
8	NOD32	82	1
9	FP-Win	80	3
10	Anti-Trojan	79	2

На жаль, багато антивірусних програм дотепер пропускають навіть найпоширеніші трояни, не говорячи вже про новітні віруси.

Прояв наявності вірусу в роботі на ПЕОМ.

Всі дії вірусу можуть виконуватися достатньо швидко і без видачі яких-небудь повідомлень, тому користувачу дуже важко відмітити, що в комп'ютері відбувається щось незвичайне.

Поки на комп'ютері заражені відносно мало програм, наявність вірусу може бути практично непомітною. Проте після деякого часу на комп'ютері починає творитися щось дивне, наприклад:

- деякі програми перестають працювати або починають працювати неправильно;
- на екран виводяться сторонні повідомлення, символи і т.д.;
- робота на комп'ютері істотно сповільнюється;
- деякі файли виявляються зіпсованими і т.д.

До цього моменту, як правило, вже достатньо багато (або навіть більшість) програм є зараженими вірусом, а деякі файли і диски - зіпсованими. Більш того, заражені програми з одного комп'ютера могли бути перенесені за допомогою дискет або за локальною мережею на інші комп'ютери.

Деякі види вірусів поводяться ще підступніше. Вони спочатку непомітно заражають велике число програм або дисків, а потім заподіюють дуже серйозні пошкодження, наприклад, форматують весь жорсткий диск на комп'ютері. А бувають віруси, які прагнуть поводитися якомога більш непомітно, але помалу і поступово псують дані на жорсткому диску комп'ютера.

Таким чином, якщо не вживати заходи з захисту від вірусу, то наслідки зараження комп'ютера можуть бути дуже серйозними.

Звідки беруться віруси і як уникнути зараження

Основним джерелом вірусів на сьогодні є Internet. Найбільше число заражень вірусом відбувається при обміні листами у форматах MS Word: користувач зараженого макровірусом редактора, сам того не підозрюючи, розсилає «інфіковані» листи своїм адресатам, а вони розсилають нові листи і т.д.

Припустимо, що користувач веде листування з десятьма адресатами, кожний з яких, у свою чергу, веде листування також з десятьма адресатами. Після посилки «вірусного» листа всі десять комп'ютерів, що одержали його, виявляються зараженими. На другому рівні розсилки будуть заражені вже 1+10+100=111 комп'ютерів. Описаний випадок розповсюдження вірусу найчастіше реєструється антивірусними компаніями. Але нерідкі випадки, коли заражений файл-документ або таблиця Excel унаслідок недогляду потрапляє в списки розсилки комерційної інформації якої-небудь великої компанії. В цьому випадку постраждають вже не десять, а сотні або

навіть тисячі абонентів таких розсилок, які потім розішлють заражені файли десяткам тисячам своїх абонентів.

Файл-сервери загального користування і електронні конференції також служать одним з основних джерел розповсюдження вірусів. Практично кожного тижня приходить повідомлення про те, що хтось з користувачів заразив свій комп'ютер вірусом, який був одержаний з BBS (дошки об'яв), ftp-сервера або електронної конференції.

При цьому часто заражені файли «закачуються» автором вірусу на декілька BBS/ftp або розсилаються за декількома конференціями під виглядом нових версій якого-небудь програмного забезпечення (аж до антивірусів).

У разі масової розсилки вірусу в файл-сервери BBS/ftp ураженими одночасно можуть виявитися тисячі комп'ютерів, проте в більшості випадків «розсилаються» DOS- або Windows-віруси, швидкість розповсюдження яких в сучасних умовах значно нижче, ніж у їх макропобратимів. З цієї причини подібні інциденти практично ніколи не кінчаються масовими епідеміями.

Третій шлях швидкого розповсюдження вірусів — локальні мережі. Якщо не вживати необхідних заходів захисту, то заражена робоча станція при вході в мережу заражає один або декілька службових файлів на сервері, різне програмне забезпечення, стандартні документи-шаблони або Excel-таблиці, вживані у фірмі, і т.д.

Небезпеку представляють також комп'ютери, встановлені в учбових закладах. Якщо один із студентів приніс на своїх дискетах вірус і заразив який-небудь з учбових комп'ютерів, то чергову «заразу» одержить і вся решта студентів, що працюють на цьому комп'ютері.

Те ж відноситься і до домашніх комп'ютерів, якщо на них працює більше однієї людини. Нерідкі ситуації, коли син-студент (або дочка), працюючи на розрахованому на багато користувачів комп'ютері в інституті, перетягують вірус на домашній комп'ютер, внаслідок чого вірус потрапляє в комп'ютерну мережу фірми тата або мами.

На закінчення хочеться відзначити, що, не дивлячись на складність боротьби, з макровірусами, забезпечити себе від цієї «інфекції» при спокійному і грамотному підході до проблеми не так вже складно.

Достатньо рідко, але дотепер цілком реально заразити свій комп'ютер вірусом при його ремонті або профілактичному огляді. Ремонтники — теж люди, і деяким з них властивий наплювацький підхід до елементарних правил комп'ютерної безпеки.

Захист від вірусів

У сучасному комп'ютеризованому світі важливу роль грає захист від несанкціонованого проникнення на комп'ютер і в мережу за допомогою вірусів і троянців. Щоб запобігти зараженню вірусами і атакам троянців, дотримуйтеся наступних рекомендацій.

Користувачам:

- Прагніть дізнатися якомога більше про віруси і способи їх розповсюдження. Вірус можна випадково занести в мережу, запустивши програму, одержану, наприклад, з Інтернету, з електронної дошки оголошень (Bulletin Board System, BBS) або у вигляді вкладення в повідомлення електронної пошти;
- Найбільш загальні ознаки зараження вірусами наступні: на екрані з'являються незвичайні повідомлення, знижується продуктивність системи, відсутні деякі дані або неможливо дістати доступ до жорсткого диска. При виникненні подібних неполадок на комп'ютері негайно запустите антивірусну програму, щоб понизити вірогідність втрати даних;
- Програми на дискетах, флешках і т.д. також можуть містити віруси. Перевіряйте їх на наявність вірусів, перш ніж копіювати або відкривати файли, що містяться на них, або виконувати завантаження комп'ютера;
- Необхідно придбати хоч би одну комерційну антивірусну програму і регулярно користуватися нею для перевірки комп'ютерів. Оскільки нові віруси створюються щодня, прагніть оперативно поповнювати свій набір файлів сигнатур вірусів новими сигнатурами.

Адміністраторам:

- Перш ніж розміщувати новий додаток в мережі, встановіть його на комп'ютері, не підключеному до мережі, і перевірте за допомогою антивірусних засобів. (Взагалі кажучи, в свою систему рекомендується входити як член групи «Користувачі», проте установку програми для перевірки слід виконувати, увійшовши до системи з обліковим записом члена локальної групи «Адміністратори», оскільки не всі програми успішно встановлюються членами групи «Користувачі».);
- Не дозволяйте користувачам входити на їх комп'ютери з обліковими записами членів групи «Адміністратори», оскільки віруси стають набагато небезпечніше, якщо вони активізуються від імені облікового запису з правами адміністратора. Користувачі повинні входити в систему як члени групи «Користувачі»; таким чином вони володітимуть лише дозволами, необхідними для виконання своїх завдань;
- Вимагайте від користувачів створювати надійні паролі, щоб віруси не могли легко підібрати пароль і одержати права адміністратора. (Вимоги до паролів можна встановити за допомогою оснащення «Групова політика».).
- Регулярна архівація файлів дозволить мінімізувати збиток від вірусної атаки.

Розглянемо на прикладі можливості деяких антивірусних програм.

Пошук, заборона та видалення несанкціонованих дій програм за допомогою програми AD-AWARE 6.0

Програма працює з операційними системами Windows 98 / 98SE / NT4 / 2000 / XP. Вона дозволяє проводити пошук та видалення спроб несанкціонованих змін у системі, спроб встановити нових програм без санкцій користувача при роботі в Internet, агресивної реклами, паразито-схожого програмного забезпечення, програм

запам'ятовування активних клавіш клавіатури, закладкок, наприклад, типу “Троянські”, складачів номера, програм, які заважають коректній роботі броузера, а також дозволяє відстежувати їх компоненти. Ad-aware 6.0 всесторонньо сканує пам'ять комп'ютера, реєстри операційної системи, жорсткі, гнучкі і оптичні диски. Ad-aware 6.0 забезпечить непошкодженою конфіденційність під час роботи в Internet.

Програма має навігатор процесу, який повністю підтримує поглиблений процес сканування. Процес сканування, який налагоджується попередньо користувачем повністю автоматизований, в тому числі, здатність поміщати в каталог карантин всі підозрілі файли. Експорт і друк звітів HTML. Маються опції командного рядка, щоб завантажити конфігураційні сценарії та посилання з віддалених дисків, і відправлення файлів протоколів на віддалені диски. Блокуються спроби забрати управління броузером, в тому числі, забороняється запуск програм і файлів, перелік яких наведений в списку фільтрів.

Ad-aware 6.0 має розвинуту довідкову систему, яка показує важливі деталі, такі як, наприклад, дата останньої повної перевірки системи, загальна статистика використовування. В панелях інструментів мається кнопка зі знаком запитання, яка дозволяє оперативно отримувати підказку.

При скануванні системи доступні наступні дані:

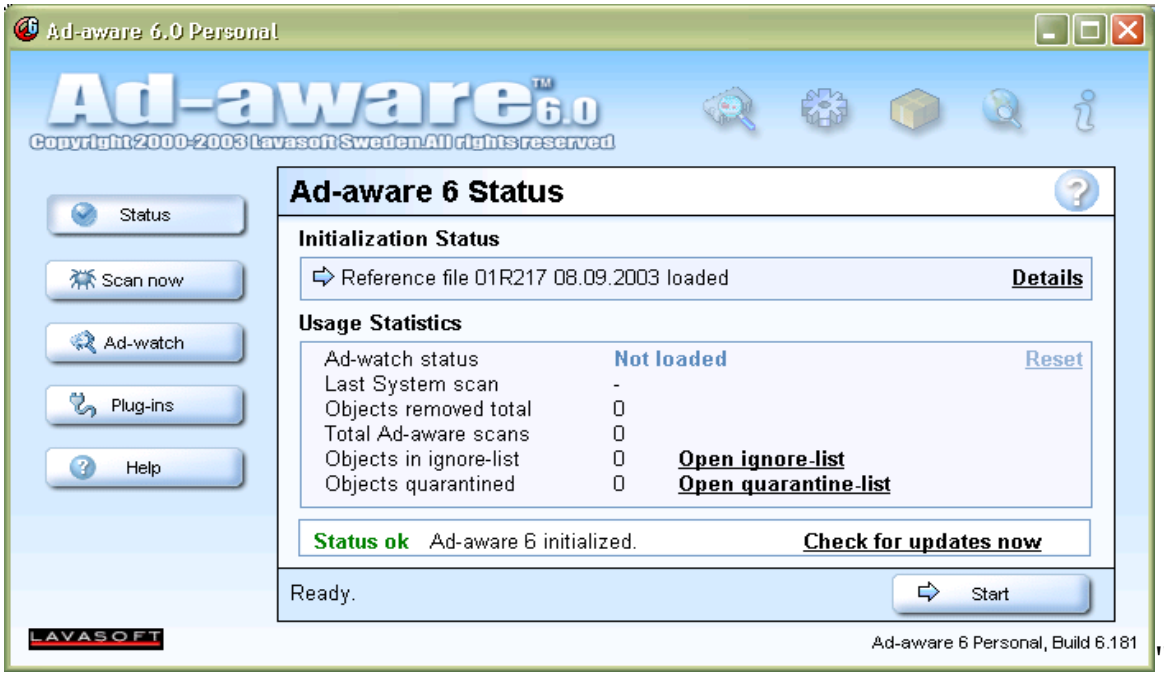
- Дата сканування;
- Повне число сканувань системи;
- Повне число видалених елементів і можливість перегляду їх;
- Повне число елементів в ігноруючому списку й можливість перегляду їх;
- Повне число об'єктів у карантині (не число архівів).

Таким чином програма дозволяє боротися з багатьма типами елементів упровадження в комп'ютерну систему.

Варіанти типового сканування:

"Scan within Archives" - використовує варіанти типового сканування. Для зміни параметрів сканування необхідно ввійти у вікно налагодження параметрів (рис. 8.2).

"Skip non executable files"-- ввести діалог "вибрані каталоги для сканування", а потім уручну вибрати те, що треба сканувати.



"Skip files greater than [x] KB" -- виконуйте швидке сканування системи.

Рис. 8.1. Вікно програми

Головне меню програми

В вікні програми (рис. 8.1) доступні п'ять команд.

Status - показує екран статусу.

Scan now - скануйте зараз - показує екран підготовки системи до сканування.

Ad-Watch -- запускає утиліту Watch.

Plug-ins-- показує екран додаткових модулів.

Help -- допомога - відкриває інструкції для користувача.

Справа вгору у вікні програми розташовані п'ять кнопок, які мають наступні функції:

 Open Ad-Watch.

Settings- відкриває вікно конфігурації "Установок" (мал. 2).

Objects in Quarantine -- відкриває вікно "піддані карантину об'єкти".

Open WebUpdate – відкриває вікно оновлення програми за Internet.

About Ad-aware 6.0 – надає відомості про програму

Початок сканування

Перед скануванням треба якомога детальніше продумати мету та план сканування системи. Для початку сканування натисніть кнопку **Scan now** з'явиться вікно (рис. 8.3).

