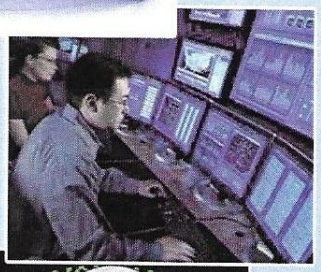
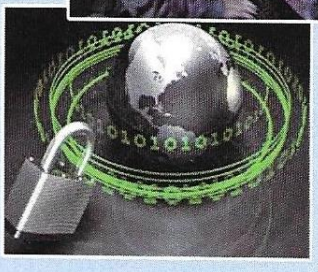
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

В. М. Ахрамович
В. М. Чегренець

Інформаційна безпека

Практикум





В.М. Ахрамович, В.М. Чегренець

Інформаційна безпека
Практикум

Київ 2017

ISBN 5-89173-079-0

УДК 004.056(075.8)
ББК 32. 884
А95
Рецензенти:
Д. т.н., проф. Жук С.Я. (НТУ України «КПІ ім. Ігоря Сікорського»
Д. т.н., проф. Вишнівський В.В. (ДУТ)
Схвалено Вченою радою Державного університету телекомунікацій
(протокол № 16 від 13 лютого 2017 р.).

Ахрамович В.М., Чегренец В.М. Інформаційна безпека. Практикум /В.М.Ахрамович., В.М. Чегренец;
Державного університету телекомунікацій. – К.:ДУТ, 2017. – 396 с. іл. – Бібліограф.:393 с.

ISBN 978-966-2142-76-1

У практикуму відображено не тільки основи рішення задач захисту інформації, але й наведена необхідна теорія до них. (в деяких випадках наведені характеристики спеціального програмного забезпечення, яке використовується) та зроблені висновки, розкриті проблеми, пов’язані з рішеннями вказаних задач.

Усі лабораторні роботи розбиті на шість розділів. У першому розділі: показані приклади захисту інформації за допомогою можливостей різних операційних систем; у другому: – за допомогою можливостей Microsoft Office 2003, 2007 та 2010; у третьому: – шифруванням інформації за допомогою операційних систем та спеціального програмного забезпечення; а також систем програмування; в четвертому: – в різних типах комп’ютерних мереж з використанням мережевих екранів; п'ятому – відновленням даних на дисках, які попередньо видалені , або видалені при форматуванні; шостому – за допомогою спеціальних антивірусних програм.

УДК 004.056(075.8)

ББК 65.290-2
ISBN 978-966-2142-76-1

ЗМІСТ

Вступ

Те, що інформація має цінність, люди усвідомили дуже давно – 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 в таємницю. Є свідоцтва тому, що мистецтво тайнопису зародилося ще в доантичні часи. Сучасне суспільство все більшою мірою стає інформаційно–обумовленим, успіх будь-якого виду діяльності все сильніше залежить від володіння певними відомостями і від відсутності їх у конкурентів. І чим сильніше виявляється вказаний ефект, тим більше потенційні збитки від зловживань в інформаційній сфері, і тим більше потреба в захисті інформації.

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 захисту. 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.

Що ж означає втрата даних, на основі яких ведеться управління бізнесом? За даними Минесотського університету, 93% компаній, що позбулися доступу до своїх даних на термін більше 10 днів, покинули бізнес, причому половина з них заявила про свою неспроможність відразу ж після неможливості доступу до інформації. Хоча компанії, побоюючись за своє реноме, вважають за краще замовчувати випадки краху їх інформаційних систем і вторгнення в них, статистика подібних подій усе ж таки існує. Так, підкомітет із розслідувань при сенаті США провів відповідний опит серед 500 найбільших індустріальних компаній країни. Більш за половину респондентів (264 фірми) утрималися від відповіді, проте 140 компаній визнали, що їх інформаційні системи піддавалися нападам протягом останнього року, і майже п'ята частина з них повідомила, що збитки, що зазнали при цьому, склали понад 1 млн. дол.

Саме із цією метою для підготовки бакалаврів введено дисципліни, «Захист інформації в банківських та комерційних системах», «Системи управління та контролю захистом інформації реального часу», «Системи технічного захисту інформації», «Методи та засоби захисту інформації», «Компонентна база засобів технічного захисту інформації», «Інформаційна безпека іноваціцйної діяльності», «Інформаційна безпека», Книга буде корисною при викладанні навчальної дисципліни бакалаврам, спеціалістам, магістрам.

Ці дисципліни спираються на знання, набуті студентами при вивченні таких дисциплін, як : «Інформатика», «Інформатика та комп'ютерна техніка», «Операційні середовища, системи й оболонки», «Теорія кіл, сигналів і процесів в ІБ», «Інтелектуальна власність», «Комп'ютерне програмування», «Інформаційні системи і технології в управлінні», «Технології проектування та адміністрування БД і СД», «Технології створення програм та інтелектуальних систем», «Інформаційний бізнес», «Комп'ютерні мережі», і т.п.

Метою вивчення навчальної дисципліни «Інформаційна безпека» є: оволодіння сучасними технологіями захисту інформації та навичками їх практичного використання для створення систем безпеки.

Головне завдання дисципліни: вивчення основ інформаційної безпеки та систем захисту, теоретичних положень дослідження складних систем захисту, комп'ютерів, комп'ютерних мереж різних розмірів, технологій захисту, які в них використовуються та системний підхід до дослідження систем безпеки, оволодіння навичками їх практичного використання для подальшої їх розробки і аналізу ефективності.

Основними завданнями вивчення навчальної дисципліни «Інформаційна безпека» є: одержання студентами необхідних теоретичних знань та практичних навичок для побудови ефективного механізму захисту інформації в державних та комерційних системах, вирішення задач організаційно-технічного захисту інформації (на основі використання правових, організаційних і технічних заходів); вибір, залежно від загроз, раціональних способів і засобів інженерно-технічного захисту інформації, прогнозуванні науково-технічного розвитку країни у сфері інформаційної безпеки.

Предметом навчальної дисципліни " Інформаційна безпека " є засоби захисту ін формації.

Науковою базою дисципліни, що вивчається, є теоретичні положення дослідження інформаційної безпеки в окремих комп'ютерах, складних телекомунікаційних та мережевих системах, комп'ютерних мережах різних розмірів, технологій, які використовуються для захисту інформації і системний підхід до дослідження та , оцінки ефективності систем захисту.

Методичною основою є комплексне використання методичних прийомів активізації навчання в ході проведення лекцій з активною самостійною роботою студентів на практичних та самостійних заняттях.

У практикуму відображено не тільки основи рішення задач захисту інформації, але й наведена необхідна теорія до них (в деяких випадках наведені характеристики спеціального програмного забезпечення, яке використовується) та зроблені висновки, розкриті проблеми, пов'язані з рішеннями вказаних задач. Всі задачі розбиті на шість розділів (видів задач):розділ 1 Захист інформації в операційних системах, розділ 2. Захист інформації в Microsoft Office, розділ 3. Захист інформації шифруванням, розділ 4. Захист інформації в мережах за допомогою спеціального програмного забезпечення, .розділ 5. Захист інформації відновленням даних на дисках, які попередньо видалені , або видалені при форматуванні, розділ 6. Захист інформації за допомогою антивірусних програм

Практикум буде корисним для студентів різних спеціальностей, які вивчають курс «Інформаційна безпека», «Захист інформації», «Основи іформаційної безпеки, «Методика розслідування комп'ютерних злочинів» і т. п.

Автори виражають вдячність завідувачу кафедри Систем технічного захисту інформації канд. техн. наук Лазаренко С.В. та директору Навчально-наукового інституту захисту інформації докт техн. наук. Наконечному В.С., Державного університету телекомунікацій за конструктивні зауваження, що були висказані під час підготовки рукопису.

РОЗДІЛ 1
Захист інформації в операційних системах

Лабораторна робота 1
Захист інформації при застосуванні операційної системи Windows XP

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в операційній системі Windows XP.

Ознайомитись з рівнями захисту комп'ютера, можливістю надання прав різним категоріям користувачів, встановлення, зміна, зберігання паролів, встановлення їх параметрів, блокуванням приймання інформації та роботи програм приховування файлів та каталогів.

ПЛАН

1. Теорія
1.1 Парольний захист комп'ютера при його запуску.
1.2. Парольний захист операційної системи
1.3. Запуск Windows у режимі захисту від збоїв
1.4. Керування доступом до каталогів і принтерів
1.5. Брандмауер Windows
1.6 Налагодження безпеки стека протоколів TCP/IP.
1.7 Налагодження безпеки ресурсів мережі.
1.8 Налагодження безпеки за допомогою групової політики.
1.9 Дослідження та захист реєстру операційної системи Windows XP
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. 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 1).
- Використовувати програму злому пароля.
- Скинути CMOS за допомогою перемички або перемикання контактів.
- Скинути CMOS видаленням акумулятора не менш чим на 10 хвилин.
- Викликати переповнення в буфері клавіатури.

- Заміна BIOS на аналогічну модель.

Для визначення типу BIOS на вашому комп'ютері необхідно, наприклад, ввести команду systeminfo із командного рядка (рис. 1).

1.2. Парольний захист операційної системи

Для забезпечення безпеки комп'ютера необхідно організувати захист окремих файлів і каталогів (тек) 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 чекаючому (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):

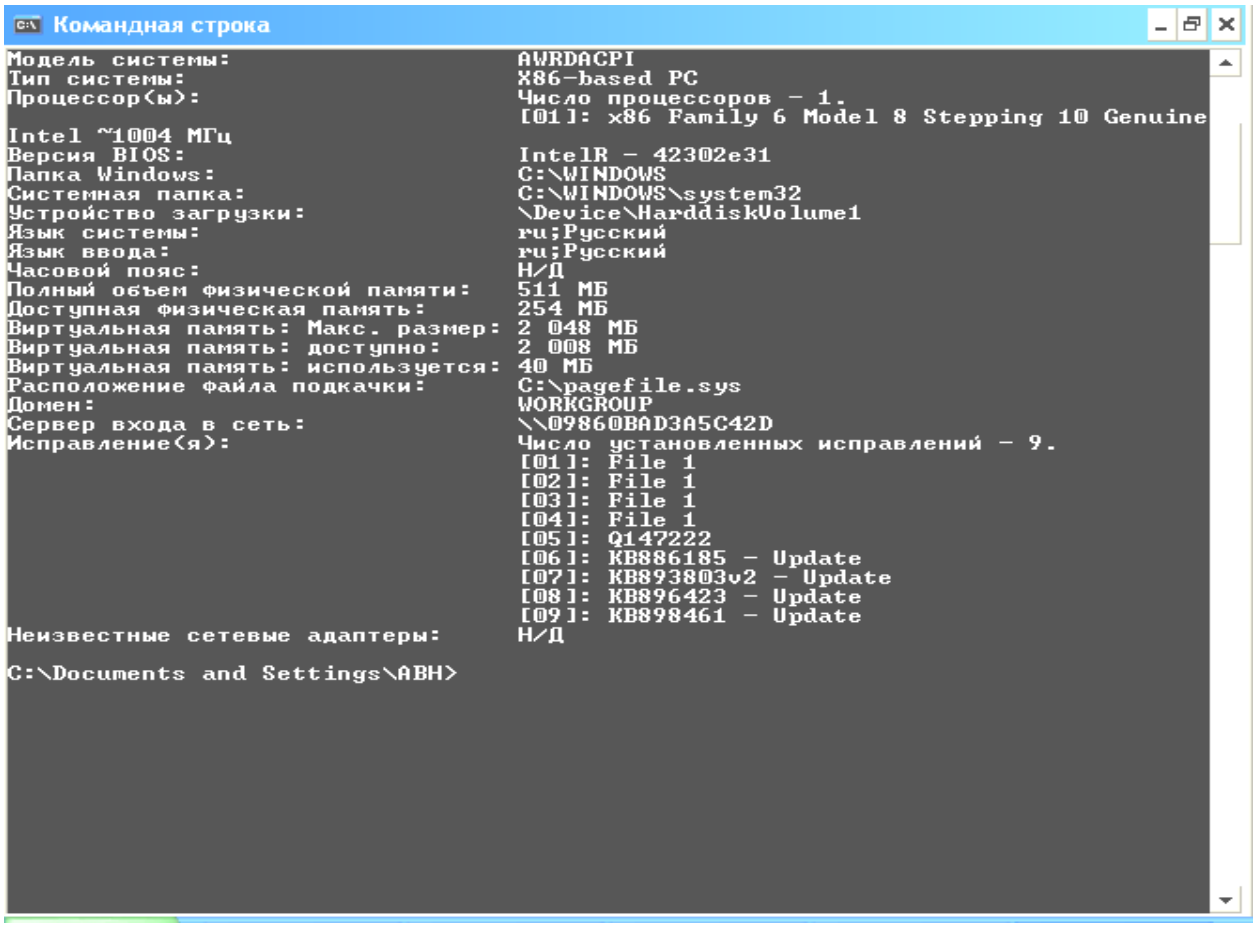


Рис. 1. Вікно командного рядка

1. Натисніть кнопку **Пуск**, виберіть команди **Настройка й Панель управления**, а потім двічі клацніть значок **Электропитание**.

2. Виберіть вкладку **Дополнительно** і встановіть прапорець **Запрашивать пароль при виходе со сплячого режиму** (рис. 3). 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.

Якщо при підключенні до веб-вузла, інтрамережі організації або мережевих тек 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 **Безопасность Windows**.
Натисніть кнопку **Смена пароля**.
Натисніть кнопку **Архивация**, щоб запустити майстер забутих паролів.
Натисніть кнопку **Далее** 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.