В указаному вікні необхідно відібрати один із трьох доступних методів сканування.

Perform smart system-scan – виконайте сканування системи;

Use custom scanning optins – виберіть параметри сканування, після натиску на кнопці **Customize** з'явиться вікно (рис. 8.4).

Select drives\folders to scan --виберіть диск\каталог для сканування, після натиску на кнопці **Select** з'явиться вікно (рис. 8.5).

Для початківців рекомендується починати сканування за наступними параметрами (мал. 8.4):

- "Scan within Archives" - використовуйте варіанти типового сканування;

- "Automatically save log-file"-- автоматична реєстрація-файла збереження;

Рис. 8.2. Вікно налагодження параметрів

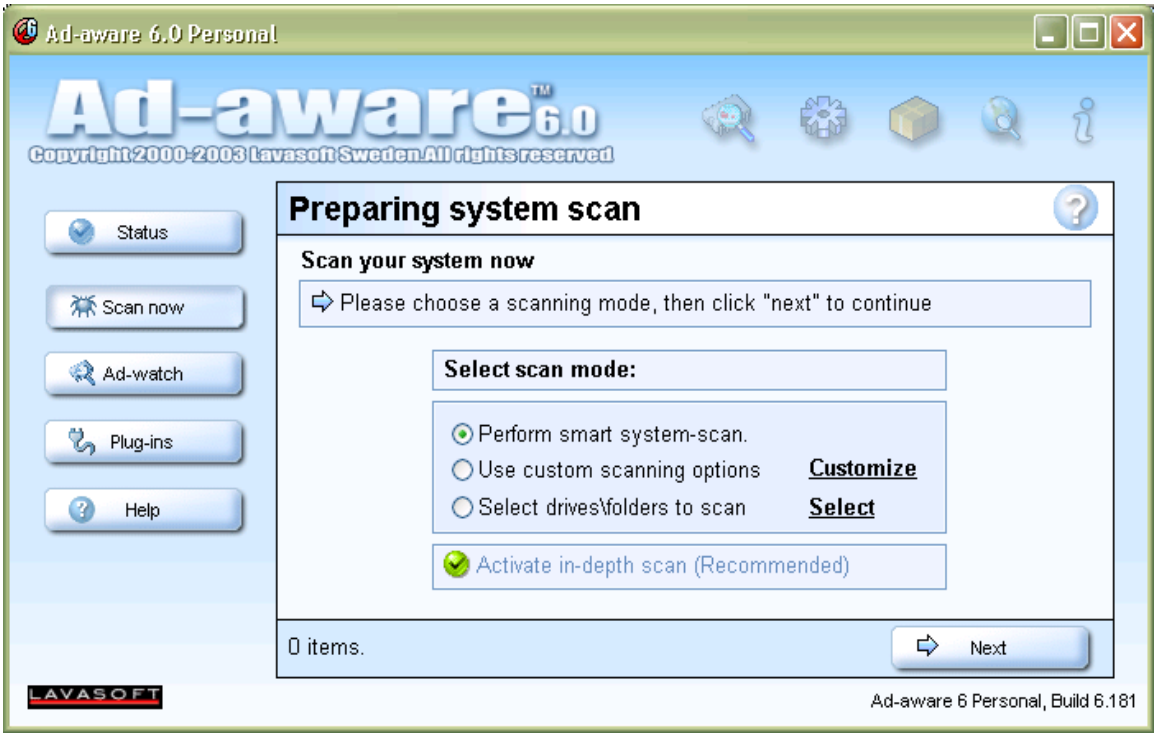


Рис. 8.3. Вікно початку сканування

Рис. 8.4. Вікно налагодження параметрів сканування

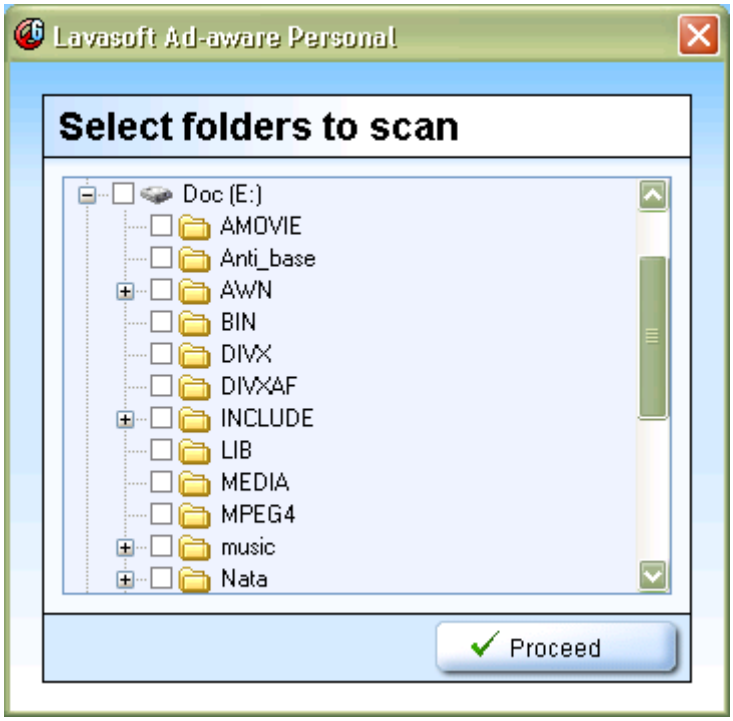


Рис. 8.5. Вікно відбору дисків та каталогів для сканування

- "Automatically quarantine objects prior to removal"-- автоматично карантинні об'єкти до видалення;

"Safe mode" -- режим, при якому завжди запрошується дозвіл користувача до ініціації будь-якого позову або процедури;

"Scan within Archives" – сканування, тому числі, архівів, неможливе старе дублювання “підозрілого” матеріалу.

"Skip non executable files" – в початковому варіанті сканування цей режим не рекомендується, оскільки при скануванні можуть бути пропущенні деякі файли.

"Skip files greater than [x] KB" --в початковому варіанті сканування цей режим не рекомендується, оскільки при скануванні можуть бути пропущенні файли за розмірами більші від указаних.

"Memory and Registry" – сканування пам'яті та реєстрів.

"Scan active processes" – сканування активних процесів.

"Scan registry” – використовується разом із наступним пунктом.

"Deep Scan Registry" -- глибоке сканування реєстру операційної системи.

При використанні програми Internet Explorer можна застосовувати наступні параметри сканування:

"Scan my IE Favorites for banned URL's” – сканує і видаляє підозрілий уміст файлів.

"Scan my Hosts file” -- сканує і видаляє підозрілий уміст файлів.

Після сканування при наступному скануванні будуть використовуватися вказані параметри. Треба вказати на деякі користі параметри налагоджування програми з вікна (рис. 8.2):

Automatically save log-file -- автоматично створює файл реєстрації для кожного сканування.

Automatically quarantine objects prior to removal - автоматично створює карантин (дублювання) знайдених елементів до видалення елементів із системи.

Safe mode (always request confirmation) - сповіщає і просить про дозвіл до видалення знайдених елементів.

Language file - показує меню файлів мови.

Scan active processes - зараз завантажені процеси скануються.

Move deleted files to recycle bin - автоматичне видалення елементів до корзини.

Load Ad-watch on windows start up – нагляд почнеться із запуском операційної системи.

Perform quick system check" -чистіть автоматично" – програма буде сканувати автоматично систему, а потім виключить будь-які цілеспрямовані компоненти впровадження без дозволу користувача.

Дії зі списком карантин

Карантин-файли використовуються, щоб ізолювати їх та як елементи дублювання. Елементи, переміщені на карантинну теку, кодуватимуться і стискатимуться, і можуть тільки читатися й відновлюватися, використання їх виконується за допомогою карантин-менеджера.

Кожний елемент у списку карантину може відображатись в чотирьох параметрах :

File name -ім'я файлу - дата, і карантин. Карантин-архіви-- збережені з розширенням .bckp.

Size - розмір - повний розмір всіх об'єктів у межах карантину-архіву.

Creation Date --дата створення - місяць, день, і рік, на якому карантин-архів був створений.

Objects Total -підсумок об'єктів - повне число об'єктів у межах карантину-архіву.

Над списком карантину можна виконувати наступні дії:

Item details --деталі елементу - показує карантинну реєстрацію, містячи імена всіх об'єктів, що входять в архів.

Reinstall --переустановіть - встановлює заново вміст від відібраного архіву та оригінального розташування елементів, до їх, видалення.

Delete archive - видаліть архів - видаляє відібраний архів.

Delete all archives -видаліть всі архіви - видаляє всі карантин-архіви відразу.

Help -допомога - відкриває інструкції для користувача.

Результати сканування

Під час сканування на екрані вказується яка частина системи сканується і яка виконується дія, надається короткий перегляд про знайдений підозрілий уміст.

Після закінчення сканування (рис.8.6) можна отримати наступні дані:

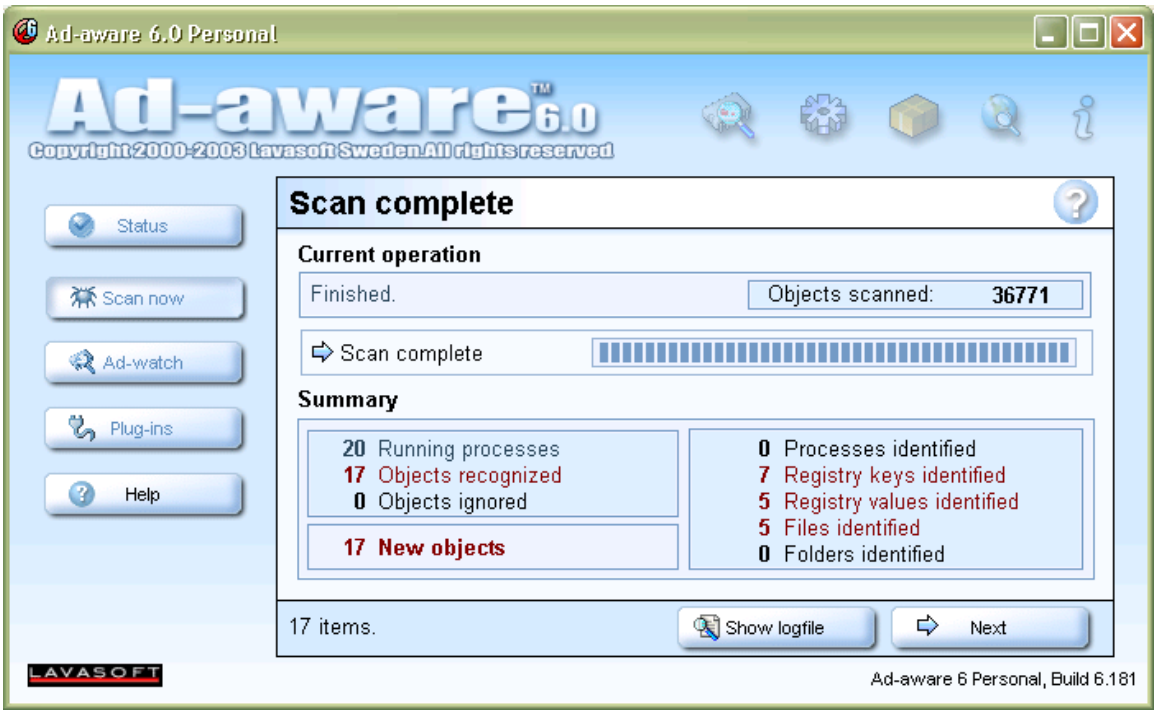


Рис. 8.6. Результати сканування

Увівши команду Next можна виділити елементи , які підлягають видаленню (рис. 8.7)

1. Running Processes-- запуск процесів - деталі процесів входять у заключний звіт файлу реєстрації.

2.Objects recognized -- визнані об'єкти - це підсумок запуску всіх знайдених об'єктів.

3. Objects ignored – об'єкти, якими нехтують - це підсумок запуску всіх об'єктів, якими нехтуватимуть, тому що споживач додав їх до списку, якими нехтують. Вони не будуть показані в результаті-списку сканування і будуть недійсні для видалення.