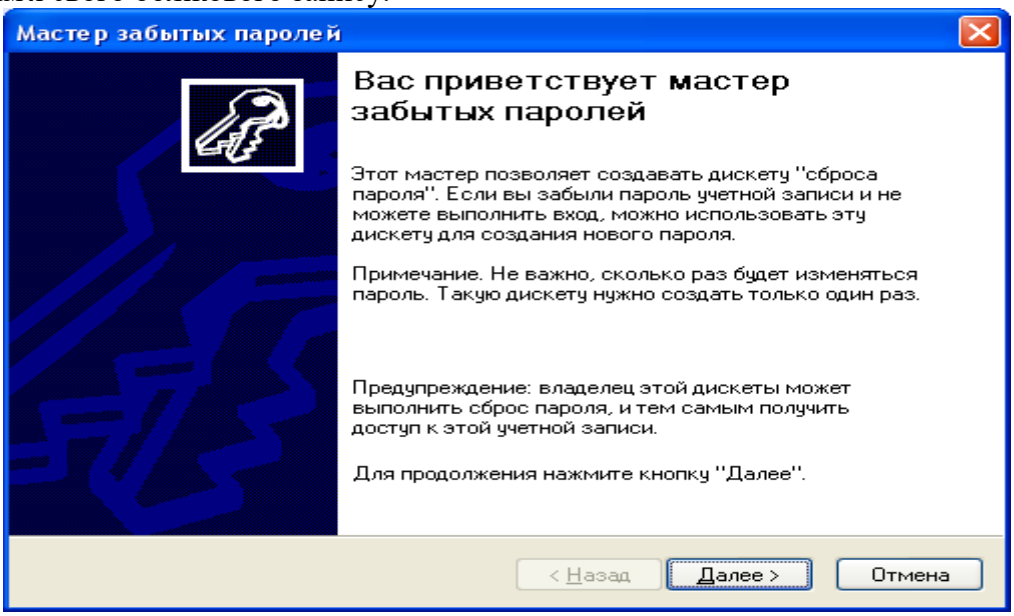


Рис. 2. Вікно майстра забутих паролів

У групі **Подсказка о пароле**, розташованій у вікні зліва, клацніть посилання. З'явиться майстер забутих паролів (рис. 2).
У майстрі забутих паролів слідуйте інструкціям на екрані.
Примітки:

Щоб відкрити компонент «Облікові записи», натисніть кнопку **Пуск**, виберіть команди **Настройка и Панель управления**, потім двічі клацніть значок **Учетные записи пользователей.**

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 **Мой компьютер** і виберіть команду **Свойства.** Якщо ім'я домена відображається на вкладці **Имя компьютера**, комп'ютер приєднаний до домена.

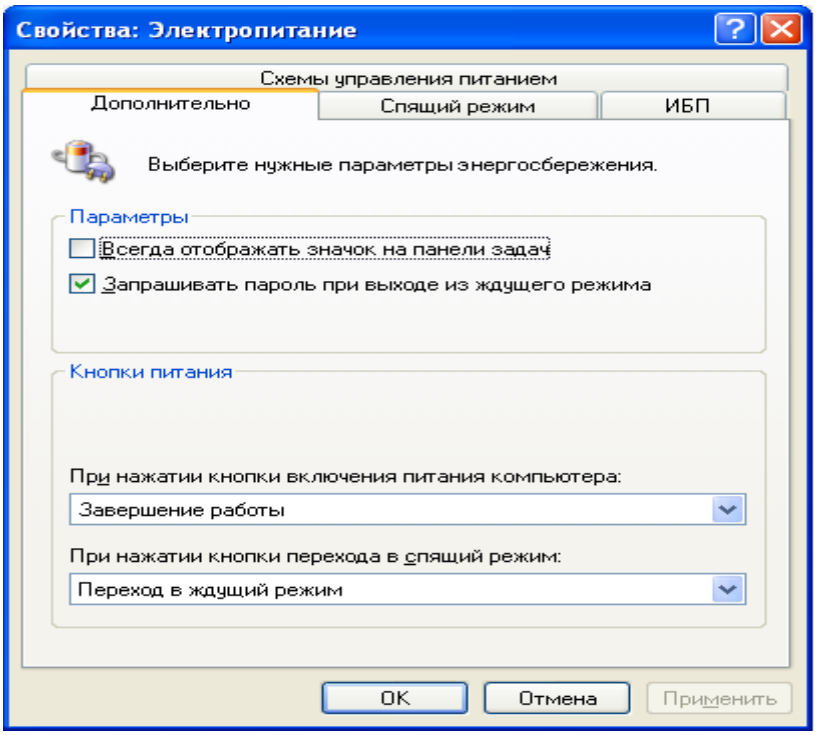


Рис. 3. Вікно Электропитание

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'ютера. Таким чином 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 управления**, потім двічі клацніть значок **Учетные записи пользователей.**

Щоб створити пароль 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.

1. Відкрийте на панелі управління компонент **Учетные записи пользователей**.
2. На вкладці Користувачі виберіть ім'я користувача, для якого потрібно створити пароль, і введіть команду **Изменить учетную запись**, а потім **Создание пароля** (рис. 4)
3. Уведіть новий пароль у поля **Новый 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.

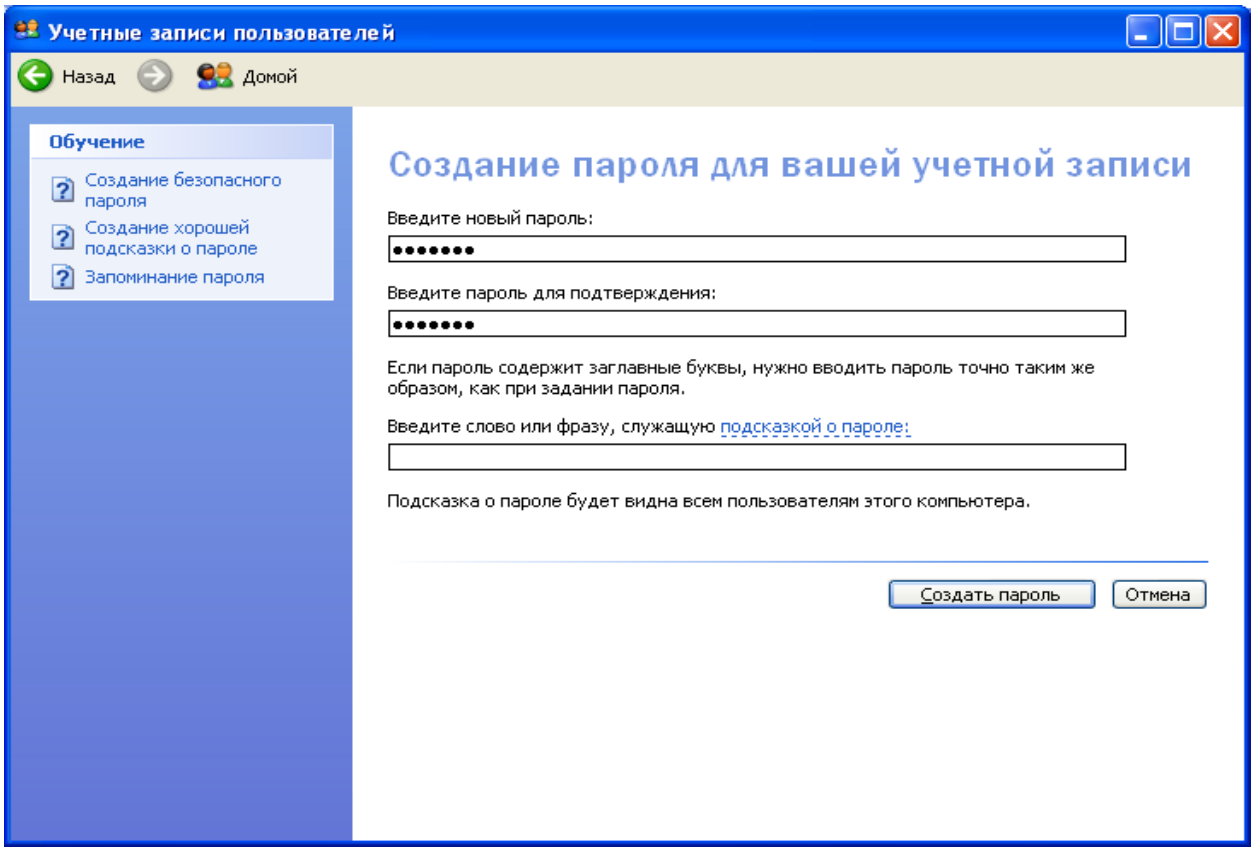


Рис. 4. Вікно введення пароля

- Пароль повинен містити знаки, що відносяться до кожної з наступних трьох груп (табл. 1).

Символи, які можна використовувати для паролів.

Таблиця 1

Група	Приклади
(прописні і рядкові)	... (або a, b, c...)
	3, 4, 5, 6, 7, 8, 9
ли (усі знаки, що не є буквами або цифрами)	# $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ?, . /

- Пароль повинен містити не менше одного символу в позиціях із другою по шосту.
- 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 розшифрування 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.

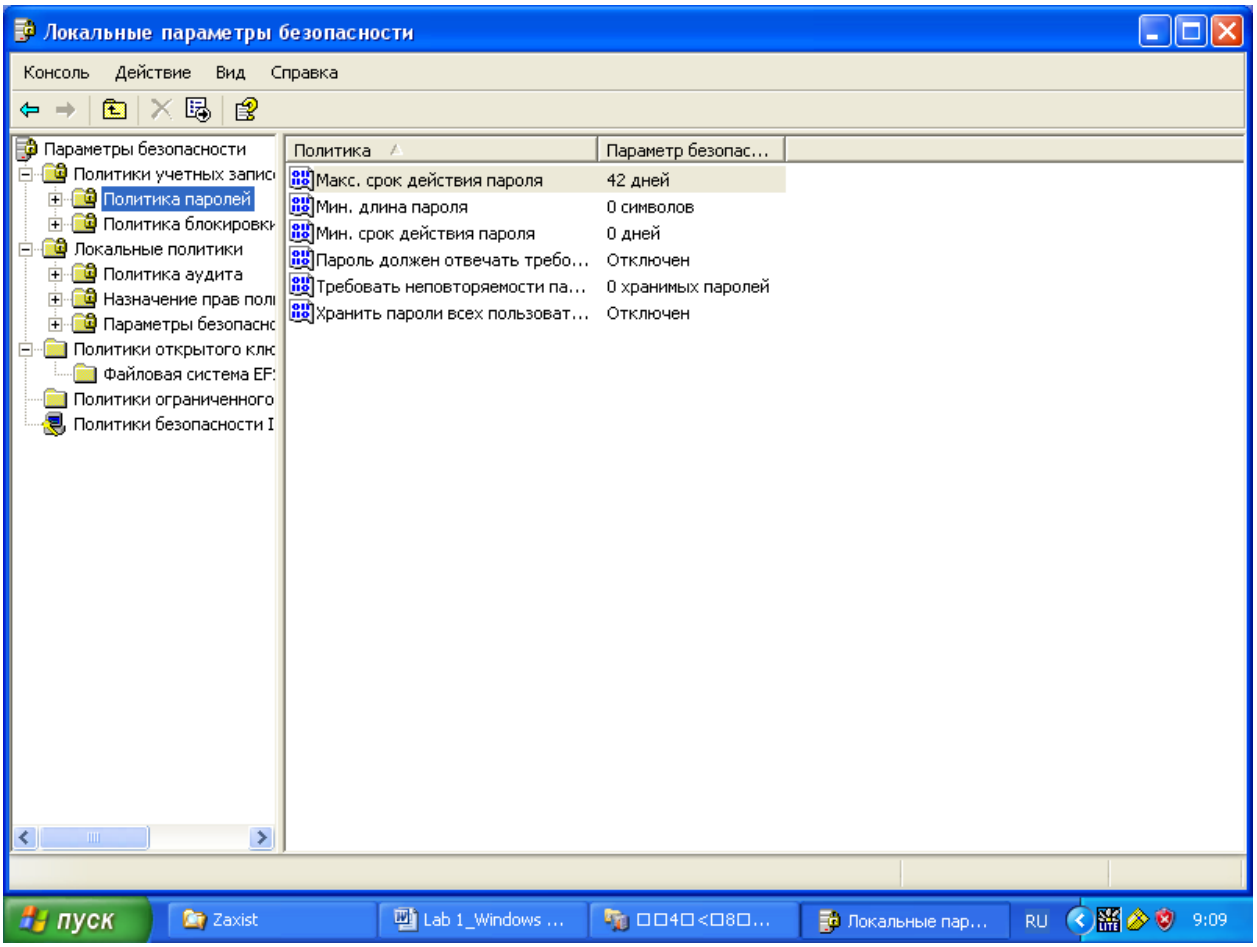


Рис. 5. Вікно встановлення параметрів паролю

Щоб зберегти пароль на комп'ютері:

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

1. У діалоговому вікні **Имя и пароль пользователя**, що виводиться при спробі підключитися до захищеного ресурсу, в полі **Имя пользователя** введіть ім'я користувача.
2. У полі **Пароль** введіть пароль.
3. Установіть прапорець **Сохранить пароль**.
4. Установіть прапорець **Больше не спрашивать этот пароль**.

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

5. Для встановлення терміну дії пароля та інших його параметрів треба натиснути кнопку **Пуск**, виберіть команди **Настройка и панель управления**, а потім двічі клацніть значок **Администрирование**, двічі клацніть значок **Локальная политика безопасности** та виберіть **Политика учетных записей** та **Политика паролей** (рис. 5). Установіть необхідні параметри паролю, наприклад, термін дії (рис. 6) .

1.3. Запуск Windows у режимі захисту від збоїв

1. Натисніть кнопку **Пуск** і виберіть команду **Завершение работы**.
2. Виберіть параметр перезавантажити комп'ютер, натисніть кнопку **OK**, а потім натисніть і утримуйте клавішу **CTRL** до появи меню завантаження Microsoft Windows.
3. На деяких комп'ютерах для виклику меню завантаження Microsoft Windows можна використовувати клавішу **F8** замість клавіші **CTRL**.

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

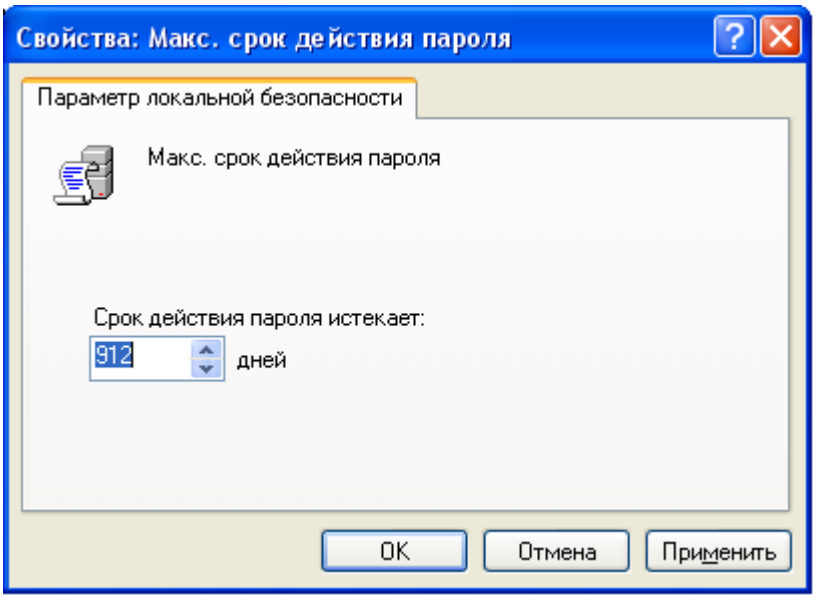


Рис. 6. Вікно встановлення терміну дії пароля

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 теж відсутній.
- Для зміни Налагодження можна натиснути кнопку **Пуск**, вибрати команди **Настройка и панель управления**, а потім двічі клацнути значок **Сеть** чи **Система**.
- Після завершення даної процедури для запуску в Windows звичайному режимі буде потрібно перезавантаження комп'ютера.

1.4. Керування доступом до каталогів і принтерів

1. У вікні **Мой компьютер** чи у вікні провідника виберіть папку чи принтер, доступ до яких потрібно обмежити.
2. У меню **Файл** виберіть команду **Свойства**.
3. Виберіть вкладку **Доступ**.
4. Якщо застосовується керування доступом на рівні користувачів, натисніть кнопку Добавить для вказівки користувачів, разом із якими варто використовувати принтер чи папку.
5. Якщо застосовується керування доступом на рівні ресурсів, уведіть пароль для доступу до каталоги чи принтеру.

1.5. 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 несанкціонованого намагаються підключитися до комп'ютера.

Можна вважати брандмауер прикордонним постом, на якому перевіряється інформація (часто звана трафік), 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)

Таблиця 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 «черв'яки», 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, «черв'яками» 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 Аркуш, поки не зв'яжетеся з відправником для отримання підтвердження.
Звістці облік (журнал безпеки) — за	Блокувати спам або несанкціоновані

бажанням користувача — записуючи дозволені й заблоковані спроби підключення до комп'ютера. Цей журнал може виявитися корисним для діагностики неполадок..	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 **Настройка и панель управления**. Двічі клацніть по піктограмі **Брандмауэр Windows.**
2. На вкладці **Общие** виберіть один із наступних параметрів.

o **Включить** рис. 7. (рекомендується). Звичайно, використовується цей параметр

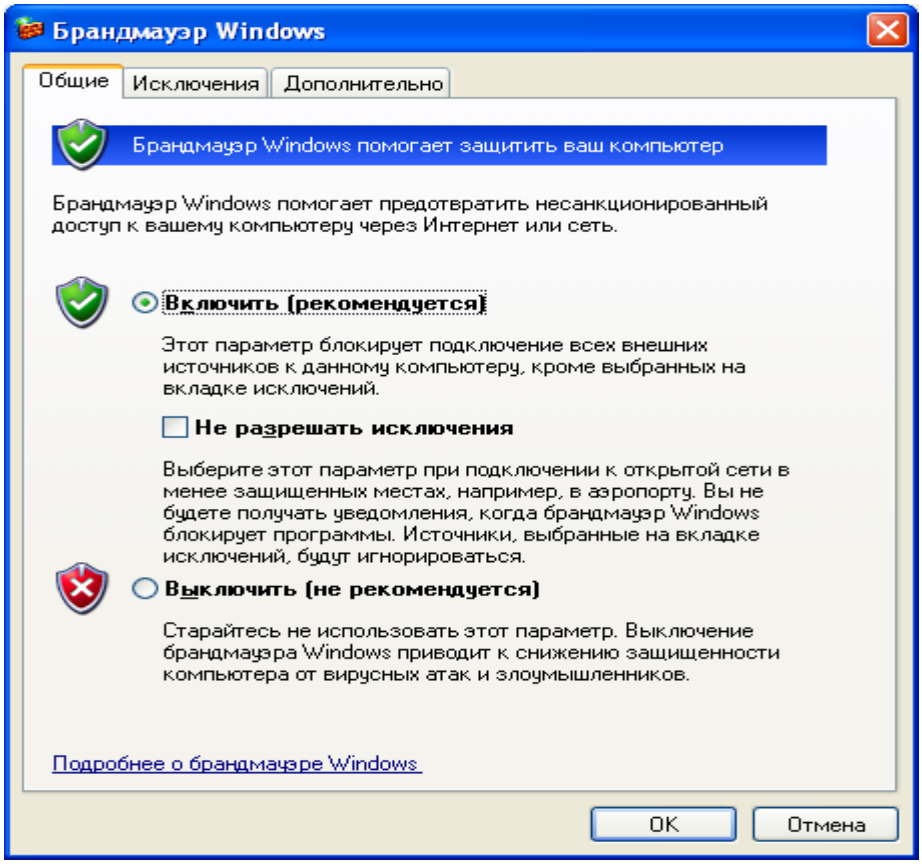


Рис. 7. Вікно брандмауера

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, наприклад, при підключенні до загальнодоступної мережі в готелі або аеропорту або в періоди розповсюдження через Інтернет особливо небезпечних вірусів або черв'яків.

- 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 бреши 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 ви можете 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 **Исключения** в групі **Программы и службы** встановіть прапорець для програми або служби, яку потрібно вимкнути, а потім натисніть кнопку **ОК**.

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

Натисніть кнопку **Добавить программу** (рис. 8).

У діалоговому вікні **Добавить программу** виберіть програму, яку потрібно додати, і натисніть кнопку **ОК**. Ця програма з'явиться (із установленим прапорцем) на вкладці **Исключения** в групі **Программы и службы**

Натисніть кнопку **ОК**.

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

У діалоговому вікні **Добавить программу** натисніть кнопку **Осмотр**, знайдіть програму, яку потрібно додати, і двічі клацніть по ній. (Програми, звичайно, зберігаються на комп'ютері в теці Program Files.) Програма з'явиться в групі Програми в діалоговому вікні **Добавить программу**.

Натисніть кнопку **ОК**. Ця програма з'явиться (із установленим прапорцем) на вкладці **Исключения** в групі **Программы и службы**.

Натисніть кнопку **OK**.

Якщо програму як і раніше не вдалося знайти, можна відкрити порт. Порт подібний маленьким дверцям у брандмауері, через які дозволяється взаємодіяти. Щоб визначити, який порт потрібно відкрити, на вкладці **Исключения** натисніть кнопку **Добавить 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.

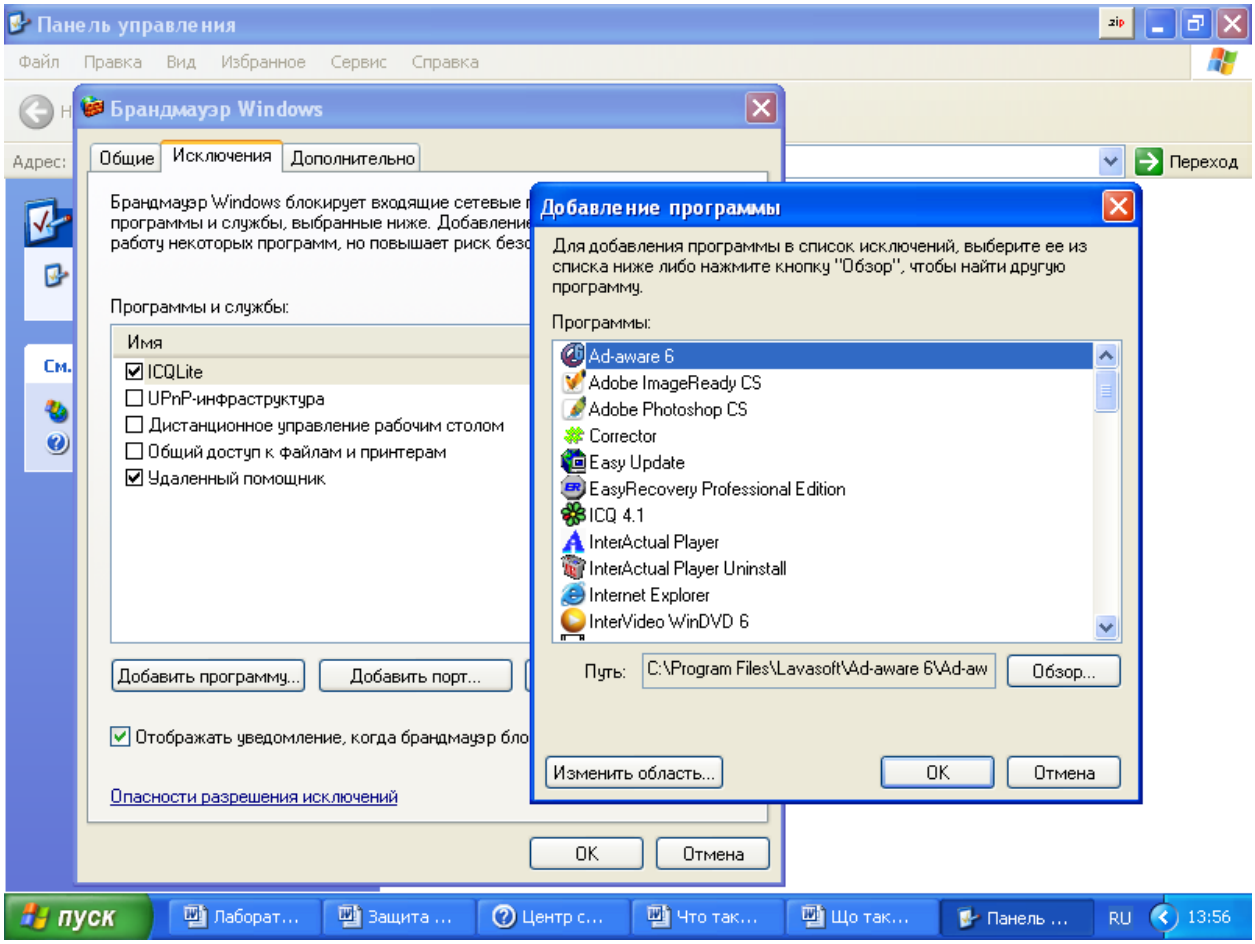


Рис. 8. Вікно додавання програми до списку виключень

Додаткові параметри

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. 9). Список портів наведений в додатку 1.

1. Відкрийте брандмауер Windows.

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

1. У діалоговому вікні **Изменение порта** або **Изменение программы** виберіть параметри, які потрібно змінити.

Визначення активних параметрів брандмауера Windows

Поєднання параметрів на вкладці **Исключения** і будь-які додаткові параметри в розділі **Параметры сетевого подключения** на вкладці **Дополнительно** називаються «Результуючим набором» параметрів брандмауера Windows.

Для кожного підключення результуючий набір параметрів може бути різним.