4. New Objects - нові об'єкти - це підсумок запуску всіх недавно знайдених елементів, яких немає в ігноруючому списку.

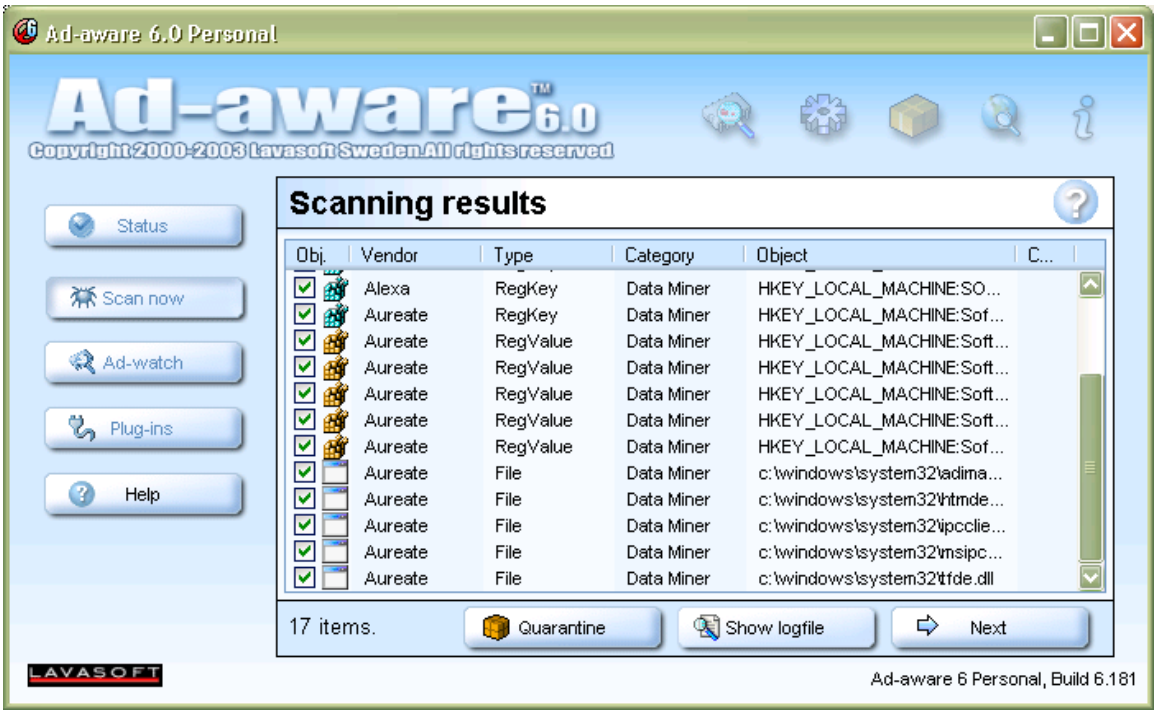


Рис. 8.7 Виділення елементів для подальшого видалення

5. Detected content breakdown -- знайдений дефект вмісту - це більша секція з правої сторони. В ній відображено наступне:

- Processes identified - ідентифіковані процеси - це повне число знайдених небезпечних процесів;
- Registry keys identified -реєстраційні ідентифіковані ключі - це повне число цілеспрямованих або підозрілих реєстраційних ключів;
- Registry values identified - реєстраційні ідентифіковані значення - це повне число підозрілих реєстраційних значень;
- Files identified - ідентифіковані файли - це повне число підозрілих файлів;
- Folders identified - ідентифіковані каталоги - це число підозрілих каталогів.

Після закінчення сканування переглянути звіт (рис. 8.8), можна натиснувши кнопку "**Show log file**".

Додавання елементів до списку ігнорування

В списку результату сканування, виділіть всі елементи, якими потрібно нехтувати.

Уведіть команду "**Add selection to ignore-list**".

Уведіть команду "**OK**".

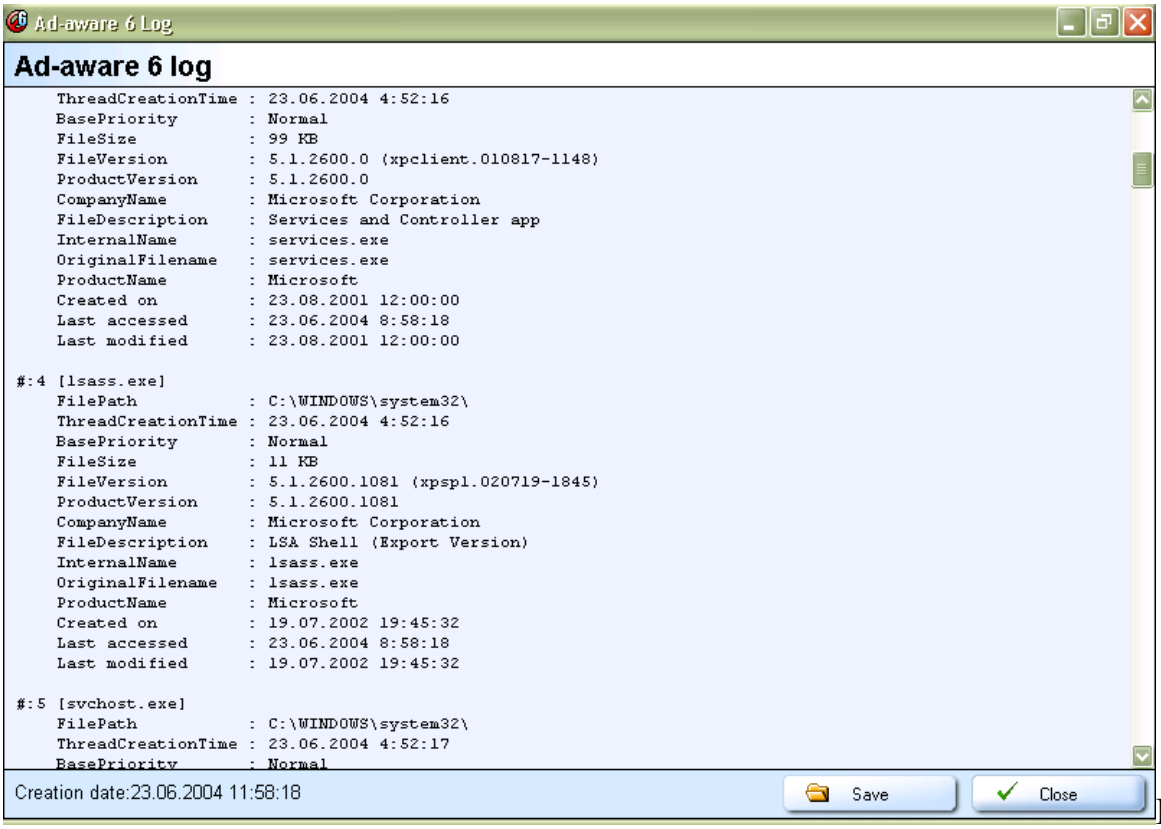


Рис. 8.8. Перегляд звіту.

КОНТРОЛЬНІ ПИТАННЯ

1. Класифікація вірусів
2. Цикл функціонування вірусів
3. Завантажувальні віруси і боротьба з ними
4. Макровіруси
5. Поштові віруси
6. Як боротися з вірусами (типи антивірусних програм)
7. Призначення програми Ad-aware 6.0 .
8. Варіанти типового сканування.
9. Головне меню програми.
10. Порядок сканування.
11. Дії над списком карантин.

12.Отримання результатів сканування.

13.Додавання елементів до списку ігнорування

СПИСОК ВИКОРИСТАННОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

ОСНОВНА ЛІТЕРАТУРА

1. Домарев В.В. Безопасность информационных технологий. -- Санкт-Петербург: DiaSoft, 2002,-688с.

2. Зегжда Д.П., Калинин М.О., Степанов П.Г.Теоретические основы информационной безопасности. Защищенные операционные системы. Руководство к практическим занятиям/ под редакцией проф. Зегжды П.Д. Санкт-Петербург, 1998 г. - 69стр.

3. Конев И., Беляев А. Информационная безопасность предприятия. – Санкт-Петербург: БХВ Петербург, 2003,-752с.

4. Методы и средства защиты информации. /Під ред. Ю.С. Ковтанюка. -- К.: ЮНИОР, 2003, -501с.

ДОДАТКОВА ЛІТЕРАТУРА

5. Ахрамович В.М. Захист інформації під час застосування особистої системи мережевого захисту McAfee Personal Firewall Plus. Науковий Вісник Державної академії статистики, обліку та аудиту 2006, №2.-с.87-96.

6. Ахрамович В.М. Захист інформації під час застосування операційної системи Windows XP. Науковий Вісник Державної академії статистики, обліку та аудиту 2007, №2.-с.92-105.

7. Ахрамович В.М. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисципліни «Інформаційна безпека» (для магістрів).-К.:МАУП,2007.-42с.

8. Ахрамович В.М. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисципліни «Комп’ютерна безпека» (для спеціалістів).-К.:МАУП,2007.-42с.

9. Ахрамович В.М. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисципліни «Технології захисту інформації» (для бакалаврів).-К.:МАУП,2007.-40с.

10. Ахрамович В.М. Резервування систем інформації в Norton Ghost. Науковий Вісник Державної академії статистики, обліку та аудиту 2007, №4.-с.90-104.

11. Баранов А.П., Зегжда Д.П., Зегжда П.Д., Ивашко А.М., Корт С.С. Теоретические основы информационной безопасности (Дополнительные главы) Учебное пособие. Санкт-Петербург, 1998 г.-173стр.

12. В. Жельников. Криптография от папируса до компьютера. – М.: ABF, 1996.

13. Галатенко В.А., Гагин А.В., "Информационная безопасность-обзор основных положений (часть 1,2,3)", Jet INFO, # 1,2,3, 1996.

14. Герасименко В.А., Размахнин М.К. Криптографические методы в автоматизированных системах. Зарубежная радиоэлектроника,1982.-№8

15. Дж. Л. Месси. Введение в современную криптологию. ТИИЭР, т.76, №5, Май 88 – М.: Мир, 1988.- с.24-42.

16. Защита компьютерных систем от разрушающих программных воздействий./ Под редакцией проф. Зегжды П.Д. Руководство к практическим занятиям. - Санкт-Петербург, 1998 г. - 128стр.

17. Зегжда Д.П., Корт С.С., Каулио В.В. Теоретические основы информационной безопасности. Руководство к практическим занятиям.// Под редакцией проф. Зегжды П.Д. - Санкт-Петербург, 1998 г. - 34стр.

18. Зегжда П.Д., Копылов Д.Ю., Корт С.С., Медведовский И.Д., Семьянов П.В., Ростовцев А.Г., Федоров А.В., Фомин А.А. Защита информации в компьютерных системах. Лабораторный практикум.// Под редакцией проф. Зегжды П.Д. - Издание СПбГТУ, 1996 г. - 89с.

19. Клоков Ю.К., Папушин В.К., Хамитов Р.Р. Методы повышения надежности программного обеспечения. Зарубежная радиоэлектроника, 1984, №6.- с. 3-22.

20. Медведовский И.Д., Безгачев В.А., Гореленков А.П. Информационная безопасность распределенных вычислительных систем. Руководство к практическим занятиям//Под редакцией проф. Зегжды П.Д.Санкт-Петербург, 1998 г. - 73с.

21. Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. 2-е изд. - М.: Энергоатомиздат, 1997. - 304 с.

22. Проскуряков А.М. Интеллектуальная собственность. - Вологда: Ардвисура, 1998.

23. Ростовцев А.Г., Маховенко Е.Б.Теоретические вопросы криптологии. Несимметричные криптоалгоритмы и элементы криптоанализа. Руководство к практическим занятиям// Под редакцией проф. Зегжды П.Д.Санкт-Петербург, 1998 г. - 47с.

24. Хорев А.А. Способы и средства защиты информации. - М.: МО РФ, 1998. - 316 с.

25. Щербаков А. Построение программных средств защиты от копирования. Практические рекомендации. Москва, Эдэль, 1992,

26. Ярочкин В.И. Безопасность информационных систем. - М.: Ось-89, 1996.

27. Ярочкин В.И. Система безопасности фирмы. - М.: Ось-89, 1998.

28. Ярочкин В.И. Технические каналы утечки информации. - М.: ИПКИР, 1994. -105 с.

ДОДАТОК 1

Р о з д і л XVI

Злочини у сфері використання електронно- обчислю-вальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислюваль-них машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації,

- карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,

- караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Примітка. Значною шкодою у статтях 361 - 363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода,

яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

(Стаття 361 в редакції Законів N 908-IV (908-15) від 05.06.2003, N 2289-IV (2289-15) від 23.12.2004)

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,

-караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

(Кодекс доповнено статтею 361-1 згідно із Законом N 2289-IV (2289-15) від 23.12.2004)

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях

такої інформації

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства,

- караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,

- караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

(Кодекс доповнено статтею 361-2 згідно із Законом N 2289-IV
(2289-15) від 23.12.2004)

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютер- них мережах або зберігається
на носіях такої інформації, вчинені особою, яка
має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї,

- караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до

двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації,

- караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,

- караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

(Стаття 362 в редакції Закону N 2289-IV (2289-15) від 23.12.2004)

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку

чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію,

- караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

(Стаття 363 в редакції Закону N 2289-IV (2289-15) від

)

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,

- карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду,

- караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

ДОДАТОК 2

Стандартні паролі до системи BIOS.