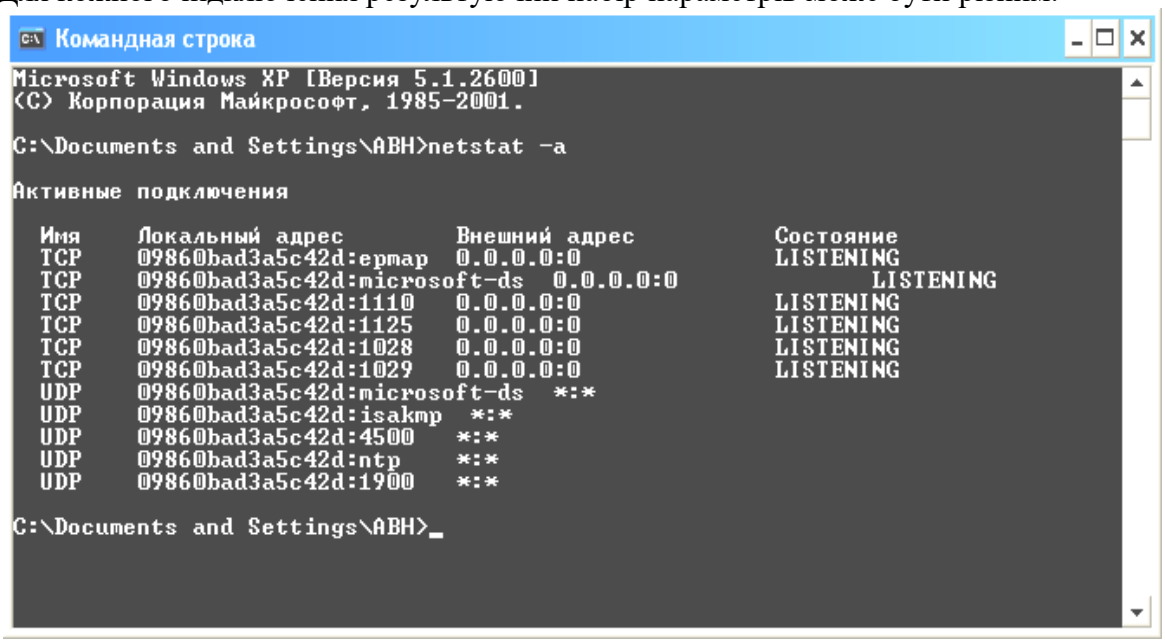


Рис.. 9. Список активних портів комп'ютера

Параметри, що відкривають порт для певного підключення, мають вищий пріоритет у порівнянні з глобальними параметрами, які можуть забороняти відкриття цього порту. У табл. 3. приведені декілька прикладів.

Поєднання параметрів брандмауера Windows

Таблиця 3

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 **Дополнительно** в групі Ведение журнала безопасности натисніть кнопку **Параметры**. Виберіть один із наступних параметрів. Щоб включити реєстрацію невдалих спроб установлення вхідного підключення, встановіть прапорець **Записывать пропущенные пакеты**. Щоб уключити реєстрацію успішних витікаючих підключень, встановіть прапорець **Записывать успешные подключения.**

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 **Дополнительно** в групі **Ведение журнала безопасности** натисніть кнопку **Параметры**.

У полі **Граничный размер файла журнала**: 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.

1. 6 Налагодження безпеки стека протоколів TCP/IP.

Щоб налагодити безпеку протоколу TCP/IP необхідно скористатися меню «Пуск», у пунктах «Налагодження», «Панель керування», вибрати «Мережа й вилучений доступ до мережі». Вибрати інтерфейс, для якого буде настроюватися контроль вхідного доступу, вибрати команду «Властивості», у списку «Відзначені компоненти використовуються цим підключенням», вибрати елемент «Протокол Інтернету (TCP/IP)», «Властивості». У вікні «Властивості протоколу Інтернету (TCP/IP)» натискнути кнопку «Додатково». Відкрити вкладку «Параметри». Вибрати параметр «Фільтрація TCP/IP» і натискнути кнопку «Властивості». Установити прапор «Задіяти фільтрацію TCP/IP (всі адаптери)». Установка цього параметра, приводить до включення фільтрації для всіх адаптерів, настроювати фільтри необхідно окремо для кожного адаптера. Одні й ті ж самі фільтри не застосовуються до всіх адаптерів.

1.7 Налагодження безпеки ресурсів мережі.

Права доступу визначають повноваження окремих користувачів або груп користувачів, які перебувають в одній мережі.

Існує два способи керування доступом:

– на рівні ресурсів, коли надається доступ всім користувачам, які знають пароль;

– на рівні користувачів, коли визначаються користувачі, яким дозволений доступ до загальних ресурсів комп'ютера й надаються права.

При керуванні доступом на рівні ресурсів пароль установлюється для кожного загального ресурсу. Різним користувачам можна надати різні типи доступу: повний доступ, доступ тільки для читання або обидва типи доступу.

При другому способі керування доступом, список користувачів мережі зберігається на сервері й може бути змінений тільки адміністратором мережі.

Для керування доступом на рівні користувачів комп'ютер повинен бути підключений до сервера ОС Windows або ОС NetWare. У мережах з рівноправними вузлами не можна управляти доступом на рівні користувача.

Для доступу до диска на іншому комп'ютері мережі потрібно відкрити директорію «Мережне оточення» (My network places). У цій директорії поміщені значки всіх комп'ютерів та всіх мережних принтерів, які входять в один домен і доступні в мережі на даний момент. Ця директорія, дозволяє одержати доступ, при наданні прав, до цих ресурсів мережі.

1.8. Налагодження безпеки за допомогою групової політики.

Редактор об'єктів групової політики являє собою засіб керування настроюванням користувача й комп'ютера, що входить до складу «Каталога домена» (Active Directory). До групової політики входять параметри безпеки, задані в редакторі об'єктів групової політики. Параметри безпеки постійно зберігаються в реєстрі, у той час як параметри адміністративних шаблонів групової політики перезаписуються при кожному відновленні політики.

Редактор об'єктів групової політики використовується для редагування об'єктів групової політики, у тому числі перетворених з формату майстра налагодження безпеки.

Крім створення й поширення політик безпеки за допомогою майстра налагодження безпеки, можна застосувати параметри безпеки, скориставшись шаблонами. Шаблони безпеки являють собою файли з розширенням INF, наприклад, securedc.inf, які за замовчуванням розташовані в каталозі systemroot%\security\templates\. Параметри шаблона безпеки в редакторі єктів групової політики й консолі керування груповою політикою розташовані в наступному місці: ім'я_об'єкта_групової_політики\Computer Configuration\WindowsSettings\ SecuritySettings\ Існує три способи застосування шаблонів безпеки:

– для підключення шаблона безпеки до об'єкта групової політики необхідно вибрати елемент «Параметри безпеки», вибрати «Імпортувати політики» і вказати місцезнаходження файла з розширенням INT;

– підключити шаблон безпеки до політики майстра налагодження безпеки вікні «Ім'я файла політики безпеки» «Включити шаблони безпеки», натиснути Додати»;

– підключити шаблон до файла політики з розширенням XML і виконати з командного рядка команду scwcmd transform/p:файл_політики.xm/g: відображуване_ім'я_об'єкта_групової політики, щоб створити об'єкт групової політики, який можна потім зв'язати за допомогою консолі керування груповою політикою.

У середовищі, де застосовується групова політика, майстер налагодження безпеки й кілька шаблонів безпеки варто використовувати наступні рекомендації, щоб спрогнозувати пріоритетність тих або інших параметрів безпеки:

Політика безпеки, застосовувана за допомогою об'єктів групової політики Active Directory, має більш високий пріоритет, ніж політика безпеки, застосовувана за допомогою файлів політики майстра налагодження безпеки (файли XML).

Пріоритет об'єктів групової політики по відношенню один до одного не залежить від того, застосовувався для їхнього створення засіб scwcmd.exe чи ні. Використовуються стандартні правила спадкування Active Directory, згідно яким послідовно застосовуються об'єкти групової політики локального рівня, рівня сайта, домена й підрозділу, а також порядок прив'язки об'єктів.

Політика безпеки, задана за допомогою засобів інтерфейсу користувача майстра налагодження безпеки, має більш високий пріоритет, ніж конфліктуюча політика шаблона безпеки INF-Файла, підключеного до XML- Файла політики.

Якщо до XML-Файла підключено кілька шаблонів безпеки, шаблон, розташований вище в списку діалогового вікна «Включення шаблонів безпеки», має більш високий пріоритет, ніж розташовані нижче.

Забезпечення безпеки за допомогою моніторингу системи. Програма «Перегляд подій» використовується для перегляду подій, записаних у журналах додатків, безпеки й системи. У журналах подій засобу перегляду подій відображають відомості про неполадки устаткування, додатків і системи. Можна вести спостереження за подіями системи безпеки.

Спостереження за продуктивністю системи є важливою складовою частиною системи обслуговування й адміністрування операційною системою.

Дані про продуктивність використовуються для:

– визначення завантаження системи й ефективності використання ресурсів системи;

– виявлення змін і тенденцій у робочому навантаженні й використанні ресурсів для планування майбутньої модернізації;

– перевірки змін конфігурації й інших способів налагодження;

– діагностики неполадок і кінцевих компонентів або процесів з метою оптимізації.

Компоненти «Системний монітор» і «Журнали й оповіщення продуктивності» надають докладні відомості про ресурси, використовувані конкретними об'єктами операційної системи й програмами, призначеними для збору даних. Дані про продуктивність відображаються у вигляді діаграм. Крім того, дані записуються в журнали. Компонент «Оповіщення» дозволяє відправити користувачам повідомлення, коли значення лічильника досягне, перевищить або впаде нижче заданого граничного значення.

Консоль «Продуктивність» включає наступні засоби:

– системний монітор;

– журнали й оповіщення продуктивності;

– диспетчер завдань.

1.9. Дослідження та захист реєстру операційної системи Windows XP

У редактора реєстру є ключ /e, що дозволяє автоматично зберігати в reg-файлі певний розділ реєстру. Це може знадобитися, коли потрібно зберегти налагодження певної програми, наприклад, при щоденному резервному копіюванні. Експорт може бути здійснений як з командного рядка, так і з пакетного файла. Наступна команда зберігає ключ реєстру HKEY_CURRENT_USER\Software\Far у файл far.reg regedit /e c:\far.reg HKEY_CURRENT_USER\Software\Far У результаті роботи цієї команди з кореня диска C:\\ буде створений файл far.reg, що містить всі підрозділи й параметри зі значеннями зазначеного розділу реєстр. Для того, щоб відновити всі налагодження, буде досить запустити цей файл.

Для автоматизації збереження ключів реєстр можна написати пакетний файл, що буде запускатися «Планувальником» у певний час. У реєстрі можуть зберігатися дані семи типів:

REG_BINARY зберігає довільні двійкові дані, без переформатування й синтаксичного розбору. Ці дані можна переглядати у двійковому або шістнадцятирічному виді за допомогою редактора реєстру.

REG_DWORD зберігає параметри, представлені восьмибайтними цілими числами. Цей тип даних звичайно застосовується, коли параметр позначає лічильник або інтервал. Ще одне його застосування як флаг (0 - флаг знятий, 1 - встановлений).

REG_SZ являє собою звичайний рядок у кодуванні Unicode будь-якої довжини. В цьому типі даних зберігається інформація, яка буде читатися користувачем, шляхи доступу, назви пристроїв.

REG_EXPAND_SZ - вид REG_SZ, використовується додатками для зберігання конструкцій виду %SystemRoot%\System32, наприклад. При читанні цього рядка Windows заміняє %SystemRoot% на ім'я папки, куди вона встановлена.

REG_MULTI_SZ являє собою набір довільної кількості параметрів типу REG_SZ. У цьому типі даних зберігається, наприклад, список IP-адрес, призначених мережному інтерфейсу.

REG_FULL_RESOURCE_DESCRIPTOR застосовується для кодування інформації про системні ресурси, необхідні для якого-небудь із пристроїв.

REG_NONE служить як семафор, тобто параметр існує, але не містить ніякого значення. Деякі додатки перевіряють наявність цього параметра й, виходячи з результату перевірки, виконують або не виконують дію.

Кореневі розділи реєстру.

HKEY_LOCAL_MACHINE (HKLM) зберігає всі налагодження, що ставляться до локального комп'ютера. У підрозділі HARDWARE зберігаються записи операційної системи й драйверів. А також спільно використовувана, поділювана інформація про фізичні пристрої, що виявляються операційною системою під час завантаження інших пристроїв Plug-and-Play, які можуть бути додані після завантаження операційної системи. Додатки повинні зберігати тут дані тільки в тому випадку, коли вони призначені для всіх, хто користується комп'ютером. Наприклад, драйвер принтера може зберігати набір настроювань принтера, застосовуваних за замовчуванням, і копіювати ці дані для кожного профілю користувача при вході користувача в систему.

HKEY_USERS (HKU) містить записи для кожного з користувачів, які коли-небудь входили в систему. Власником кожної із цих записів є відповідний користувальницький обліковий запис, там утримуються налагодження профілю цього користувача. Якщо використовується групова політика, то налагодження, що задаються в ній, застосовуються тут до профілів окремих користувачів.

HKEY_CURRENT_CONFIG (HKCC) зберігає інформацію про поточну завантажувальну конфігурацію комп'ютера. Зокрема, тут зберігається інформація про поточний набір системних служб і про пристрої, що були під час завантаження. Цей кореневий розділ є покажчиком на розділ усередині HKLM.

HKEY_CURRENT_USER (HKCU) указує на профіль поточного користувача, що ввійшов у цей момент у систему. Microsoft вимагає, щоб додатки зберігали всі переваги користувачів у підрозділах під HKCU. Наприклад, HKCU\Software\Microsoft\Windows\Current Version\Applets\Paint містить особисті налагодження користувачів програми Paint.

HKEY_CLASSES_ROOT (HKCR) співставляє розширення файлів і ідентифікатори класів OLE. Фактично він указує на HKLM\Software\Classes. Система використовує ці відповідності щоб визначити, які додатки або компоненти потрібно використовувати при відкритті або створенні тих чи інших типів файлів, або об'єктів даних. Синтаксис REG-Файлу. Перший рядок може бути двох типів:

– REGEDIT4 - формат reg-файла, який співпадає з операційними системами Windows 98/NT.

– Windows Registry Editor Version 5.00 указує на те, що даний файл співпадає з операційними системами Windows 2000 і вище.

Другий рядок повинен бути порожній.

Далі, необхідно вказати розділ реєстру. який являє собою шлях до параметра, який змінюється. У форматі REG-Файлів розділи завжди вказують у квадратних дужках.

Далі, необхідно вказати параметр реєстру і його значення. Залежно від значення параметра, змінюється поводження операційної системи або об'єкта.

Багато параметрів можна налагодити в графічному інтерфейсі операційної системи, але не всі. У таких випадках для зміни параметра використовують редактори реєстру, «твікери» або REG-файли. Якщо необхідно провести зміни в декількох розділах, один рядок між останнім параметром попереднього розділу й назвою наступного розділу залишається порожнім.

Всі рядки, що починаються з крапки з комою, являються коментарями. Значення параметрів REG-Файла. Кожному типу параметрів відповідають свої значення. Для видалення розділу з реєстру треба перед його ім'ям у квадратних дужках поставити символ «-». Запуск reg-файлів з командних файлів. Якщо reg-файли необхідно періодично застосовувати, можна використовувати командний bat-файл із рядками виду REGEDIT /S "D:\path\filename.reg" Ключ /S, (silent), не виводить запит на підтвердження внесення змін до реєстру й появу повідомлення про внесення змін.

Можна скористатися командним файлом для швидкого збереження розділів реєстру в reg-файли. Такий командний файл повинен складатися з рядків виду:

REGEDIT /EA «D:\path\filename.reg» «HKEY_CURRENT_USER\name» Ключ /EA, export ANSI, означає експорт у форматі REGEDIT4, що має кодування ANSI. Якщо вказати ключ /E, то Windows 2000/XP експортує розділи реєстру в кодуванні UNICODE, що створює проблеми при редагуванні reg-файлів редакторами, що не підтримують UNICODE, наприклад, стандартним блокнотом і його аналогами. Windows 95/98/Me/NT кожного разу експортує в кодуванні ANSI.

2. Хід роботи

1. Установіть парольний захист для BIOS вашого комп'ютера. Пароль із метою виключення помилок обов'язково записати в зошит.
2. Зніміть парольний захист для BIOS вашого комп'ютера.
3. Установіть парольний захист для Windows вашого комп'ютера. Пароль із метою виключення помилок обов'язково записати в зошит.
4. Зніміть парольний захист для Windows вашого комп'ютера.
5. Змініть, а потім зніміть парольний захист для групи користувачів з обмеженим доступом до Windows вашого комп'ютера
6. Установіть та зніміть парольний захист у режимах чекання та сплячки.
7. Запустіть ваш комп'ютер у режимі захисту від збоїв.
8. Запустіть ваш комп'ютер у звичайному режимі.
9. Установіть за вказівкою викладача на диску “C” керування доступом до каталогів та файлів.
10. Запустіть брандмауер Windows та проведіть його налагодження згідно попередньої теорії за вказівкою викладача.
11. Включити фільтрацію для всіх адаптерів в Windows XP
12. Надати права доступу до диска комп’ютера
13. Підключити шаблон безпеки до об'єкта групової політики
14. Підключити шаблон до файла політики з розширенням XML
15. Продивитися системний монітор, журнали й оповіщення продуктивності, диспетчер завдань.

3. 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. Налагодження безпеки стека протоколів TCP/IP
15. Способи керування доступом до мережі
16. Налагодження безпеки за допомогою групової політики
17. Який тип політики має більш високий приорітет: Active Directory чи файли XML?
18. Яке призначення компоненти «Системний монітор» і 1. «Журнали й оповіщення продуктивності»?
19. Дослідження та захист реєстру операційної системи Windows XP
20. Які типи даних зберігаються в реєстрі?
21. Призначення файлу far.reg.
22. Охарактеризуйте кореневі розділи реєстру.

Лабораторна робота 2
Захист інформації у мережах Microsoft Windows

Мета роботи – Засвоїти принципи і технологію захисту інформації у операційній системі Microsoft Windows.

Ознайомитись з можливістю надання прав різним категоріям користувачів, доступу до дисків, каталогів, файлів, використання загальних ресурсів в локальній мережі та контролю за їх використанням, зміною мережевих паролів.

ПЛАН

1. Теорія

Робота мережі забезпечується програмами операційних систем Windows 3.X, Windows 95, Windows 98, Windows NT, Windows XP, Windows 2000, Windows 7, Windows 8, Windows 10. Як правило, відразу при запуску системи машина автоматично запитує Login name (те ж саме, що і user ID) і пароль.

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 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 **Сетевое окружение** на робочому столі, а потім двічі клацніть значок комп'ютера. Якщо потрібного комп'ютера немає в списку, двічі клацніть піктограму **Вся сеть**.

1.1 Призначення загального каталогу

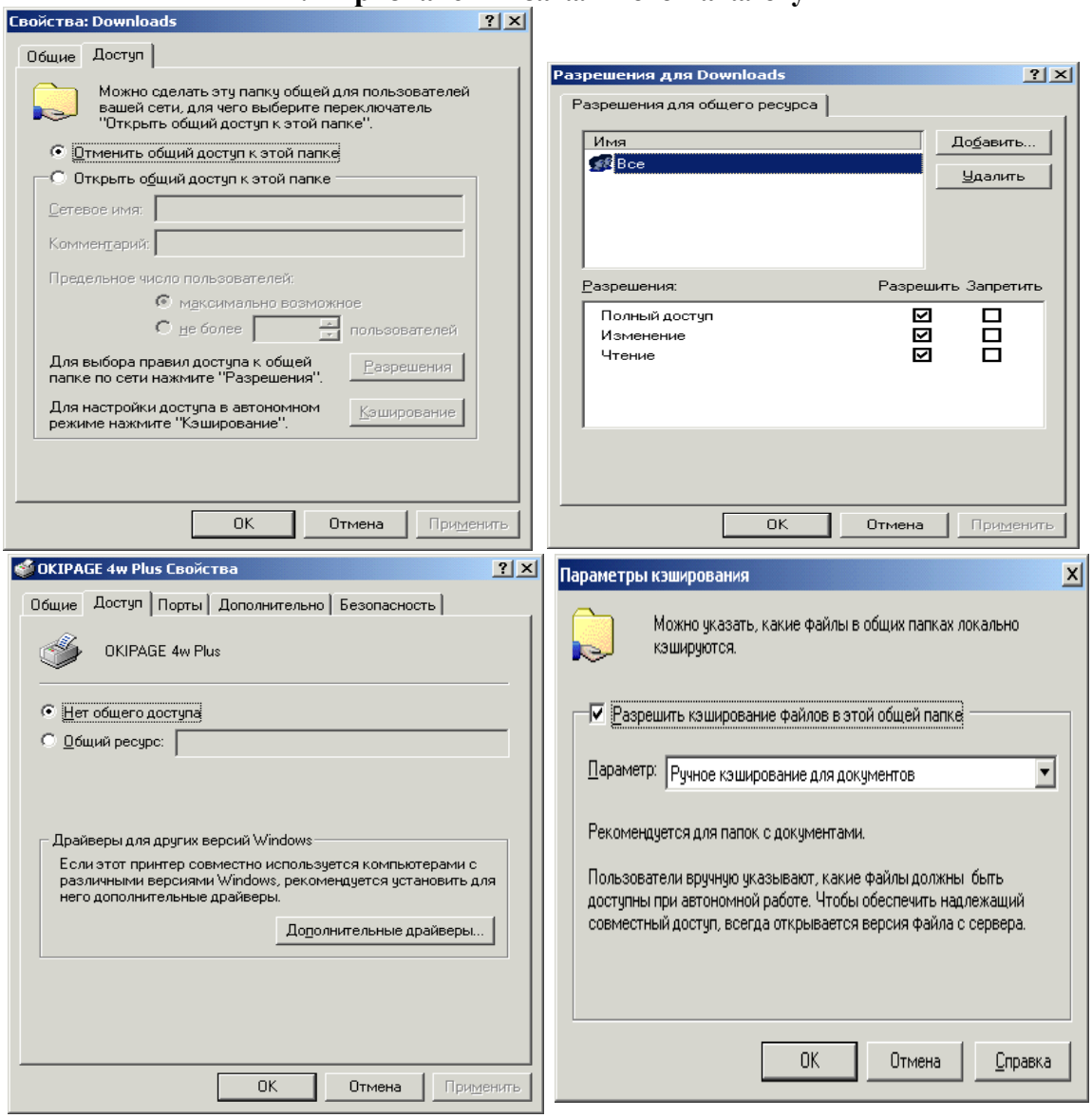


Рис.1. Вибір типу доступу до каталога.

У вікні **Мой компьютер** або в провіднику Windows виберіть каталог, що потрібно зробити загальним. У меню **Файл** виберіть команду **Свойства**. Виберіть вкладку **Доступ**, а потім виберіть параметр **Открыть доступ к этой папке** (рис. 1). Виберіть тип доступу в групі **Тип доступа** 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.

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

1.2 Призначення загального принтера

Натисніть кнопку **Пуск**, виберіть команду **Настройка**, а потім виберіть **Принтеры**. Клацніть значок принтера, що потрібно зробити загальним. У меню **Файл** виберіть команду **Свойства**. Виберіть вкладку **Доступ**, а потім виберіть параметр **Общий ресурс**.

1.3 Керування доступом до каталогів і принтерів

У вікні Мій комп'ютер або у вікні провідника виберіть загальну папку або принтер, доступ до яких потрібно обмежити. У меню **Файл** виберіть команду **Свойства**. Виберіть вкладку **Доступ**. Якщо застосовується керування доступом на рівні користувачів, натисніть кнопку **Добавить** 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.

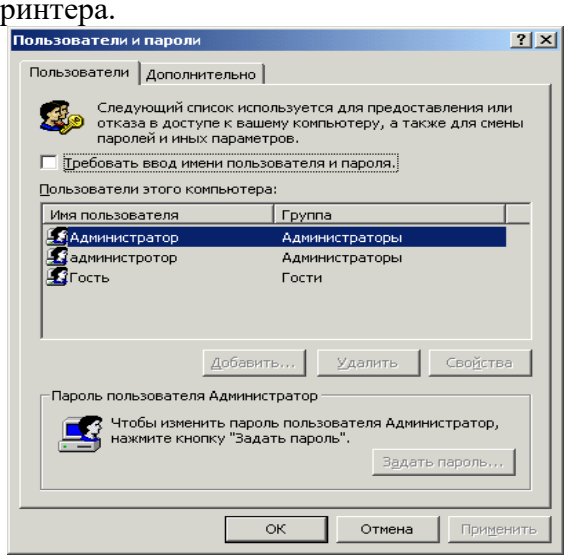


Рис. 2. Вікно користувачів

1.4 Зміна мережевого пароля

Для відкриття діалогового вікна Властивостію. Треба натиснути кнопку **Пуск**, вибрати команди **Настрока и панель управления**, а потім двічі клацнути значок **Пользователи** (рис 2). Натисніть кнопку **Задать пароли**. Виберіть пароль, що потрібно перемінити, і натисніть кнопку **Изменить**. Уведіть старий пароль. Уведіть новий пароль, а потім знову введіть його в поле **Подтверждение пароля**.

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

1.5 Призначення прав адміністратора, користувача, гостя.

На комп'ютері з операційною системою Windows NT натисніть кнопку **Пуск** і виберіть команди **Программы и Администрирование**, Локальна політика безпеки, а потім **Политика учетных записей**, виберіть **Политика паролей** (рис. 3), аналогічно вибираються права користувача (рис. 4). Виконуйте інструкції, які виводяться на екран. На комп'ютері з операційною системою більш пізньої натисніть кнопку **Пуск**, виберіть команди **Программы**, **Стандартные** й **Служебные**, а потім виберіть **Назначенные задания**.

На комп'ютері з операційною системою Windows NT натисніть кнопку **Пуск** і виберіть команди **Программы** й **Администрирование**, **Назначение прав пользователя**. 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 **Программы** й **Администрирование**, **Управление компьютером** та перегляньте відповідні можливості діалогових вікон (рис. 5).

1.6 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 **Программы**, **Стандартные** й **Служебные**, а потім вибрати команду **Инспектор**.

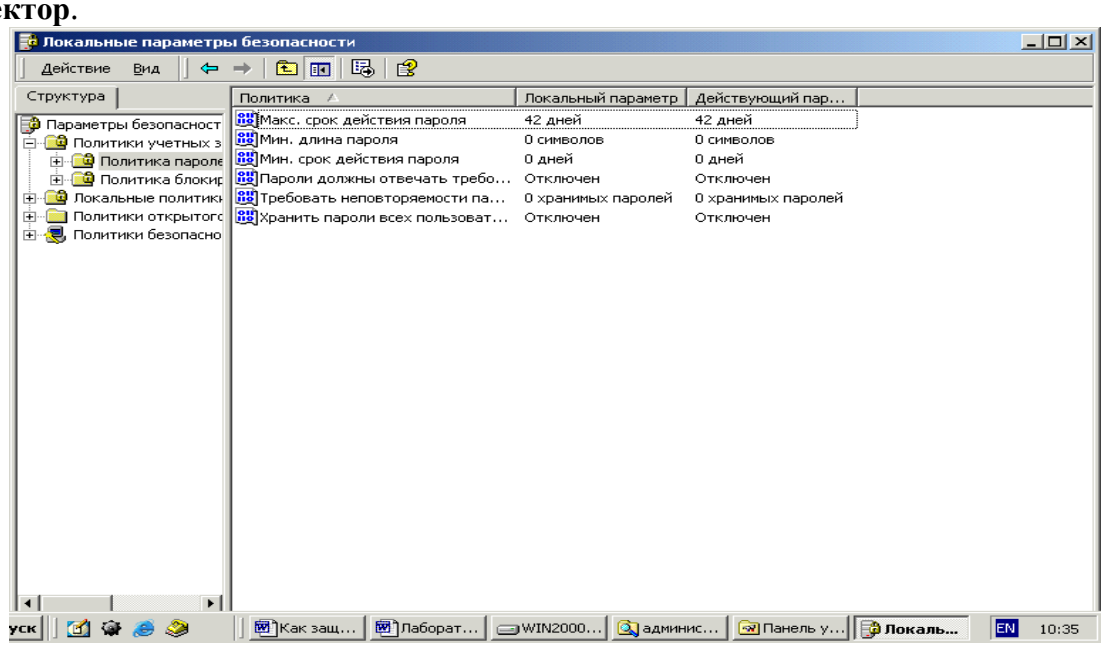


Рис. 3. Призначення параметрів паролів адміністратора, користувача, гостя.