Універсальні паролі до AWARD BIOS версій:

2.50	2.51	2.51G	2.51U	4.5x
AWARD_SW	AWARD_WG	g6PJ	1EAAh	AWARD_SW
j262	j256	j322	condo	AWARD_PW
TTPTHA	BIOSTAR	ZJAAADC	biostar	589589
01322222	HLT	Wodj	CONDO	PASSWORD
KDD	ZAAADA	bios*	CONCAT	SKY_FOX
ZBAAACA	Syxz	biosstar	djonet	AWARD SW
aPAf	?award	h6BB	efmukl	award.sw
lkwpeter	256256	HELGA-S	g6PJ	AWARD?SW
t0ch88	alfarome	HEWITT RAND	j09F	award_?
t0ch20x	SWITCHES_SW	HLT	j64	award_ps
h6BB	Sxyz	t0ch88	zbaaaca	ZAAADA
j09F	SZYX	zjaaadc		
TzqF	t0ch20x			

Універсальні паролі до AMI BIOS:

AMI	AMI_SW - не універсальний, але встановлюється при скиданні CMOS/SETUP'a
SER	Ctrl+Alt+Del+Ins (тримати при завантаженні, іноді просто INS)

A.M.I.	aammii	ami.kez	ami°	amiami
AMI!SW	AMI.KEY	AMI?SW	AMISETUP	AMI~

AMIPSWD	amipswd	helgaЯs	bios310	amidecod
BIOSPASS	CMOSPWD	HEWITT RAND	KILLCMOS	

Універсальні паролі до AMPTON BIOS:

Polrty

Універсальні паролі до AST BIOS:

SnuFG5

Універсальні паролі до BIOSTAR BIOS:

Biostar
Q54arwms

Універсальні паролі до COMPAQ BIOS:

Compaq

Універсальні паролі до CONCORD BIOS:

last

Універсальні паролі до CTX International BIOS:

CTX_123

Універсальні паролі до CyberMax BIOS:

Congress

Універсальні паролі до Daewoo BIOS:

Daewuu

Універсальні паролі до Daytek BIOS:

Daytec

Універсальні паролі до DELL BIOS:

Dell

Універсальні паролі до Digital Equipment BIOS:

komprie

Універсальні паролі до Enox BIOS:

xo11n

Універсальні паролі до Epox BIOS:

central

Універсальні паролі до Freetech BIOS:

Posterie

Універсальні паролі до HP Vectra BIOS:

hewlpack

Універсальні паролі до IBM BIOS:

IBM
MBIUO
sertafu

Універсальні паролі до Iwill BIOS:

iwill

Універсальні паролі до JetWay BIOS:

spoom1

Універсальні паролі до Joss Technology BIOS:

57gbz6
technolgi

Універсальні паролі до M Technology BIOS:

mMm

Універсальні паролі до MachSpeed BIOS:

sp99dd

Універсальні паролі до Magic-Pro BIOS:

prost

Універсальні паролі до Megastar BIOS:

star

Універсальні паролі до Megastar BIOS:

sldkj754
xyzall

Універсальні паролі до Micronics BIOS:

dn_04rjc

Універсальні паролі до Nimble BIOS:

xdfk9874t3

Універсальні паролі до Packard Bell BIOS:

bell9

Універсальні паролі до QDI BIOS:

QDI

Універсальні паролі до Quantex BIOS:

te1
xljlbj

Універсальні паролі до Research BIOS:

Col2ogro2

Універсальні паролі до Shuttle BIOS:

Col2ogro2

Універсальні паролі до Siemens Nixdorf BIOS:

SKY_FOX

Універсальні паролі до SpeedEasy BIOS:

lesarot1

Універсальні паролі до SuperMicro BIOS:

ksdjfg934t

Універсальні паролі до Tinys BIOS:

tiny

Універсальні паролі до TMC BIOS:

BIGO

Універсальні паролі до Toshiba BIOS:

Toshiba
24Banc81
toshy99

Універсальні паролі до Vextrec Technology BIOS:

Vextrex

Універсальні паролі до Vobis BIOS:

merlin

Універсальні паролі до WIMBIOSnbsp v2.10 BIOS:

Compleri

Універсальні паролі до Zenith BIOS:

3098z
Zenith

Універсальні паролі до ZEOS BIOS:

Zeosx

ДОДАТОК 3

Список портів

1=TCP-MUX - TCP Port Service Multiplexer

2=COMPRESSNET - Management Utility

3=COMPRESSNET - Compression Process

5=RJE - Remote Job Entry

7=ECHO - Echo

9=DISCARD - Discard

11=SYSSTAT - System Status

13=DAYTIME - Daytime

15=NETSTAT - Network Status

17=QOTD - Quote of the Day

18=MSP - Message Send Protocol

19=CHARGEN - Character Generator

20=FTP-DATA - File Transfer Protocol [Default Data]

21=FTP - File Transfer Protocol [Control]

22=SSH - SSH (Secure Shell) Remote Login Protocol

1426=SAIS - Satellite-data Acquisition System 1

1427=MLOADD - mloadd monitoring tool

1428=INFORMATIK-LM - Informatik License Manager

1429=NMS - Hypercom NMS

1430=TPDU - Hypercom TPDU

1431=RGTP - Reverse Gossip Transport

1432=BLUEBERRY-LM - Blueberry Software License Manager

1433=MS-SQL-S - Microsoft-SQL-Server

1434=MS-SQL-M - Microsoft-SQL-Monitor

1435=IBM-CICS - IBM CICS

1436=SAISM - Satellite-data Acquisition System 2

1437=TABULA - Tabula

1438=EICON-SERVER - Eicon Securi-

23=TELNET - Telnet

24=PMS - Private Mail System

25=SMTP - Simple Mail Transfer Protocol

27=NSW-FE - NSW User System FE

29=MSG-ICP - Messege ICP

31=MSG-AUTH - Messege Authentication

33=DSP - Display Support Protocol

35=PPS - Private Printer Server

37=TIME - Time

38=RAP - Route Access Protocol

39=RLP - Resource Location Protocol

41=GRAPHICS - Graphics

42=NAMESERVER - Host Name Server

43=WHOIS - Who Is

44=MPM-FLAGS - MPM FLAGS Protocol

45=MPM - Message Processing Module [recv]

46=MPM-SND - MPM [default send]

ty Agent/Server

1439=EICON-X25 - Eicon X25/SNA Gateway

1440=EICON-SLP - Eicon Service Location Protocol

1441=CADIS-1 - Cadis License Management

1442=CADIS-2 - Cadis License Management

1443=IES-LM - Integrated Engineering Software

1444=MARCAM-LM - Marcam License Management

1445=PROXIMA-LM - Proxima License Manager

1446=ORA-LM - Optical Research Associates License Manager

1447=APRI-LM - Applied Parallel Research LM

1448=OC-LM - OpenConnect License Manager

1449=PEPORT - PEport

47=NI-FTP - NI FTP (File Transfer Protocol)

48=AUDITD - Digital Audit Daemon

49=BBN-LOGIN - Login Host Protocol (TACACS)

50=RE-MAIL-CK - Remote Mail Checking Protocol

51=LA-MAINT - IMP Logical Address Maintenance

52=XNS-TIME - XNS Time Protocol

53=DOMAIN - Domain Name Server

54=XNS-CH - XNS Clearinghouse

55=ISI-GL - ISI Graphics Language

56=XNS-AUTH - XNS Authentication

57=MTP - Private terminal access

58=XNS-MAIL - XNS Mail

59=PFS - Private File System

60=Unassigned

61=NI-MAIL - NI MAIL

62=ACAS - ACA Services

63=WHOIS++ - whois++

64=COVIA - Communications Integra-

1450=DWF - Tandem Distributed Workbench Facility

1451=INFOMAN - IBM Information Management

1452=GTEGSC-LM - GTE Government Systems License Man

1453=GENIE-LM - Genie License Manager

1454=INTERHDL_ELMD - interHDL License Manager

1455=ESL-LM - ESL License Manager

1456=DCA - DCA

1457=VALISYS-LM - Valisys License Manager

1458=NRCABQ-LM - Nichols Research Corp.

1459=PROSHARE1 - Proshare Notebook Application

1460=PROSHARE2 - Proshare Notebook Application

1461=IBM_WRLESS_LAN - IBM Wireless LAN

tor (CI) **65=TACACS-DS - TACACS-Database Service** **66=SQL*NET - Oracle SQL*NET** **67=BOOTPS - Bootstrap Protocol Server** **68=BOOTPC - Bootstrap Protocol Client** **69=TFTP - Trivial File Transfer Protocol** **70=GOPHER - Gopher** **71=NETRJS-1 - Remote Job Service** **72=NETRJS-2 - Remote Job Service** **73=NETRJS-3 - Remote Job Service** **74=NETRJS-4 - Remote Job Service** **75=PDOS - Private dial out service** **76=DEOS - Distributed External Object Store** **77=RJE - Private RJE (Remote Job Entry) service** **78=VETTCP - vettcp** **79=FINGER - Finger**	**1462=WORLD-LM - World License Manager** **1463=NUCLEUS - Nucleus** **1464=MSL_LMD - MSL License Manager** **1465=PIPES - Pipes Platform** **1466=OCEANSOFT-LM - Ocean Software License Manager** **1467=CSDMBASE - CSDMBASE** **1468=CSDM - CSDM** **1469=AAL-LM - Active Analysis Limited License Manager** **1470=UAIACT - Universal Analytics** **1471=CSDMBASE - csdmbase** **1472=CSDM - csdm** **1473=OPENMATH - OpenMath** **1474=TELEFINDER - Telefinder** **1475=TALIGENT-LM - Taligent License Manager** **1476=CLVM-CFG - clvm-cfg** **1477=MS-SNA-SERVER - ms-sna-server**

80=WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)

81=HOSTS2-NS - HOSTS2 Name Server

82=XFER - XFER Utility

83=MIT-ML-DEV - MIT ML Device

84=CTF - Common Trace Facility

85=MIT-ML-DEV - MIT ML Device

86=MFCOBOL - Micro Focus Cobol

87=LINK - Private terminal link

88=KERBEROS - Kerberos

89=SU-MIT-TG - SU/MIT Telnet Gateway

90=DNSIX - DNSIX Securit Attribute Token Map

91=MIT-DOV - MIT Dover Spooler

92=NPP - Network Printing Protocol

93=DCP - Device Control Protocol

94=OBJCALL - Tivoli Object Dispatcher

95=SUPDUP - SUPDUP

96=DIXIE - DIXIE Protocol Specifica-

1478=MS-SNA-BASE - ms-sna-base

1479=DBEREGISTER - dberegister

1480=PACERFORUM - PacerForum

1481=AIRS - AIRS

1482=MITEKSYS-LM - Miteksys License Manager

1483=AFS - AFS License Manager

1484=CONFLUENT - Confluent License Manager

1485=LANSOURCE - LANSource

1486=NMS_TOPO_SERV - nms_topo_serv

1487=LOCALINFOSRVR - LocalInfoSrvr

1488=DOCSTOR - DocStor

1489=DMDOCBROKER - dmdocbroker

1490=INSITU-CONF - insitu-conf

1491=ANYNETGATEWAY - anynetgateway

1492=STONE-DESIGN-1 - stone-design-1

tion

97=SWIFT-RVF - Swift Remote Virtural File Protocol

98=TACNEWS - TAC News

99=METAGRAM - Metagram Relay

100=NEWACCT - [unauthorized use]

101=HOSTNAMES - NIC Host Name Server

102=ISO-TSAP - ISO-TSAP Class 0

103=X400 - x400

104=X400-SND - x400-snd

105=CSNET-NS - Mailbox Name Nameserver

106=3COM-TSMUX - 3COM-TSMUX

107=RTELNET - Remote Telnet Service

108=SNAGAS - SNA Gateway Access Server

109=POP - Post Office Protocol - Version 2

110=POP3 - Post Office Protocol - Version 3

1493=NETMAP_LM - netmap_lm

1494=ICA - ica

1495=CVC - cvc

1496=LIBERTY-LM - liberty-lm

1497=RFX-LM - rfx-lm

1498=WATCOM-SQL - Watcom-SQL

1499=FHC - Federico Heinz Consultora

1500=VLSI-LM - VLSI License Manager

1501=SAISCM - Satellite-data Acquisition System 3

1502=SHIVADISCOVERY - Shiva

1503=IMTC-MCS - Databeam

1504=EVB-ELM - EVB Software Engineering License Manager

1505=FUNKPROXY - Funk Software Inc.

1506=UTCD - Universal Time daemon (utcd)

1507=SYMPLEX - symplex

1508=DIAGMOND - diagmond

111=SUNRPC - SUN Remote Procedure Call

112=MCIDAS - McIDAS Data Transmission Protocol

113=IDENT - Authentication Service

114=AUDIONEWS - Audio News Multicast

115=SFTP - Simple File Transfer Protocol

116=ANSANOTIFY - ANSA REX Notify

117=UUCP-PATH - UUCP Path Service

118=SQLSERV - SQL Services

119=NNTP - Network News Transfer Protocol

120=CFDPTKT - CFDPTKT

121=ERPC - Encore Expedited Remote Pro.Call

122=SMAKYNET - SMAKYNET

123=NTP - Network Time Protocol

124=ANSATRADER - ANSA REX

1509=ROBCAD-LM - Robcad Ltd. License Manager

1510=MVX-LM - Midland Valley Exploration Ltd. Lic. Man.