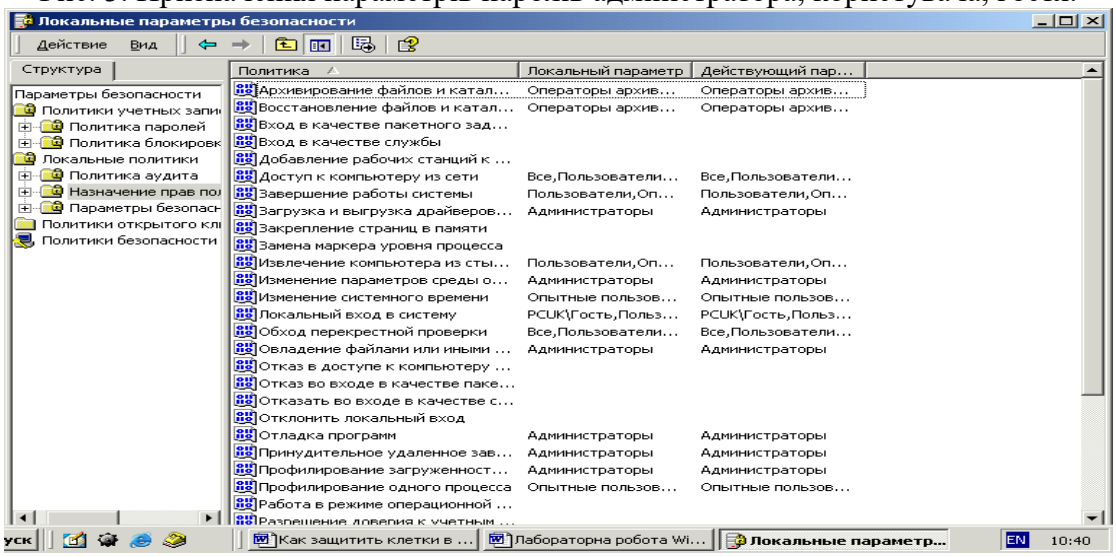


Рис. 4. Підбір прав користувачів.

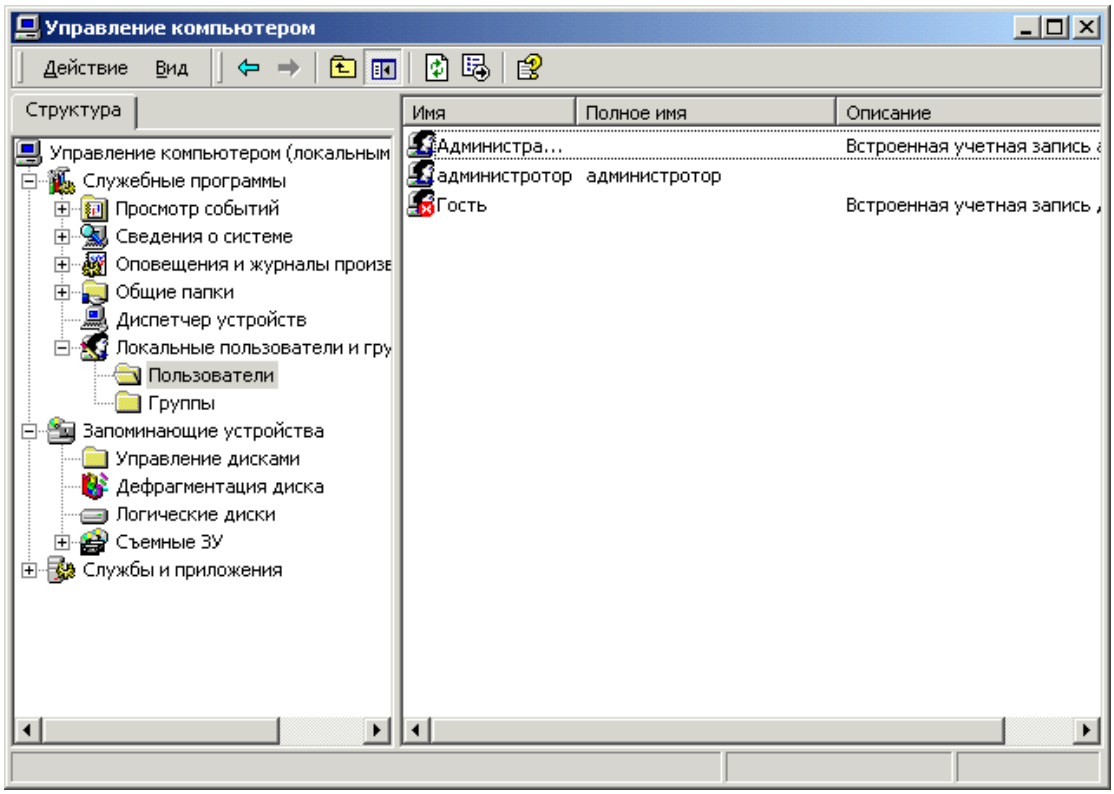


Рис.5. Підбір параметрів безпеки.

2. Хід роботи:

1. Установіть загальний доступ на один із файлів та каталог на диску “D”.
2. Установіть загальний доступ на диск “C”.
3. Відмініть загальний доступ на диск “C”.
4. Відмініть загальний доступ на один із файлів та каталог на диску “D”.
5. Установіть загальний доступ на принтер.
6. Відмініть загальний доступ на принтер.
7. Змініть мережений пароль адміністратора.
8. Змініть мережений пароль користувача.
9. Поверніть мережений пароль адміністратора.
10. Змініть назву комп'ютера в мережі.
11. Покажіть можливості розширення прав користувача.
12. Покажіть можливості розширення прав гостя.
13. Покажіть можливості використання інспектора для контролю за використанням загальних ресурсів

3. Контрольні питання:

1. Послідовність налагодження роботи комп'ютера в мережі.
2. Як провадиться пошук комп'ютера в мережі?
3. Як провадиться пошук принтера в мережі?
4. Послідовність надання доступу до файлу або каталогу в мережі.
5. Послідовність заборони доступу до файлу або каталогу в мережі.

6. Послідовність надання доступу до принтера в мережі.
7. Послідовність заборони доступу до принтера в мережі.
8. Послідовність зміни мереженого паролю.
9. Послідовність вказівки імені комп'ютера і робочої групи.
10. Послідовність призначення прав адміністратора.
11. Послідовність призначення прав користувача.
12. Послідовність призначення прав гостя.
13. Використання інспектора для контролю за використанням загальних ресурсів.
14. Послідовність обмеження доступу до файлу або каталогу груп користувачів.
15. Політика відкритого ключа.
16. Політика безпеки IP.

Лабораторна робота № 3 Одержання інформації про процеси, що відбуваються в системі Windows XP

Зміст

1. Теорія

1.1. Аудит подій. Налагодження аудита подій

Практично всі події системи, що відбивають процеси, відбуваються на рівні ядра ОС й представляють інтерес для користувача будь-якого рівня, можуть бути визначені й збережені у файлі завдяки спеціальному механізму *Windows XP*, який називається *аудитом системи*. Перегляд збережених подій здійснюється спеціальною програмою *Перегляд подій*.

Цей механізм є дуже гнучким у налагодженні й дозволяє вести аудит різних подій, що відбуваються в системі, як за їхнім класом приналежності, так і по тому, вдало або невдало була завершена подія. Наприклад, можна змусити систему контролювати всі успішні спроби користувачів і додатків одержання доступу до реєстру. Або можна контролювати всі спроби входу користувачів у систему, які закінчилися невдало.

Налагодження аудита локальної системи проводиться у програмі *Локальна політика безпеки* (*Local Security Settings*):

Пуск\Усі програми\Панель керування\Адміністрування\ Локальна політика безпеки

Для налагодження аудита подій необхідно:
запустити програму *Локальна політика безпеки*;
- вибрати пункт *Локальні політики* (рис.1);
- вибирати пункт *Політика аудита*;
- з'являться налагодження політики аудита (рис. 2).

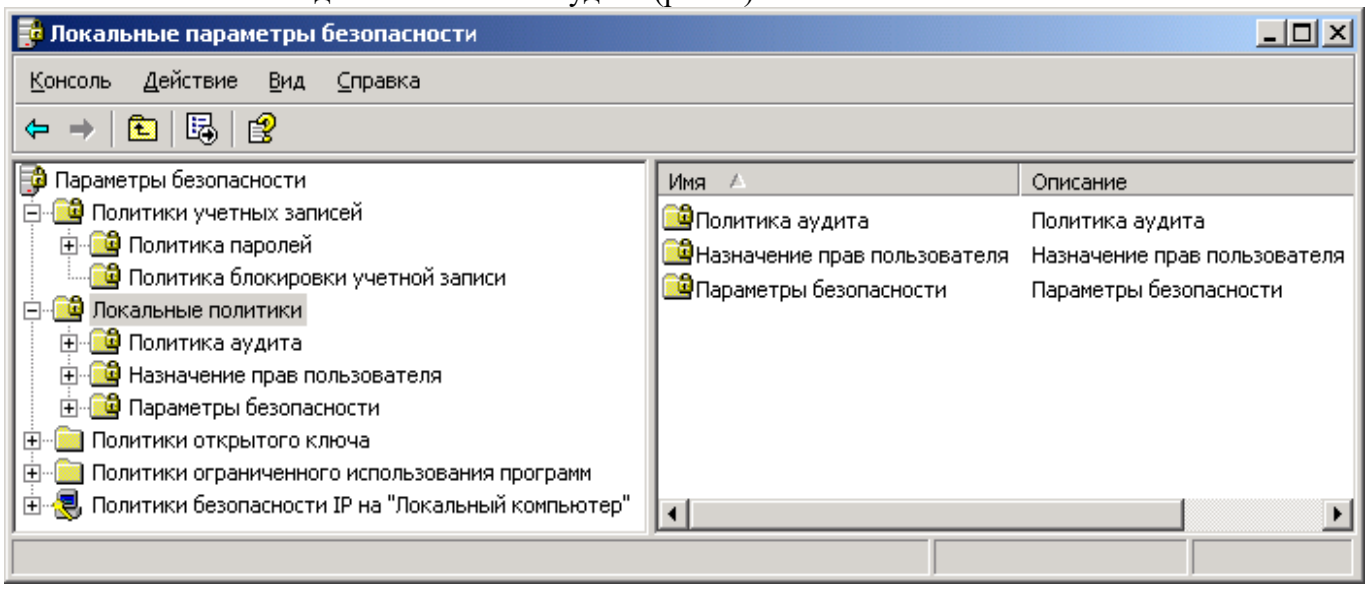


Рис 1 Вікно програми *Локальні параметри безпеки*

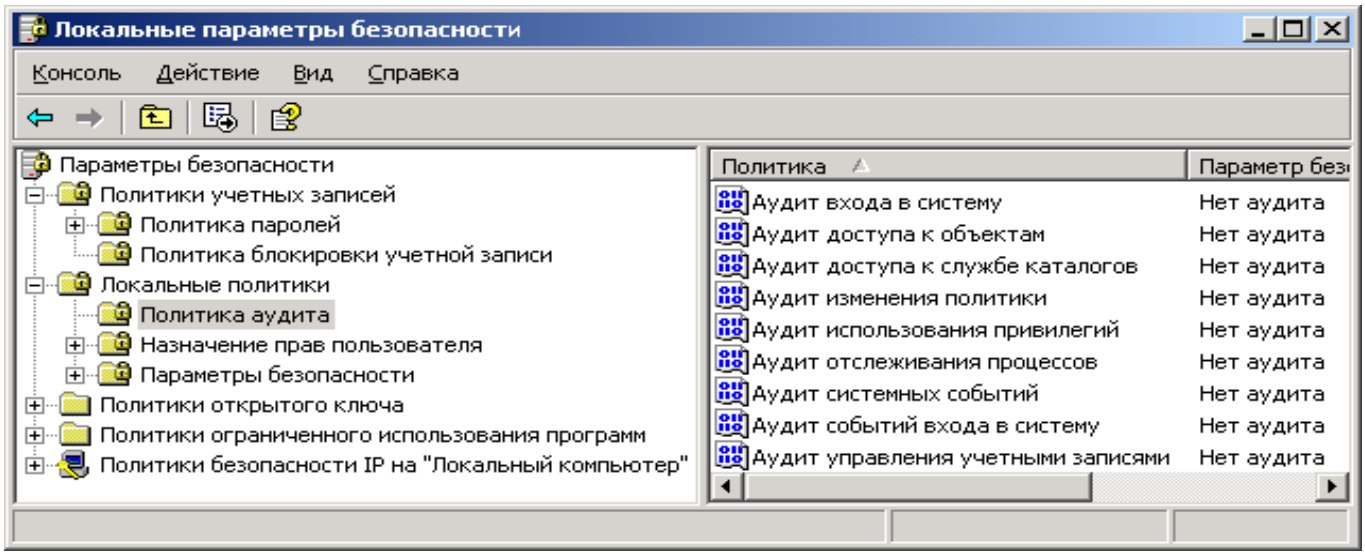


Рис 2 Вікно налагодження аудита

Налагодження аудита подій являють собою список контрольованих подій, а також ознака того, коли буде здійснюватися запис цієї події: при його успішному результаті, відмові або в обох випадках. Факт успішності завершення події визначається за його кодом завершення, що існує усередині системи. Для визначення того, коли буде відбуватися запис тої або іншої події, відповідним рядком списку політики аудита, необхідно по ній зробити подвійне клацання мишею, після чого на екрані з'явиться вікно налагодження політики аудита (рис. 3).

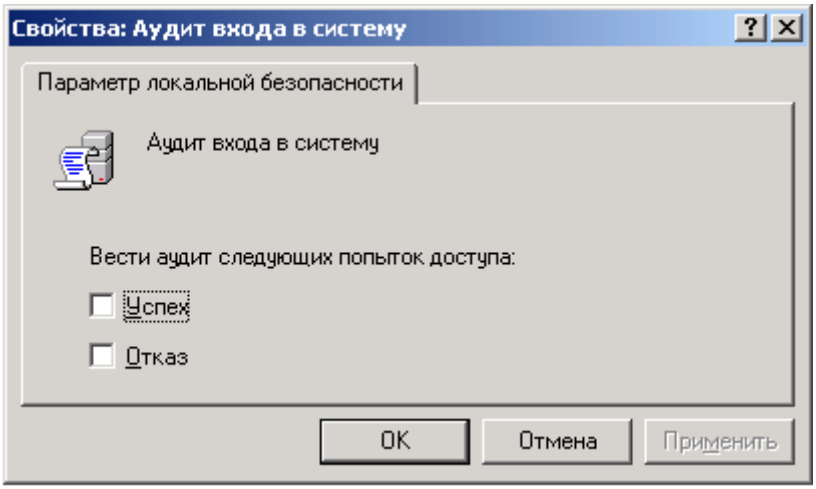


Рис. 3 Діалогове вікно введення значень опцій, які визначають, коли буде проводитися аудит певного події

Дане вікно дозволяє користувачеві вибрати вид аудита події для перегляду: при успішнім завершенні події, у випадку його збою або в кожному разі, налагодження досягаються установкою прапорця у відповідних режимах: *Успіх*, *Відмова* або в обох режимах. Кожна з політик аудита має свої характерні риси:

1.Політика аудита *Аудит подій входу в систему* відповідальна за запис подій, які генеруються операційною системою при вході й виході користувачів на інших мережевих комп'ютерах, за умови, що даний комп'ютер використовується для перевірки дійсності

обліковому запису. При установці опції *Успіх*, буде проводитися запис подій, у результаті яких користувачі успішно ввійшли в систему, у випадку установки опції *Відмова*, буде проводитися запис подій, у результаті яких користувачі не змогли ввійти в систему. У випадку установки обох опцій буде проводитися запис усіх спроб входу користувачів у систему, як удалих, так і невдалих.

У більших системах використовується повне протоколювання входу користувачів у систему, яке досягається установкою обох опцій. Для невеликих організацій і домашніх систем досить вести протоколювання входу користувачів тільки за критерієм *Відмова*, щоб завжди можна було виявити випадки підбору паролів або спроби вторгнення зломщиків, які не увінчалися успіхом, і вжити відповідних заходів. Так само буде отримана інформація про можливе джерело проблем і користувачів, які постійно забувають свій пароль, і, імовірно, намагаються його десь записувати.

2.Політика аудита *Аудит керування обліковими записами* відповідальна за запис подій, що виникають при роботі з обліковими записами користувачів: створення, зміна або видалення групи користувачів; перейменування облікового запису користувача, її вимикання, включення; установка йди зміна пароля. У всіх випадках системою, відповідно до встановлених опцій *Успіх* і *Відмова* буде проводитися запис подій. Рекомендується поставити політику на запис події у випадку невдалого завершення операції доступу до об'єктів цієї служби, що охоронить від можливих атак, які можуть проводитися в мережевих структурах.

3.Політика аудита *Аудит доступу до служби каталогів* відповідальна за протоколювання доступу до об'єктів служби *Active Directory*, яка являє собою, спеціальну мережеву файлову систему, елементами якої можуть бути не тільки файли й папки. Рекомендується її поставити на запис події у випадку невдалого завершення операції доступу до об'єктів цієї служби, що охоронить від можливих атак, які можуть проводитися в мережевих структурах.

4.Політика аудита *Аудит входу в систему* відповідальна за запис подій, які генеруються операційною системою при вході й виході користувачів на даному комп'ютері. При установці опції *Успіх* буде проводитися запис подій, у результаті яких користувачі успішно ввійшли в систему. У випадку установки опції *Відмова* буде проводитися запис подій, у результаті яких користувачі за якимись причинами не змогли ввійти в систему. У випадку установки обох опцій будуть робитися записи усіх спроб входу користувачів.

5.Політики аудита *Аудит доступу до об'єктів* і *Аудит зміни політики* відповідальні, відповідно, за аудита доступу до різних об'єктів системи, які контролюються за допомогою прав доступу, і за аудит робіт із правами користувачів і політики аудита. У більшості випадків досить буде робити аудит за відмовою для цих двох подій. Дані записи можуть робитися у випадку, якщо в системі буде відбуватися щось дивне й необхідно з'ясувати причини виниклих ситуацій.

6.Політика аудита *Аудит використань привілеїв* робить запис подій, у випадку використання користувачами специфічних системних привілеїв. Рекомендується встановити її на запис подій у випадку відмови для їхнього одержання користувачам. Дана інформація може допомогти фахівцям з комп'ютерної безпеки в з'ясуванні того, що відбулося із системою.

7.Політика аудита *Аудит відстеження процесів* дозволяє вести аудит за такими подіями процесу, як запуск програми, вихід з неї, а також іншими важливими системними подіям. Установка аудита даних подій за відмовою може допомогти зрозуміти, що відбувається в системі й, можливо, де їй потрібна допомога.

8.Політика аудита *Аудит системних подій* дозволяє проводити аудит таких системних подій як перезавантаження або вимикання комп'ютера, а також інших важливих повідомлень, що стосуються безпеки системи. Рекомендується завжди встановлювати дану політику аудита, як мінімум, на запис події, у випадку його відмови.

Особливості аудита системи:

1.Чим більше подій у різних ситуаціях протоколюється, тим більше повідомлень аудита системи буде отримано, отже, тим більше інформації буде про процеси, що відбуваються усередині системи, що ініціюються користувачами або різним програмним забезпеченням.

2. Чим більше повідомлень системи буде отримано, тем повільніше буде працювати система й можливо занадто швидке переповнення журналу безпеки операційної системи. У результаті чого прийдеться досить часто робити його очищення в програмі *Перегляд подій*.

1.2. Перегляд подій

Програма *Перегляд подій* (*Event Viewer*) представляє спеціальну системну програму, що входить до складу *Windows XP*, яка дозволяє бачити всі повідомлення, записані в журнал різними додатками й самою ОС. Програма *Event Viewer* (рис. 4) перебуває:

Пуск\Панель керування\Адміністрування\Перегляд подій

У данім вікні втримується три пункти: *Додаток, Безпека, Система* (*Application, Security, System*), інакше їх називають відповідно, *журналом додатків, журналом безпеки* й *журналом системи*. Інформація, що втримується в них, є повідомленнями, записаними додатками системної безпеки ОС і системними компонентами *Windows XP*. Передбачається, що інформація, що втримується в цих розділах важлива для користувача, і він повинен періодично з нею знайомитися.

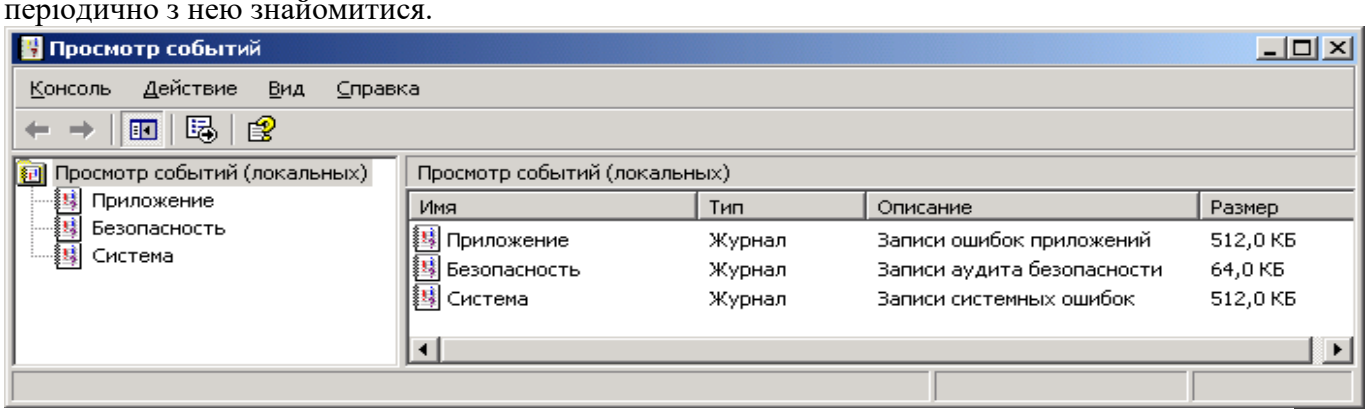


Рис. 1.Стартове вікно програми *Перегляд подій*

Типи подій, що прокотолюються системою у журналах:

- *помилка* – дане повідомлення повідомляє про помилку, таку як можлива втрата даних або порушення функціонування програмного забезпечення, наприклад, неможливість старту одного із системних сервісів або помилка при завершенні додатка;

- *попередження* – повідомлення не обов'язкове є чимось важливим, але може говорити про помилку, яка може виникнути згодом, наприклад, небажання якої-небудь програми або сервісу під час вимикання машини коректно завершуватися;

- *повідомлення* – повідомлення, що описувана подія успішна завершилося в додатку, драйвері або сервісі, наприклад, успішний старт якого-небудь системного сервісу або його зупинка;

- *аудит успіхів* – повідомлення про те, що контрольована подія в політиці аудита й системою безпеки успішно завершилося, наприклад, був зроблений коректний вхід одного з користувачів у систему;

- *аудит відмов* – клас подій, який буде повідомляти про те, що контрольована в політиці

аудита й системою безпеки подія завершилася з помилкою, наприклад, повідомлення, яке генерується при помилці доступу до якого-небудь об'єкта системи, або повідомлення при реєстрації користувача, якщо він помилився паролем.