1511=3L-L1 - 3l-l1

1512=WINS - Microsoft's Windows Internet Name Service

1513=FUJITSU-DTC - Fujitsu Systems Business of America Inc

1514=FUJITSU-DTCNS - Fujitsu Systems Business of America Inc

1515=IFOR-PROTOCOL - ifor-protocol

1516=VPAD - Virtual Places Audio data

1517=VPAC - Virtual Places Audio control

1518=VPVD - Virtual Places Video data

1519=VPVC - Virtual Places Video control

1520=ATM-ZIP-OFFICE - atm zip of-

Trader **125=LOCUS-MAP - Locus PC-Interface Net Map Ser** **126=UNITARY - Unisys Unitary Login** **127=LOCUS-CON - Locus PC-Interface Conn Server** **128=GSS-XLICEN - GSS X License Verification** **129=PWDGEN - Password Generator Protocol** **130=CISCO-FNA - cisco FNATIVE** **131=CISCO-TNA - cisco TNATIVE** **132=CISCO-SYS - cisco SYSMAINT** **133=STATSRV - Statistics Service** **134=INGRES-NET - INGRES-NET Service** **135=RPC-LOCATOR - RPC (Remote Procedure Call) Location Service** **136=PROFILE - PROFILE Naming System** **137=NETBIOS-NS - NETBIOS Name Service**	**fice** **1521=NCUBE-LM - nCube License Manager** **1522=RNA-LM - Ricardo North America License Manager** **1523=CICHILD-LM - cichild** **1524=INGRESLOCK - ingres** **1525=PROSPERO-NP - Prospero Directory Service non-priv** **1526=PDAP-NP - Prospero Data Access Prot non-priv** **1527=TLISRV - oracle** **1528=MCIAUTOREG - micautoreg** **1529=COAUTHOR - oracle** **1530=RAP-SERVICE - rap-service** **1531=RAP-LISTEN - rap-listen** **1532=MIROCONNECT - miroconnect** **1533=VIRTUAL-PLACES - Virtual Places Software** **1534=MICROMUSE-LM - micromuse-lm**

138=NETBIOS-DGM - NETBIOS Datagram Service

139=NETBIOS-SSN - NETBIOS Session Service

140=EMFIS-DATA - EMFIS Data Service

141=EMFIS-CNTL - EMFIS Control Service

142=BL-IDM - Britton-Lee IDM

143=IMAP - Interim Mail Access Protocol v2

144=NEWS - NewS

145=UAAC - UAAC Protocol

146=ISO-TP0 - ISO-IP0

147=ISO-IP - ISO-IP

148=CRONUS - CRONUS-SUPPORT

149=AED-512 - AED 512 Emulation Service

150=SQL-NET - SQL-NET

151=HEMS - HEMS

152=BFTP - Background File Transfer Program

1535=AMPR-INFO - ampr-info

1536=AMPR-INTER - ampr-inter

1537=SDSC-LM - isi-lm

1538=3DS-LM - 3ds-lm

1539=INTELLISTOR-LM - Intellistor License Manager

1540=RDS - rds

1541=RDS2 - rds2

1542=GRIDGEN-ELMD - gridgen-elmd

1543=SIMBA-CS - simba-cs

1544=ASPECLMD - aspeclmd

1545=VISTIUM-SHARE - vistium-share

1546=ABBACCURAY - abbaccuray

1547=LAPLINK - laplink

1548=AXON-LM - Axon License Manager

1549=SHIVAHOSE - Shiva Hose

1550=3M-IMAGE-LM - Image Storage license manager 3M Company

1551=HECMTL-DB - HECMTL-DB

153=SGMP - SGMP

154=NETSC-PROD - NETSC

155=NETSC-DEV - NETSC

156=SQLSRV - SQL Service

157=KNET-CMP - KNET/VM Command/Message Protocol

158=PCMAIL-SRV - PCMail Server

159=NSS-ROUTING - NSS-Routing

160=SGMP-TRAPS - SGMP-TRAPS

161=SNMP - SNMP (Simple Network Management Protocol)

162=SNMPTRAP - SNMPTRAP (Simple Network Management Protocol)

163=CMIP-MAN - CMIP/TCP Manager

164=CMIP-AGENT - CMIP/TCP Agent

165=XNS-COURIER - Xerox

166=S-NET - Sirius Systems

167=NAMP - NAMP

168=RSVD - RSVD

169=SEND - SEND

1552=PCIARRAY - pciarray

1553=SNA-CS - sna-cs

1554=CACI-LM - CACI Products Company License Manager

1555=LIVELAN - livelan

1556=ASHWIN - AshWin CI Tecnologies

1557=ARBORTEXT-LM - ArborText License Manager

1558=XINGMPEG - xingmpeg

1559=WEB2HOST - web2host

1560=ASCI-VAL - asci-val

1561=FACILITYVIEW - facilityview

1562=PCONNECTMGR - pconnect-mgr

1563=CADABRA-LM - Cadabra License Manager

1564=PAY-PER-VIEW - Pay-Per-View

1565=WINDDLB - WinDD

1566=CORELVIDEO - CORELVIDEO

170=PRINT-SRV - Network PostScript

171=MULTIPLEX - Network Innovations Multiplex

172=CL/1 - Network Innovations CL/1

173=XYPLEX-MUX - Xyplex

174=MAILQ - MAILQ

175=VMNET - VMNET

176=GENRAD-MUX - GENRAD-MUX

177=XDMCP - X Display Manager Control Protocol

178=NEXTSTEP - NextStep Window Server

179=BGP - Border Gateway Protocol

180=RIS - Intergraph

181=UNIFY - Unify

182=AUDIT - Unisys Audit SITP

183=OCBINDER - OCBinder

184=OCSERVER - OCServer

185=REMOTE-KIS - Remote-KIS

186=KIS - KIS Protocol

187=ACI - Application Communica-

1567=JLICELMD - jlicelmd

1568=TSSPMAP - tsspmap

1569=ETS - ets

1570=ORBIXD - orbixd

1571=RDB-DBS-DISP - Oracle Remote Data Base

1572=CHIP-LM - Chipcom License Manager

1573=ITSCOMM-NS - itscomm-ns

1574=MVEL-LM - mvel-lm

1575=ORACLENAMES - oraclenames

1576=MOLDFLOW-LM - moldflow-lm

1577=HYPERCUBE-LM - hypercube-lm

1578=JACOBUS-LM - Jacobus License Manager

1579=IOC-SEA-LM - ioc-sea-lm

1580=TN-TL-R1 - tn-tl-r1

1581=VMF-MSG-PORT - vmf-msg-port

1582=TAMS-LM - Toshiba America

tion Interface

188=MUMPS - Plus Five's MUMPS

189=QFT - Queued File Transport

190=GACP - Gateway Access Control Protocol

191=PROSPERO - Prospero Directory Service

192=OSU-NMS - OSU Network Monitoring System

193=SRMP - Spider Remote Monitoring Protocol

194=IRC - Internet Relay Chat Protocol

195=DN6-NLM-AUD - DNSIX Network Level Module Audit

196=DN6-SMM-RED - DNSIX Session Mgt Module Audit Redir

197=DLS - Directory Location Service

198=DLS-MON - Directory Location Service Monitor

199=SMUX - SMUX

200=SRC - IBM System Resource Con-

Medical Systems

1583=SIMBAEXPRESS - simbaexpress

1584=TN-TL-FD2 - tn-tl-fd2

1585=INTV - intv

1586=IBM-ABTACT - ibm-abtact

1587=PRA_ELMD - pra_elmd

1588=TRIQUEST-LM - triquest-lm

1589=VQP - VQP

1590=GEMINI-LM - gemini-lm

1591=NCPM-PM - ncpm-pm

1592=COMMONSPACE - commonspace

1593=MAINSOFT-LM - mainsoft-lm

1594=SIXTRAK - sixtrak

1595=RADIO - radio

1596=RADIO-SM - radio-sm

1597=ORBPLUS-IIOP - orbplus-iiop

1598=PICKNFS - picknfs

1599=SIMBASERVICES - simbaservices

1600=ISSD -

troller

201=AT-RTMP - AppleTalk Routing Maintenance

202=AT-NBP - AppleTalk Name Binding

203=AT-3 - AppleTalk Unused

204=AT-ECHO - AppleTalk Echo

205=AT-5 - AppleTalk Unused

206=AT-ZIS - AppleTalk Zone Information

207=AT-7 - AppleTalk Unused

208=AT-8 - AppleTalk Unused

209=QMTP - The Quick Mail Transfer Protocol

210=Z39.50 - ANSI Z39.50

211=914C/G - Texas Instruments 914C/G Terminal

212=ANET - ATEXSSTR

213=IPX - IPX

214=VMPWSCS - VM PWSCS

215=SOFTPC - Insignia Solutions

216=CAILIC - Computer Associates

1601=AAS - aas

1602=INSPECT - inspect

1603=PICODBC - pickodbc

1604=ICABROWSER - icabrowser

1605=SLP - Salutation Manager (Salutation Protocol)

1606=SLM-API - Salutation Manager (SLM-API)

1607=STT - stt

1608=SMART-LM - Smart Corp. License Manager

1609=ISYSG-LM - isysg-lm

1610=TAURUS-WH - taurus-wh

1611=ILL - Inter Library Loan

1612=NETBILL-TRANS - NetBill Transaction Server

1613=NETBILL-KEYREP - NetBill Key Repository

1614=NETBILL-CRED - NetBill Credential Server

1615=NETBILL-AUTH - NetBill Authorization Server

Int'l License Server **217=DBASE - dBASE Unix** **218=MPP - Netix Message Posting Protocol** **219=UARPS - Unisys ARPs** **220=IMAP3 - Interactive Mail Access Protocol v3** **221=FLN-SPX - Berkeley rlogind with SPX auth** **222=RSH-SPX - Berkeley rshd with SPX auth** **223=CDC - Certificate Distribution Center** **242=DIRECT -** **243=SUR-MEAS - Survey Measurement** **244=DAYNA -** **245=LINK - LINK** **246=DSP3270 - Display Systems Protocol** **247=SUBNTBCST_TFTP -** **248=BHFHS -**	**1616=NETBILL-PROD - NetBill Product Server** **1617=NIMROD-AGENT - Nimrod Inter-Agent Communication** **1618=SKYTELNET - skytelne** **1619=XS-OPENBACKUP - xs-openbackup** **1620=FAXPORTWINPORT - fax-portwinport** **1621=SOFTDATAPHONE - softdata-phone** **1622=ONTIME - ontime** **1623=JALEOSND - jaleosnd** **1624=UDP-SR-PORT - udp-sr-port** **1625=SVS-OMAGENT - svs-omagent** **1636=CNCP - CableNet Control Protocol** **1637=CNAP - CableNet Admin Protocol** **1638=CNIP - CableNet Info Protocol** **1639=CERT-INITIATOR - cert-initiator**

256=RAP -

257=SET - Secure Electronic Transaction

258=YAK-CHAT - Yak Winsock Personal Chat

259=ESRO-GEN - Efficient Short Remote Operations

260=OPENPORT -

261=NSIIOPS - IIOP Name Service Over TLS/SSL

262=ARCISDMS -

263=HDAP -

264=BGMP -

280=HTTP-MGMT -

281=PERSONAL-LINK -

282=CABLEPORT-AX - Cable Port A/X

308=NOVASTORBAKCUP - Novastor Backup

309=ENTRUSTTIME -

310=BHMDS -

311=ASIP-WEBADMIN - Appleshare

1640=CERT-RESPONDER - cert-responder

1641=INVISION - InVision

1642=ISIS-AM - isis-am

1643=ISIS-AMBC - isis-ambc

1644=SAISEH - Satellite-data Acquisition System 4

1645=DATAMETRICS - datametrics

1646=SA-MSG-PORT - sa-msg-port

1647=RSAP - rsap

1648=CONCURRENT-LM - concurrent-lm

1649=INSPECT - inspect

1650=NKD -

1651=SHIVA_CONFSRVR - shiva_confsrvr

1652=XNMP - xnmp

1653=ALPHATECH-LM - alphatech-lm

1654=STARGATEALERTS - stargatealerts

1655=DEC-MBADMIN - dec-

IP Webadmin **312=VSLMP -** **313=MAGENTA-LOGIC -** **314=OPALIS-ROBOT -** **315=DPSI -** **316=DECAUTH -** **317=ZANNET -** **321=PIP -** **344=PDAP - Prospero Data Access Protocol** **345=PAWSERV - Perf Analysis Workbench** **346=ZSERV - Zebra server** **347=FATSERV - Fatmen Server** **348=CSI-SGWP - Cabletron Management Protocol** **349=MFTP -** **350=MATIP-TYPE-A - MATIP Type A** **351=MATIP-TYPE-B - MATIP Type B or bhoetty** **352=DTAG-STE-SB - DTAG, or**	**mbadmin** **1656=DEC-MBADMIN-H - dec-mbadmin-h 1657=FUJITSU-MMPDC - fujitsu-mmpdc** **1658=SIXNETUDR - sixnetudr** **1659=SG-LM - Silicon Grail License Manager** **1660=SKIP-MC-GIKREQ - skip-mc-gikreq** **1661=NETVIEW-AIX-1 - netview-aix-1** **1662=NETVIEW-AIX-2 - netview-aix-2** **1663=NETVIEW-AIX-3 - netview-aix-3** **1664=NETVIEW-AIX-4 - netview-aix-4** **1665=NETVIEW-AIX-5 - netview-aix-5** **1666=NETVIEW-AIX-6 - netview-aix-6** **1667=NETVIEW-AIX-7 - netview-aix-**

bhoedap4 **353=NDSAUTH -** **354=BH611 -** **355=DATEX-ASN -** **356=CLOANTO-NET-1 - Cloanto Net 1** **357=BHEVENT -** **358=SHRINKWRAP -** **359=TENEBRIS_NTS - Tenebris Network Trace Service** **360=SCOI2ODIALOG -** **361=SEMANTIX -** **362=SRSSEND - SRS Send** **363=RSVP_TUNNEL -** **364=AURORA-CMGR -** **365=DTK - Deception Tool Kit** **366=ODMR -** **367=MORTGAGEWARE -** **368=QBIKGDP -** **369=RPC2PORTMAP -** **370=CODAAUTH2 -** **371=CLEARCASE - Clearcase**	**7** **1668=NETVIEW-AIX-8 - netview-aix-8** **1669=NETVIEW-AIX-9 - netview-aix-9** **1670=NETVIEW-AIX-10 - netview-aix-10** **1671=NETVIEW-AIX-11 - netview-aix-11** **1672=NETVIEW-AIX-12 - netview-aix-12** **1673=PROSHARE-MC-1 - Intel Proshare Multicast** **1674=PROSHARE-MC-2 - Intel Proshare Multicast** **1675=PDP - Pacific Data Products** **1676=NEFCOMM1 - netcomm1** **1677=GROUPWISE - groupwise** **1723=PPTP - pptp** **1807=SpySender** **1812=RADIUS - RADIUS Authentication Protocol**

372=ULISTSERV - Unix Listserv

373=LEGENT-1 - Legent Corporation

374=LEGENT-2 - Legent Corporation

375=HASSLE - Hassle

376=NIP - Amiga Envoy Network Inquiry Proto

377=TNETOS - NEC Corporation

378=DSETOS - NEC Corporation

379=IS99C - TIA/EIA/IS-99 modem client

380=IS99S - TIA/EIA/IS-99 modem server

381=HP-COLLECTOR - HP Performance Data Collector

382=HP-MANAGED-NODE - HP Performance Data Managed Node

383=HP-ALARM-MGR - HP Performance Data Alarm Manager

384=ARNS - A Remote Network Server System

385=IBM-APP - IBM Application

386=ASA - ASA Message Router Ob-

1813=RADACCT - RADIUS Accounting Protocol

1827=PCM - PCM Agent

1981=Shockrave

1986=LICENSEDAEMON - cisco license management

1987=TR-RSRB-P1 - cisco RSRB Priority 1 port

1988=TR-RSRB-P2 - cisco RSRB Priority 2 port

1989=MSHNET - MHSnet system

1990=STUN-P1 - cisco STUN Priority 1 port

1991=STUN-P2 - cisco STUN Priority 2 port

1992=IPSENDMSG - IPsendmsg

1993=SNMP-TCP-PORT - cisco SNMP TCP port

1994=STUN-PORT - cisco serial tunnel port

1995=PERF-PORT - cisco perf port

1996=TR-RSRB-PORT - cisco Remote

ject Def. **387=AURP - Appletalk Update-Based Routing Pro.** **388=UNIDATA-LDM - Unidata LDM Version 4** **389=LDAP - Lightweight Directory Access Protocol** **390=UIS - UIS** **391=SYNOTICS-RELAY - SynOptics SNMP Relay Port** **392=SYNOTICS-BROKER - SynOptics Port Broker Port** **393=DIS - Data Interpretation System** **394=EMBL-NDT - EMBL Nucleic Data Transfer** **395=NETCP - NETscout Control Protocol** **396=NETWARE-IP - Novell Netware over IP** **397=MPTN - Multi Protocol Trans. Net.** **398=KRYPTOLAN - Kryptolan**	**SRB port** **1997=GDP-PORT - cisco Gateway Discovery Protocol** **1998=X25-SVC-PORT - cisco X.25 service (XOT)** **1999=TCP-ID-PORT - cisco identification port** **2000=CALLBOOK -** **2001=DC -** **2002=GLOBE -** **2003=CFINGER - cfinger** **2004=MAILBOX -** **2005=BERKNET -** **2006=INVOKATOR -** **2007=DECTALK -** **2008=CONF -** **2009=NEWS -** **2010=SEARCH -** **2011=RAID-CC - raid** **2012=TTYINFO -** **2013=RAID-AM -** **2014=TROFF -**

399=ISO-TSAP-C2 - ISO Transport Class 2 Non-Control over TCP

400=WORK-SOL - Workstation Solutions

401=UPS - Uninterruptible Power Supply

402=GENIE - Genie Protocol

403=DECAP - decap

404=NCED - nced

405=NCLD - ncld

406=IMSP - Interactive Mail Support Protocol

407=TIMBUKTU - Timbuktu

408=PRM-SM - Prospero Resource Manager Sys. Man.

409=PRM-NM - Prospero Resource Manager Node Man.

410=DECLADEBUG - DECLadebug Remote Debug Protocol

411=RMT - Remote MT Protocol

412=SYNOPTICS-TRAP - Trap Convention Port

2015=CYPRESS -

2016=BOOTSERVER -

2017=CYPRESS-STAT -

2018=TERMINALDB -

2019=WHOSOCKAMI -

2020=XINUPAGESERVER -

2021=SERVEXEC -

2022=DOWN -

2023=XINUEXPANSION3 -

2024=XINUEXPANSION4 -

2025=ELLPACK -

2026=SCRABBLE -

2027=SHADOWSERVER -

2028=SUBMITSERVER -

2030=DEVICE2 -

2032=BLACKBOARD -

2033=GLOGGER -

2034=SCOREMGR -

2035=IMSLDOC -

2038=OBJECTMANAGER -

2040=LAM -

2041=INTERBASE -

413=SMSP - SMSP

414=INFOSEEK - InfoSeek

415=BNET - BNet

416=SILVERPLATTER - Silverplatter

417=ONMUX - Onmux

418=HYPER-G - Hyper-G

419=ARIEL1 - Ariel

420=SMPTE - SMPTE

421=ARIEL2 - Ariel

422=ARIEL3 - Ariel

423=OPC-JOB-START - IBM Operations Planning and Control Start

424=OPC-JOB-TRACK - IBM Operations Planning and Control Track

425=ICAD-EL - ICAD

426=SMARTSDP - smartsdp

427=SVRLOC - Server Location

428=OCS_CMU - OCS_CMU

429=OCS_AMU - OCS_AMU

430=UTMPSD - UTMPSD

431=UTMPCD - UTMPCD

2042=ISIS - isis

2043=ISIS-BCAST - isis-bcast

2044=RIMSL -

2045=CDFUNC -

2046=SDFUNC -

2047=DLS -

2048=DLS-MONITOR - dls-monitor

2064=DISTRIB-NETASSHOLES - A group of lamers working on a closed-source client for solving the RSA cryptographic challenge

2065=DLSRPN - Data Link Switch Read Port Number

2067=DLSWPN - Data Link Switch Write Port Number

2080=Wingate Winsock Redirector Service

2103=ZEPHYR-CLT - Zephyr Serv-HM Conncetion

2104=Zephyr Host Manager

2105=EKLOGIN - Kerberos (v4) En-

432=IASD - IASD

433=NNSP - NNSP

434=MOBILEIP-AGENT - MobileIP-Agent

435=MOBILIP-MN - MobilIP-MN

436=DNA-CML - DNA-CML

437=COMSCM - comscm

438=DSFGW - dsfgw

439=DASP - dasp

440=SGCP - sgcp

441=DECVMS-SYSMGT - decvms-sysmgt

442=CVC_HOSTD - cvc_hostd

443=HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)

444=SNPP - Simple Network Paging Protocol

445=MICROSOFT-DS - Microsoft-DS

446=DDM-RDB - DDM-RDB

447=DDM-DFM - DDM-RFM

crypted RLogin

2106=EKSHELL - Kerberos (v4) Encrypted RShell

2108=RKINIT - Kerberos (v4) Remote Initialization

2111=KX - X Over Kerberos

2112=KIP - IP Over Kerberos

2115=Bugs

2120=KAUTH - Remote kauth

2140=Deep Throat, The Invasor

2155=Illusion Mailer

2201=ATS - Advanced Training System Program

2221=UNREG-AB1 - Allen-Bradley unregistered port

2222=UNREG-AB2 - Allen-Bradley unregistered port

2223=INREG-AB3 - Allen-Bradley unregistered port

2232=IVS-VIDEO - IVS Video default

2241=IVSD - IVS Daemon

2283=HVL Rat5

448=DDM-BYTE - DDM-BYTE

449=AS-SERVERMAP - AS Server Mapper

450=TSERVER - TServer

451=SFS-SMP-NET - Cray Network Semaphore server

452=SFS-CONFIG - Cray SFS config server

453=CREATIVESERVER - Crea-tiveServer

454=CONTENTSERVER - Content-Server

455=CREATIVEPARTNR - Creative-Partnr

456=MACON-TCP - macon-tcp

457=SCOHELP - scohelp

458=APPLEQTC - Apple Quick Time

459=AMPR-RCMD - ampr-rcmd

460=SKRONK - skronk

461=DATASURFSRV - DataRampSrv

462=DATASURFSRVSEC - Data-RampSrvSec

2301=CIM - Compaq Insight Manager

2307=PEHELP - pehelp

2401=CVSPSERVER - CVS Network Server

2430=VENUS -

2431=VENUS-SE -

2432=CODASRV -

2433=CODASRV-SE -

2500=RTSSERV - Resource Tracking system server

2501=RTSCLIENT - Resource Track-ing system client

2564=HP-3000-TELNET - HP 3000 NS/VT block mode telnet

2565=Striker

2583=WinCrash

2592=NETREK[GAME] - netrek[game]

2600=Digital Rootbeer

2601=ZEBRA - Zebra VTY

2602=RIPD - RIPd VTY

2603=RIPNGD - RIPngd VTY

463=ALPES - alpes

464=KPASSWD - kpasswd

465=SSMTP - ssmtp

466=DIGITAL-VRC - digital-vrc

467=MYLEX-MAPD - mylex-mapd

468=PHOTURIS - proturis

469=RCP - Radio Control Protocol

470=SCX-PROXY - scx-proxy

471=MONDEX - Mondex

472=LJK-LOGIN - ljk-login

473=HYBRID-POP - hybrid-pop

474=TN-TL-W1 - tn-tl-w1

475=TCPNETHASPSRV - tcpnethaspsrv

476=TN-TL-FD1 - tn-tl-fd1

477=SS7NS - ss7ns

478=SPSC - spsc

479=IAFSERVER - iafserver

480=IAFDBASE - iafdbase

481=PH - Ph service

482=BGS-NSI - bgs-nsi

483=ULPNET - ulpnet

2604=OSPFD - OSPFd VTY

2605=BGPD - BGPd VTY

2627=WEBSTER -

2638=Sybase Database

2700=TQDATA - tqdata

2766=LISTEN - System V Listener Port

2784=WWW-DEV - world wide web - development

2800=Phineas Phucker

2989=(UDP) - RAT

3000=UNKNOWN - Unknown Service

3001=NESSUSD - Nessus Security Scanner

3005=DESLOGIN - Encrypted Sym-metric Telnet

3006=DESLOGIND -

3024=WinCrash

3049=NSWS -

3064=DISTRIB-NET-PROXY - Stupid closed source distrib.net proxy

3086=SJ3 - SJ3 (Kanji Input)

484=INTEGRA-SME - Integra Software Management Environment

485=POWERBURST - Air Soft Power Burst

486=AVIAN - avian

487=SAFT - saft

488=GSS-HTTP - gss-http

489=NEST-PROTOCOL - nest-protocol

490=MICOM-PFS - micom-pfs

491=GO-LOGIN - go-login

492=TICF-1 - Transport Independent Convergence for FNA

493=TICF-2 - Transport Independent Convergence for FNA

494=POV-RAY - POV-Ray

495=INTECOURIER -

496=PIM-RP-DISC -

497=DANTZ -

498=SIAM -

499=ISO-ILL - ISO ILL Protocol

500=ISAKMP -

3128=RingZero -

3129=Masters Paradise -

3130=SQUID-IPC -

3141=VMODEM - VMODEM

3150=Deep Throat, The Invasor

3155=HTTP Proxy

3264=CCMAIL - cc:mail/lotus

3295=PORT

3306=MYSQL

3333=DEC-NOTES - DEC Notes

3421=BMAP - Bull Apprise portmapper

3454=MIRA - Apple Remote Access Protocol

3455=PRSVP - RSVP Port

3456=VAT - VAT default data

3457=VAT-CONTROL - VAT default control

3459=Eclipse 2000

3700=Portal of Doom

3791=Eclypse

3801=(UDP) - Eclypse

501=STMF -

502=ASA-APPL-PROTO -

503=INTRINSA -

504=CITADEL -

505=MAILBOX-LM -

506=OHIMSRV -

507=CRS -

508=XVTTP -

509=SNARE -

510=FCP - FirstClass Protocol

511=PASSGO -

512=EXEC - Remote Process Execution

513=LOGIN - Remote Login via Telnet;

514=SHELL - Automatic Remote Process Execution

515=PRINTER - Printer Spooler

516=VIDEOTEX -

517=TALK -

518=NTALK -

519=UTIME - Unix Time

3871=PORT

3900=UDT_OS - Unidata UDT OS

3905=PORT

3908=PORT

3920=PORT

3921=PORT

3922=PORT

3923=PORT

3925=PORT

3975=PORT

3984=MAPPER-NODEMGR - MAPPER network node manager

3985=MAPPER-MAPETHD - MAPPER TCP/IP server

3986=MAPPER-WS_ETHD - MAPPER workstation server

3996=PORT

4000=UNKNOWN - Unknown Service

4001=PORT

4008=NETCHEQUE - NetCheque accounting

4045=LOCKD - NFS Lock Daemon

520=EFS - Extended File Server

521=RIPNG -

522=ULP -

523=IBM-DB2 -

524=NCP -

525=TIMED - Time Server

526=TEMPO - newdate

527=STX - Stock IXChange

528=CUSTIX - Customer IXChange

529=IRC-SERV -

530=COURIER - rpc

531=CONFERENCE - chat

532=NETNEWS - readnews

533=NETWALL - Emergency Broadcasts

534=MM-ADMIN - MegaMedia Admin

535=IIOP -

536=OPALIS-RDV -

537=NMSP - Networked Media Streaming Protocol

538=GDOMAP -

4092=WinCrash

4132=NUTS_DEM - NUTS Daemon

4133=NUTS_BOOTP - NUTS Bootp Server

4321=RWHOIS - Remote Who Is

4333=MSQL - Mini SQL Server

4343=UNICALL - UNICALL

4444=NV-VIDEO - NV Video default

4500=SAE-URN - sae-urn

4501=URN-X-CDCHOICE - urn-x-cdchoice

4557=FAX - fax

4559=HYLAFAX - HylaFAX cli-svr Protocol

4567=File Nail

4590=ICQTrojan

4672=RFA - remote file access server

4899=RAdmin - Remote Administrator

5000=UNKNOWN - Unknown Service

5001=COMMPLEX-LINK -

5002=RFE - radio free ethernet

5003=CLARIS-FMPRO - Claris Fi-

539=APERTUS-LDP - Apertus Technologies Load Determination

540=UUCP - UUCPD (Unix to Unix Copy)

541=UUCP-RLOGIN - uucp (Unix to Unix Copy) - rlogin (Remote Login)

542=COMMERCE -

543=KLOGIN -

544=KSHELL - krcmd

545=APPLEQTCSRVR - Apple qtcsrvr

546=DHCP-CLIENT - DHCP (Dynamic Host Configuration Protocol) Client

547=DHCP-SERVER - DHCP (Dynamic Host Configuration Protocol) Server

548=AFPOVERTCP - AFP over TCP

549=IDFP -

550=NEW-RWHO - new-who

551=CYBERCASH - CyberCash

552=DEVICESHARE - deviceshare

553=PIRP - pirp

leMaker Pro

5004=AVT-PROFILE-1 - avt-profile-1

5005=AVT-PROFILE-2 - avt-profile-2

5010=TELELPATHSTART - TelepathStart

5011=TELELPATHATTACK - TelepathAttack

5031=NetMetro

5050=MMCC - multimedia conference control tool

5075=IISADMIN = IIS Administration Web Site

5145=RMONITOR_SECURE -

5190=AOL - America-Online

5191=AOL-1 - AmericaOnline1

5192=AOL-2 - AmericaOnline2

5193=AOL-3 - AmericaOnline3

5232=SGI-DGL - SGI Distributed Graphics

5236=PADL2SIM

5300=HACL-HB - HA Cluster Heartbeat

554=RTSP - Real Time Stream Control Protocol

555=DSF -

556=REMOTEFS - rfs (Remote File System) server

557=OPENVMS-SYSIPC - openvms-sysipc

558=SDNSKMP - SDNSKMP

559=TEEDTAP - TEEDTAP

560=RMONITOR - rmonitord

561=MONITOR -

562=CHSHELL - chcmd

563=SNEWS - snews

564=9PFS - plan 9 file service

565=WHOAMI - whoami

566=STREETTALK - streettalk

567=BANYAN-RPC - banyan-rpc

568=MS-SHUTTLE - Microsoft Shuttle

569=MS-ROME - Microsoft Rome

570=METER - demon

571=METER - udemon

5301=HACL-GS - HA Cluster General Services

5302=HACL-CFG - HA Cluster Configuration

5303=HACL-PROBE - HA Cluster Probing

5304=HACL-LOCAL

5305=HACL-TEST

5308=CFENGINE -

5321=Firehotcker

5376=MS FTP

5400=Blade Runner, Back Construction

5401=Blade Runner, Back Construction

5402=Blade Runner, Back Construction

5432=POSTGRES - Postgres Database Server

5500=Hotline Server

5510=SECUREIDPROP - ACE/Server Services

572=SONAR - sonar

573=BANYAN-VIP - banyan-vip

574=FTP-AGENT - FTP Software Agent System

575=VEMMI - VEMMI

576=IPCD -

577=VNAS -

578=IPDD -

579=DECBSRV -

580=SNTP-HEARTBEAT -

581=BDP - Bundle Discovery Protocol

582=SCC-SECURITY -

583=PHILIPS-VC - PHilips Video-Conferencing

584=KEYSERVER -

585=IMAP4-SSL - IMAP4+SSL

586=PASSWORD-CHG -

587=SUBMISSION -

588=CAL -

589=EYELINK -

590=TNS-CML -

591=HTTP-ALT - FileMaker, Inc. -

5512=Illusion Maker

5520=SDLOG - ACE/Server Services

5530=SDSERV - ACE/Server Services

5540=SDXAUTHD - ACE/Server Services

5550=Xtcp

5555=ServeMe

5556=Bo

5557=Bo

5569=Robo-Hack

5631=PCANYWHEREDATA -

5632=PCANYWHERESTAT -

5650=MS FTP PORT

5680=CANNA - Canna (Jap Input)

5713=PROSHAREAUDIO - proshare conf audio

5714=PROSHAREVIDEO - proshare conf video

5715=PROSHAREDATA - proshare conf data

5716=PROSHAREREQUEST - proshare conf request

HTTP Alternate

592=EUDORA-SET -

593=HTTP-RPC-EPMAP - HTTP RPC Ep Map

594=TPIP -

595=CAB-PROTOCOL -

596=SMSD -

597=PTCNAMESERVICE - PTC Name Service

598=SCO-WEBSRVRMG3 - SCO Web Server Manager 3

599=ACP - Aeolon Core Protocol

600=IPCSERVER - Sun IPC server

606=URM - Cray Unified Resource Manager

607=NQS - nqs

608=SIFT-UFT - Sender-Initiated/Unsolicited File Transfer

609=NPMP-TRAP - npmp-trap

610=NPMP-LOCAL - npmp-local

611=NPMP-GUI - npmp-gui

628=QMQP - Qmail Quick Mail

5717=PROSHARENOTIFY - proshare conf notify

5742=WinCrash

5800=VNC - Virtual Network Computing

5801=VNC - Virtual Network Computing

5858=NETREK[GAME] - netrek[game]

5900=VNC - Virtual Network Computing

5901=VNC-1 - Virtual Network Computing Display

5902=VNC-2 - Virtual Network Computing Display

5977=NCD-PREF-TCP - NCD Preferences

5978=NCD-DIAG-TCP - NCD Diagnostics

5979=NCD-CONF-TCP - NCD Configuration

5997=NCD-PREF - NCD Preferences

Queueing **633=SERVSTAT - Service Status update (Sterling Software)** **634=GINAD - ginad** **635=MOUNT - NFS Mount Service** **636=LDAPSSL - LDAP Over SSL** **640=PCNFS - PC-NFS DOS Authentication** **650=BWNFS - BW-NFS DOS Authentication** **666=DOOM - doom Id Software** **674=PORT** **704=ELCSD - errlog copy/server daemon** **709=ENTRUSTMANAGER - EntrustManager** **729=NETVIEWDM1 - IBM NetView DM/6000 Server/Client** **730=NETVIEWDM2 - IBM NetView DM/6000 send/tcp** **731=NETVIEWDM3 - IBM NetView DM/6000 receive/tcp**	**Telnet** **5998=NCD-DIAG - NCD Diagnostics Telnet** **5999=NCD-CONF - NCD Configuration Telnet** **6000=X11 - X Window System** **6001=X11:1 - X Window Server** **6002=X11:2 - X Window Server** **6003=X11:3 - X Window Server** **6004=X11:4 - X Window Server** **6005=X11:5 - X Window Server** **6006=X11:6 - X Window Server** **6007=X11:7 - X Window Server** **6008=X11:8 - X Window Server** **6009=X11:9 - X Window Server** **6110=SOFTCM - HP SoftBench CM** **6111=SPC - HP SoftBench Sub-Process Control** **6112=DTSPCD - dtspcd** **6141=META-CORP - Meta Corporation License Manager** **6142=ASPENTEC-LM - Aspen Tech-**

737=SOMETIMES-RPC2 - Rusersd on my OpenBSD Box

740=NETCP - NETscout Control Protocol

741=NETGW - netGW

742=NETRCS - Network based Rev. Cont. Sys.

744=FLEXLM - Flexible License Manager

747=FUJITSU-DEV - Fujitsu Device Control

748=RIS-CM - Russell Info Sci Calendar Manager

749=KERBEROS-ADM - kerberos administration

750=KERBEROS-SEC -

751=KERBEROS_MASTER -

752=QRH -

753=RRH -

754=KBR5_PROP -

758=NLOGIN -

759=CON -

nology License Manager

6143=WATERSHED-LM - Watershed License Manager

6144=STATSCI1-LM - StatSci License Manager - 1

6145=STATSCI2-LM - StatSci License Manager - 2

6146=LONEWOLF-LM - Lone Wolf Systems License Manager

6147=MONTAGE-LM - Montage License Manager

6148=RICARDO-LM - Ricardo North America License Manager

6149=TAL-POD - tal-pod

6400=The Thing

6455=SKIP-CERT-RECV - SKIP Certificate Receive

6456=SKIP-CERT-SEND - SKIP Certificate Send

6558=XDSXDM -

6660=IRC-SERV - irc-serv

6661=IRC-SERV - irc-serv

760=NS -

761=RXE -

762=QUOTAD -

763=CYCLESERV -

764=OMSERV -

765=WEBSTER -

767=PHONEBOOK - phone

769=VID -

770=CADLOCK -

771=RTIP -

772=CYCLESERV2 -

773=SUBMIT -

774=RPASSWD -

775=ENTOMB -

776=WPAGES -

780=WPGS -

781=HP-COLLECTOR - HP Performance Data Collector

782=HP-MANAGED-NODE - HP Performance Data Managed Node

783=HP-ALARM-MGR - HP Performance Data Alarm Manager

6662=IRC-SERV - irc-serv

6663=IRC-SERV - irc-serv

6664=IRC-SERV - irc-serv

6665=IRC-SERV - irc-serv

6666=IRC-SERV - irc-serv

6667=IRC - irc

6668=IRC - irc

6669=Vampyre

6670=DeepThroat

6671=IRC-SERV - irc-serv

6771=DeepThroat

6776=BackDoor-G, SubSeven

6912=Shit Heep

6939=Indoctrination

6969=ACMSODA - acmsoda

6970=GateCrasher, Priority, IRC 3

7000=AFSSERV - file server itself

7001=UNKNOWN - Unknown Service

7002=UNKNOWN - Unknown Service

7003=AFS3-VLSERVER - volume location database

7004=AFS3-KASERVER -

786=CONCERT - Concert

799=CONTROLIT -

800=MDBS_DAEMON -

801=DEVICE -

808=PORT

871=SUPFILESRV = SUP Server

888=CDDATABASE - CDDataBase

901=PORT

911=Dark Shadow

989=FTPS-DATA - FTP Over TLS/SSL

990=FTP Control TLS/SSL

992=TELNETS - telnet protocol over TLS/SSL

993=IMAPS - Imap4 protocol over TLS/SSL

995=POP3S - Pop3 (Post Office Protocol) over TLS/SSL

996=VSINET - vsinet

997=MAITRD -

998=BUSBOY -

999=PUPROUTER -

AFS/Kerberos authentication service

7005=AFS3-VOLSER - volume managment server

7006=AFS3-ERRORS - error interpretation service

7007=AFS3-BOS - basic overseer process

7008=AFS3-UPDATE - server-to-server updater

7009=AFS3-RMTSYS - remote cache manager service

7010=UPS-ONLINET - onlinet uninterruptable power supplies

7100=FONT-SERVICE - X Font Service

7120=IISADMIN = IIS Administration Web Site

7121=VIRPROT-LM - Virtual Prototypes License Manager

7200=FODMS - FODMS FLIP

7201=DLIP - DLIP

7300=NetMonitor

1000=CADLOCK -

1001=Silence

1008=UFSD - UFSD

1010=Doly-Trojan

1011=Doly-Trojan

1012=Doly-Trojan

1015=Doly-Trojan

1023=RESERVED - Reserved

1024=OLD_FINGER - old_finger

1025=LISTEN - listen

1026=NTERM - nterm

1027=NT

1028=NT

1029=NT

1030=IAD1 - BBN IAD

1031=IAD2 - BBN IAD

1032=IAD3 - BBN IAD

1033=NT

1034=NT

1035=NT

1036=NT

1037=NT

7301=NetMonitor

7306=NetMonitor

7307=NetMonitor

7308=NetMonitor

7309=NetMonitor

7326=ICB - Internet Citizen's Band

7648=CUCME-1 - CucMe live vid-eo/Audio Server

7649=CUCME-2 - CucMe live vid-eo/Audio Server

7650=CUCME-3 - CucMe live vid-eo/Audio Server

7651=CUCME-4 - CucMe live vid-eo/Audio Server

7770=IRC

7777=CBT - cbt

7789=Back Door Setup, ICKiller

8000=Generic - Shared service port

8001=Generic - Shared service port

8002=Generic - Shared service port

8003=Generic - Shared service port

8004=Generic - Shared service port

1038=NT

1039=NT

1040=NT

1041=NT

1042=Bla

1043=NT

1044=NT

1045=Rasmin

1046=NT

1047=NT

1048=NT

1049=NT

1058=NIM - nim

1059=NIMREG - nimreg

1067=INSTL_BOOTS - Installation Bootstrap Proto. Serv.

1068=INSTL_BOOTC - Installation Bootstrap Proto. Cli.

1080=SOCKS - Socks

1083=ANSOFT-LM-1 - Anasoft License Manager

1084=ANSOFT-LM-2 - Anasoft Li-

8005=Generic - Shared service port

8006=Generic - Shared service port

8007=Generic - Shared service port

8008=Generic - Shared service port

8009=Generic - Shared service port

8010=Generic - Shared service port

8080=Generic - Shared service port

8081=Generic - Shared service port

8082=Generic - Shared service port

8083=Generic - Shared service port

8084=Generic - Shared service port

8085=Generic - Shared service port

8086=Generic - Shared service port

8087=Generic - Shared service port

8088=Generic - Shared service port

8100=Generic - Shared service port

8101=Generic - Shared service port

8102=Generic - Shared service port

8103=Generic - Shared service port

8104=Generic - Shared service port

8105=Generic - Shared service port

8106=Generic - Shared service port

cense Manager

1090=Xtreme

1103=XAUDIO - Xaserver

1109=KPOP - kpop

1110=NFSD-STATUS - Cluster Status Info

1112=MSQL - Mini-SQL Server

1127=SUPFILEDBG - SUP Debugging

1155=NFA - Network File Access

1167=PHONE - Conference Calling

1170=Psyber Stream Server, Streaming Audio trojan, Voice

1178=SKKSERV - SKK (Kanji Input)

1212=LUPA - lupa

1222=NERV - SNI R&D network

1234=Ultors Trojan

1241=MSG - Remote Message Server

1243=BackDoor-G, SubSeven, SubSeven Apocalypse

1245=Voodoo Doll

1248=HERMES - Multi Media Conferencing

8107=Generic - Shared service port

8108=Generic - Shared service port

8109=Generic - Shared service port

8110=Generic - Shared service port

8181=Generic - Shared service port

8383=Generic - Shared service port

8450=NPMP - npmp

8765=Ultraseek

8807=DEMOS NNTP

8888=SiteScope - SiteScope Remote Server Monitoring

8892=SEOSLOAD - eTrust ACX

9000=UNKNOWN - Unknown Service

9001=UNKNOWN

9010=SERVICE

9090=ZEUS-ADMIN - Zeus Admin Server

9095=SERVICE

9100=JETDIRECT - HP JetDirect Card

9200=WAP - Wireless Application Protocol

1269=Mavericks Matrix

1330=PORT

1346=ALTA-ANA-LM - Alta Analytics License Manager

1347=BBN-MMC - Multi Media Conferencing

1348=BBN-MMX - Multi Media Conferencing

1349=SBOOK - Registration Network Protocol

1350=EDITBENCH - Registration Network Protocol

1351=EQUATIONBUILDER - Digital Tool Works (MIT)

1352=LOTUSNOTE - Lotus Note

1353=RELIEF - Relief Consulting

1354=RIGHTBRAIN - RightBrain Software

1355=INTUITIVE EDGE - Intuitive Edge

1356=CUILLAMARTIN - CuillaMartin Company

9201=WAP - Wireless Application Protocol

9202=WAP - Wireless Application Protocol

9203=WAP - Wireless Application Protocol

9400=InCommand

9535=MAN -

9872=Portal of Doom

9873=Portal of Doom

9874=Portal of Doom

9875=Portal of Doom

9876=SD - Session Director

9989=iNi-Killer

9998=DEMOS SMTP

9999=DISTINCT - distinct

10005=STEL - Secure Telnet

10067=(UDP) - Portal of Doom

10080=AMANDA - Amanda Backup Util

10082=AMANDA-IDX - Amanda Indexing

1357=PEGBOARD - Electronic Peg-Board

1358=CONNLCLI - CONNLCLI

1359=FTSRV - FTSRV

1360=MIMER - MIMER

1361=LINX - LinX

1362=TIMEFLIES - TimeFlies

1363=NDM-REQUESTER - Network DataMover Requester

1364=NDM-SERVER - Network DataMover Server

1365=ADAPT-SNA - Network Software Associates

1366=NETWARE-CSP - Novell NetWare Comm Service Platform

1367=DCS - DCS

1368=SCREENCAST - ScreenCast

1369=GV-US - GlobalView to Unix Shell

1370=US-GV - Unix Shell to GlobalView

1371=FC-CLI - Fujitsu Config Proto-

10083=AMIDXTAPE - Amanda Tape Indexing

10101=BrainSpy

10167=(UDP) - Portal of Doom

10520=Acid Shivers

10607=Coma

11000=Senna Spy

11223=Progenic trojan

11371=PKSD - PGP Pub. Key Server

12067=Gjamer

12223=Hackr99 KeyLogger

12345=NB - NetBus

12346=GabanBus, NetBus, X-bill

12361=Whack-a-mole

12362=Whack-a-mole

12631=Whackjob

13000=Senna Spy

13326=CROSSFIRE[GAME] - cross-fire[game]

16660=Stacheldraht Master Serverd

16969=Priority

17007=ISODE-DUA -

col

1372=FC-SER - Fujitsu Config Protocol

1373=CHROMAGRAFX - Chromagrafx

1374=MOLLY - EPI Software Systems

1375=BYTEX - Bytex

1376=IBM-PPS - IBM Person to Person Software

1377=CICHLID - Cichlid License Manager

1378=ELAN - Elan License Manager

1379=DBREPORTER - Integrity Solutions

1380=TELESIS-LICMAN - Telesis Network License Manager

1381=APPLE-LICMAN - Apple Network License Manager

1382=UDT_OS -

1383=GWHA - GW Hannaway Network License Manager

1384=OS-LICMAN - Objective Solu-

17300=Kuang2 The Virus

18000=BIIMENU - Beckman Instruments Inc.

20000=Millennium

20001=Millennium backdoor

20005=BTX - Xcept4

20034=Netbus 2 Pro

20203=Logged

21544=Girlfriend

21845=WEBPHONE - webphoned

21846=INFO SERVER - info server

21847=CONNECT SERVER - connect server

22222=Prosiak

22273=WNN6 - Wnn6 (Jap. Input)

22289=WNN6_CN - Wnn6 (Chi. Input)

22305=WNN6_KR - Wnn6 (Kor. Input)

22321=WNN6_TW - Wnn6 (Tai. Input)

23456=Evil FTP, Ugly FTP , Whack Job

tions License Manager

1385=ATEX_ELMD - Atex Publishing License Manager

1386=CHECKSUM - CheckSum License Manager

1387=CADSI-LM - Computer Aided Design Software Inc LM

1388=OBJECTIVE-DBC - Objective Solutions DataBase Cache

1389=ICLPV-DM - Document Manager

1390=ICLPV-SC - Storage Controller

1391=ICLPV-SAS - Storage Access Server

1392=ICLPV-PM - Print Manager

1393=ICLPV-NLS - Network Log Server

1394=ICLPV-NLC - Network Log Client

1395=ICLPV-WSM - PC Workstation Manager software

1396=DVL-ACTIVEMAIL - DVL Ac-

23476=Donald Dick

23477=Donald Dick

24326=Netscape Server

25000=ICL-TWOBASE1 - icl-twobase1

25001=ICL-TWOBASE2 - icl-twobase2

25002=ICL-TWOBASE3 - icl-twobase3

25003=ICL-TWOBASE4 - icl-twobase4

25004=ICL-TWOBASE5 - icl-twobase5

25005=ICL-TWOBASE6 - icl-twobase6

25006=ICL-TWOBASE7 - icl-twobase7

25007=ICL-TWOBASE8 - icl-twobase8

25008=ICL-TWOBASE9 - icl-twobase9

25009=ICL-TWOBASE10 - icl-

tive Mail

1397=AUDIO-ACTIVMAIL - Audio Active Mail

1398=VIDEO-ACTIVMAIL - Video Active Mail

1399=CADKEY-LICMAN - Cadkey License Manager

1400=CADKEY-TABLET - Cadkey Tablet Daemon

1401=GOLDLEAF-LICMAN - Goldleaf License Manager

1402=PRM-SM-NP - Prospero Resource Manager

1403=PRM-NM-NP - Prospero Resource Manager

1404=IGI-LM - Infinite Graphics License Manager

1405=IBM-RES - IBM Remote Execution Starter

1406=NETLABS-LM - NetLabs License Manager

twobase10

26000=QUAKEXX

26001=QUAKEXX

26002=QUAKEXX

26208=WNN6_DS - Wnn6 (Dserver)

26274=(UDP) - Delta Source

27119=QUAKEXX

27444=TRINOO_BCAST - Trinoo Attack Tool

27500=QUAKEXX

27501=QUAKEXX

27502=QUAKEXX

27665=TRINOO_MASTER - Trinoo Attack Tool

27910=QUAKEXX

27911=QUAKEXX

27912=QUAKEXX

27913=QUAKEXX

27920=QUAKEXX

27960=QUAKE3SERVER - Quake 3 Arena Server

29891=(UDP) - The Unexplained

1407=DBSA-LM - DBSA License Manager

1408=SOPHIA-LM - Sophia License Manager

1409=HERE-LM - Here License Manager

1410=HIQ - HiQ License Manager

1411=AF - AudioFile

1412=INNOSYS - InnoSys

1413=INNOSYS-ACL - Innosys-ACL

1414=IBM-MQSERIES - IBM MQSeries

1415=DBSTAR - DBStar

1416=NOVELL-LU6.2 - Novell LU6.2

1417=TIMBUKTU-SRV1 - Timbuktu Service 1 Port

1418=TIMBUKTU-SRV2 - Timbuktu Service 2 Port

1419=TIMBUKTU-SRV3 - Timbuktu Service 3 Port

1420=TIMBUKTU-SRV4 - Timbuktu Service 4 Port

29970=PORT

30029=AOL Trojan

30100=NetSphere

30101=Netsphere

30102=NetSphere

30303=Sockets de Troie

30999=Kuang2

31335=TRINOO_REGISTER - Trinoo Attack Tool

31336=Whack

31337=BO - BackOrifice

31338=NetSpy DK

31457=TETRINET (Tetris GAME)

31666=BO Whack

31785=HackrarTack

31787=HackrarTack

31788=HackrarTack

31789=HackrarTack (udp)

31791=HackrarTack (udp)

31792=HackrarTack

32000=Generic - Shared service port

33333=Prosiak

1421=GANDALF-LM - Gandalf License Manager

1422=AUTODESK-LM - Autodesk License Manager

1423=ESSBASE - Essbase Arbor Software

1424=HYBRID - Hybrid Encryption Protocol

1425=ZION-LM - Zion Software License Manager

33911=Spirit 2001a

34324=BigGluck, TN

40193=NetWare

40412=The Spy

40421=Agent 40421, Masters Paradise

40422=Masters Paradise

40423=Masters Paradise

40426=Masters Paradise

43188=REACHOUT -

44333=WinRoute

47262=(UDP) - Delta Source

47557=DBBROWSE - Databeam Corporation

50505=Sockets de Troie

50766=Fore , Schwindler

53001=Remote Window Shutdown

54320=BO 2K

54321=SchoolBus

60000=Deep Throat

61466=TeleCommando

65000=Devil

65301=PCANYWHERE

ДОДАТОК 4

Список міжнародних стандартів з області захисту інформаційних технологій:

- ISO/IEC 09594-8-88 - "Взаємозв'язок відкритих систем. Довідник. Частина 8. Основи аутентифікації";
- ISO/IEC 10116-91- "Банківська справа. Режими роботи n-біт блокового алгоритму шифрування";
- ISO/IEC 10118-1,2-88 - "Інформаційні технології. Шифрування даних. Хэш-функция для цифрового підпису";
- ISO/IEC 10126-2-91 - "Банківська справа. Процедури шифрування повідомлення. Частина 2. Алгоритм DEA";
- ISO/IEC 10164-7-92. "Інформаційних технологій. Взаємозв'язок відкритих систем. Адміністративне управління системи. Частина 7. Функції повідомлення про порушення інформаційної безпеки".
- ISO/IEC 11166-94 - "Банківська справа. Управління ключами за допомогою асиметричного алгоритму".
- ISO/IEC 11568-94 - "Банківська справа. Управління ключами".

- ISO/IEC 11577-94 - "Інформаційні технології. Передача даних і обмін інформацією між системами. Взаємозв'язок відкритих систем. Протокол захисту інформації на мережевому рівні";
- ISO/IEC 7498-2-89 - "Інформаційні технології. Взаємозв'язок відкритих системи. Базова еталонна модель. Частина 2. Архітектура інформаційної безпеки";
- ISO/IEC 8732-87 - "Інформаційні технології. Захист інформації. Режими використання 64-бітового блокового алгоритму";
- ISO/IEC 8732-88 - "Банківська справа. Управління ключами";
- ISO/IEC 9796-91 - "Інформаційні технології. Схема електронного підпису, при якому проводиться відновлення повідомлення";
- ISO/IEC 9798-91 - "Інформаційні технології. Захист інформації. Аутентифікація об'єкту".
- ISO/IEC CD 10118-3,4 - "Інформаційні технології. Захист інформації. Функції хешування";
- ISO/IEC CD 11770 - "Інформаційні технології. Захист інформації. Управління ключами".
- ISO/IEC CD 13888 - "Механізми запобігання запереченню".
- ISO/IEC CD 14888 - "Інформаційні технології. Захист інформації. Цифровий підпис з додаванням".
- ISO/IEC DIS 13492 - "Банківська справа. Управління ключами, що відносяться до елементів даних";
- ISO/IEC DTR 10181- "Інформаційні технології. Взаємозв'язок відкритих систем. Основи захисту інформації для відкритих систем".
- ISO/IEC DTR 10181-1 - "Інформаційні технології. Взаємозв'язок відкритих систем. Основи захисту інформації для відкритих систем. Частина 1. Загальний опис основ захисту інформації";
- ISO/IEC DTR 10736 - "Інформаційні технології. Передача даних і обмін інформацією між системами. Протокол захисту інформації на транспортному рівні";

- ISO/IEC DTR 10745 - "Інформаційні технології. Взаємозв'язок відкритих систем. Модель захисту інформації верхніх рівнів";
- ISO/IEC DTR 11586. "Інформаційних технологій. Взаємозв'язок відкритих систем. Загальні функції захисту верхніх рівнів".
- ISO/IEC DTR 11586-1 - "Інформаційні технології. Взаємозв'язок відкритих систем. Загальні функції захисту верхніх рівнів. Частина 1. Загальний опис, моделі і нотація";
- ISO/IEC DTR 13335-1 - "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 1. Концепції і моделі безпеки інформаційних технологій