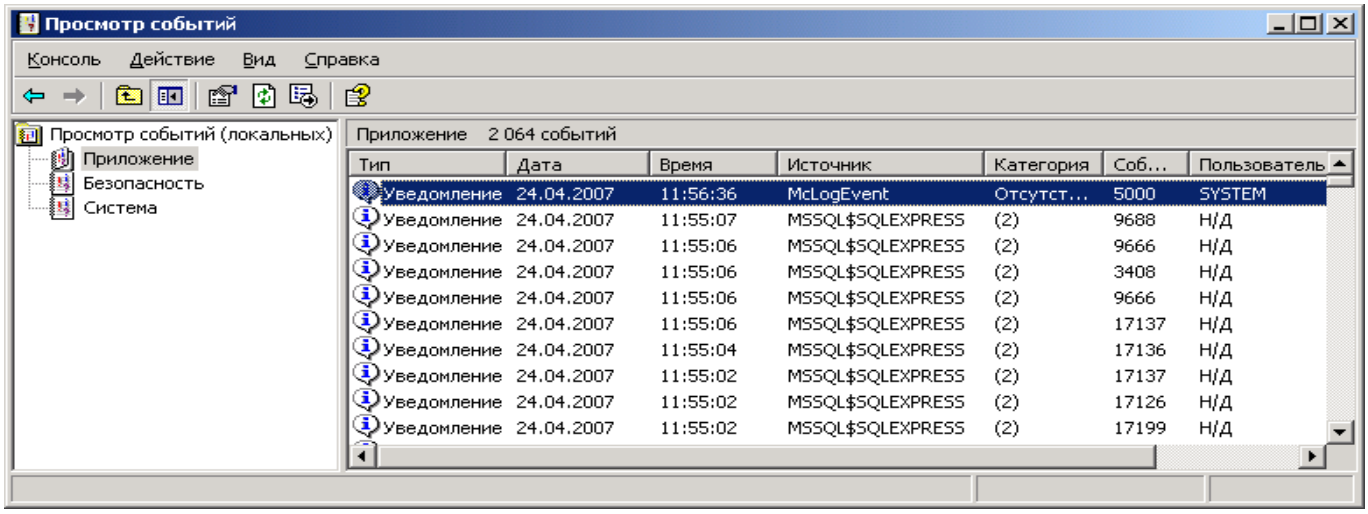


Рис . 5 Уміст вкладка *Додаток* програми *Перегляд подій*

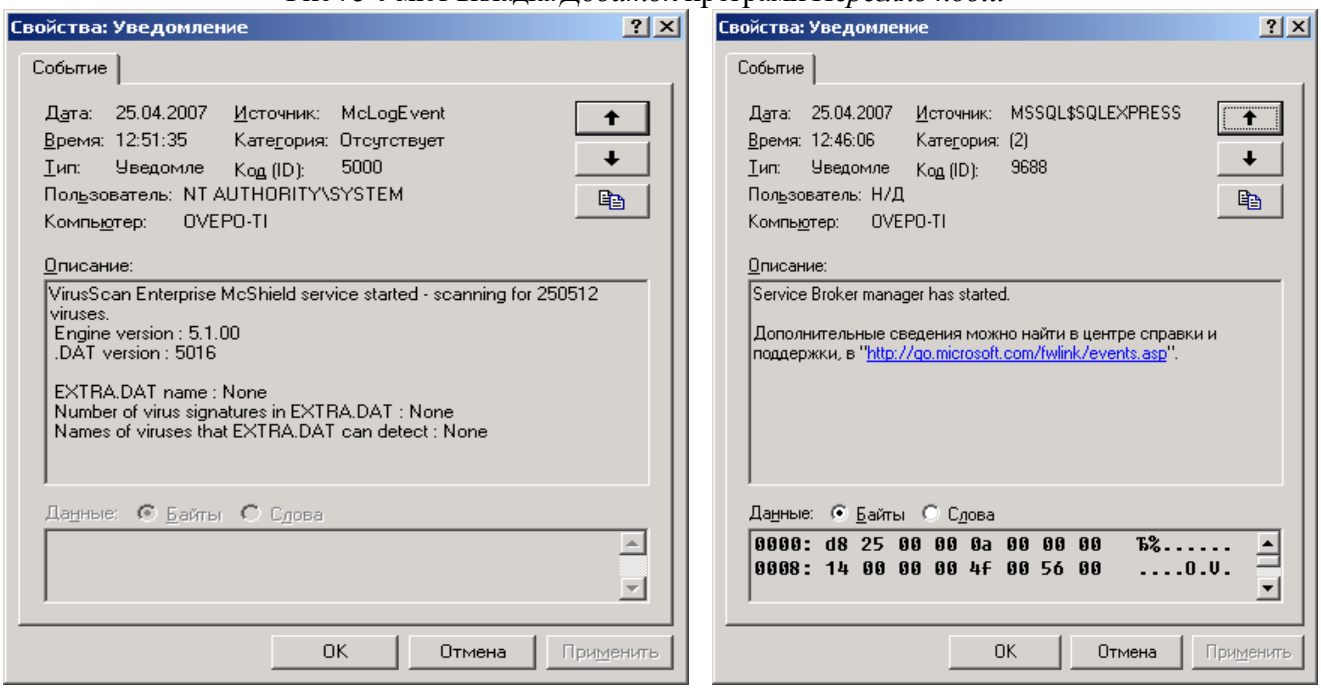


Рис. 6 Типове повідомлення, що втримується в системі

За запис повідомлень у системі відповідальний сервіс *Event Log*, який стартує при завантаженні *Windows XP*. Вхід у розділ *Security* мають тільки користувачі, що входять до складу групи локальних адміністраторів. За замовчуванням у цей розділ система не пише ніяких повідомлень. Для активації запису повідомлень необхідно встановити необхідну політику аудита системи (п.1.1.).

Для перегляду властивостей конкретного повідомлення слід зробити клацання правою кнопкою миші на події. У контекстному меню, що з'явився, вибрати *команду* **Властивості**. З'явиться вікно *Властивості: Повідомлення*. У верхній частині вікна (рис.6) утримується

типова інформація. У середній і нижній його частині втримується інформація, різна для кожного з повідомлень. Інформаційні поля в описі події *Even* (формат протоколюємих подій):

- *дата* – поле визначає дату, коли дана подія відбулася;
- *час* – поле визначає локальний час, коли ця подія настала;
- *користувач* – поле визначає користувача, від імені якого відбулася подія (опис користувача поміщений в *Event Log*); поле може містити ім'я клієнта, що викликав подію, при обробці його запиту в програмі-сервері, «*N/A*» визначає приналежність даного події до операційної системи.
- *комп'ютер* – поле містить ім'я комп'ютера, на якім відбулася дана подія;
- *код (ID)* – поле містить ідентифікатор події, який разом з полем *Джерело* використовуються для аналізу ситуації розроблювачами програмного забезпечення, що викликав даний запис; при зверненні до служби підтримки на їхню вимогу потрібно повідомити ці значення полів;
- *джерело* – поле містить ім'я програмного забезпечення, драйвера або компонента системи, що викликали запис події; цей ідентифікатор, а також поле *Event ID* використовуються для аналізу ситуації розроблювачами програмного забезпечення;
- *тип* – поле містить один з п'яти типів повідомлень, яким воно є;
- *категорія* – поле класифікує подію в програмнім забезпеченні, яке його викликало; дана інформація найбільше часто використовується системою безпеки як ідентифікатор того, який саме тип контрольованої події в політику аудита був при записі внесений.
- *опис* – поле використовується для виводу додаткової інформації, яка допоможе краще зрозуміти природу що відбувся в системі події.

У процесі запуску, роботи й вимикання системи накопичується велика кількість подій, на вивчення й перегляд яких потрібно багато часу. Тому свою увагу слід сконцентрувати на подіях, що мають тип: *Помилка*, *Попередження*, *Аудит відмов*. Перші два типи звичайно з'являються в розділах *System* і *Application* і повідомляють про те, на що слід звернути увагу в роботі системи й додатка, наприклад, проблеми в роботі жорстких дисків, системних програм або самої операційної системи. Слід уважно ставитися до таких повідомлень, якщо їх пропускати, то може трапитися, що в майбутньому система перестане коректно функціонувати, а дані можуть виявитися загубленими, якщо не проводилося їхнє регулярне резервування.

Повідомлення системи безпеки *Аудит відмов* можуть бути пов'язані з тим, що на систему здійснювалася яка-небудь атака ззовні або хтось із користувачів забув свій пароль. Часта поява таких повідомлень може означати, що хтось підбирає пароль до певних облікових записів системи. У даних випадках слід бути особливо уважними, тому що таких записів в *Event Log* буває не багато.

При переповненні розділів системи необхідно:

- увійти в систему під правами системного адміністратора;
- завантажити програму *Перегляд подій* (*Event Viewer*);
- вибрати розділ;
- розкрити пункт операційного меню *Дії* або зробити клацання правою кнопкою миші на розділі і в контекстному меню вибрати пункт *Стерти всі події* (рис.7);
- на екрані з'явиться діалогове вікно, у якім буде запропоновано зберегти події, які будуть вилучені, в окремому файлі, (рис.8).

Рекомендується мати історію зроблених подій, що може допомогти при вирішенні виниклих проблем, тому що при збереженні подій завжди можна простежити їх початок і

прийняти відповідний розв'язок. Тому слід нажати кнопку *Так* (рис. 8) і вибрати місце й ім'я для файлу, що зберігається.

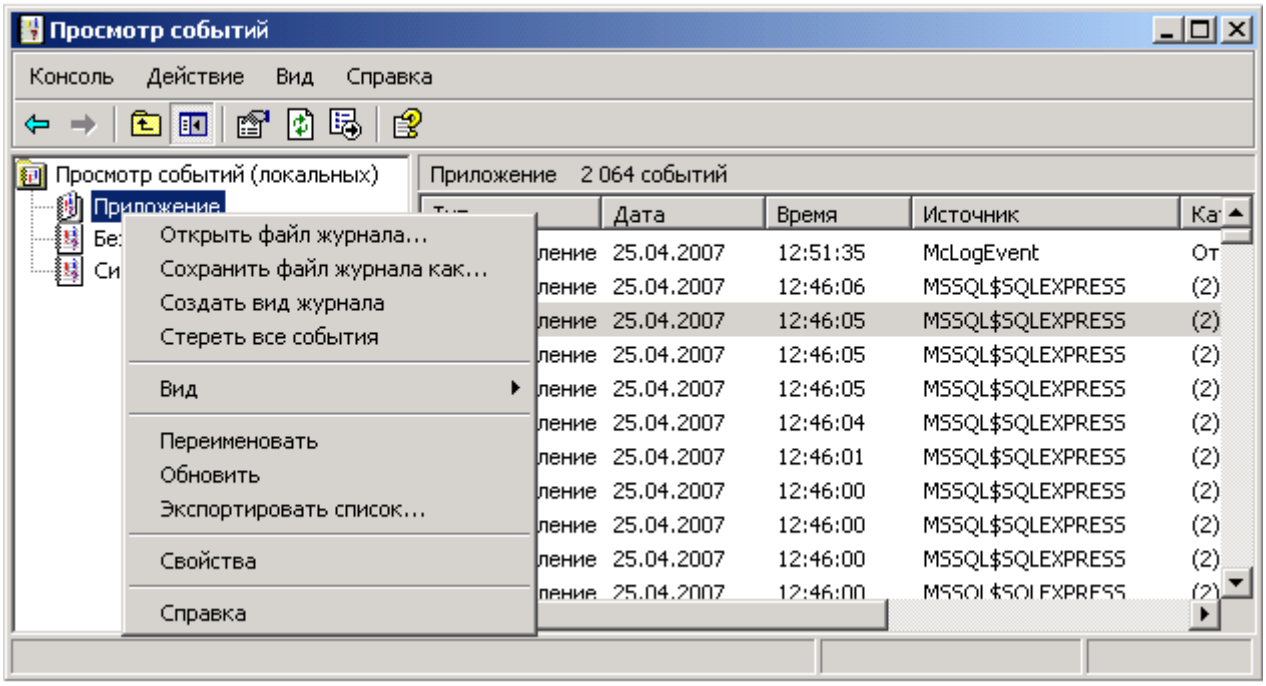


Рис. 7 Меню для очищення обраного розділу системи

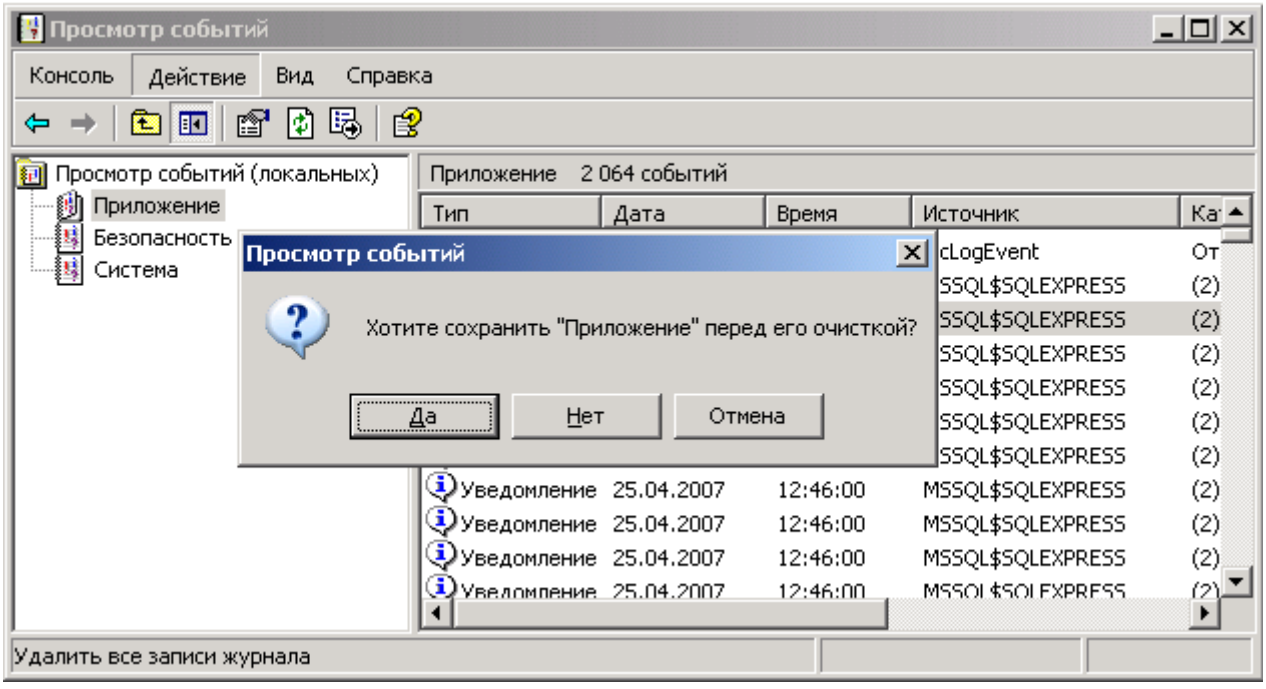


Рис. 8 Пропозиція системи про збереження подій, що стираються

Якщо згодом прийдеться переглянути збережені події, то необхідно в програмі *Перегляд подій* розкрити пункт операційного меню *Дії* й вибрати команду *Відкрити файл журналу* (рис. 7), події, що перебувають у файлі, відобразяться на екрані. Для виконання операцій

очищення розділів *Events Log*, а також збереження й завантаження файлів, що містять повідомлення із цих розділів, потрібні права системного адміністратора.

1.3. Диспетчер завдань і внутрішні параметри системи

Диспетчер завдань є вбудованим в операційну систему додатком, який дозволяє переглядати й аналізувати працюючі в цей момент у системі додатки й процеси, а також робити керування ними, незалежно від того, у якому стані вони перебувають (рис. 9). *Диспетчер завдань* дозволяє:

- аналізувати поточні параметри продуктивності операційної системи й параметри, які були в її недавньому минулому, що дозволяє найбільш зручно й вірогідно набудовувати продуктивність системи відповідно до пропонованих вимог;
- відображає стан мережевих з'єднань і ступінь їх завантаженості, що дозволить проводити наочний моніторинг мережевих з'єднань, якщо вони присутні в системі, також можна виявити програми, які таємно пересилають інформацію з комп'ютера в мережу.
- показує інформацію про користувачів (якщо в системі включена опція швидкого перемикання користувачів), що працюють із системою в цей момент часу: ім'я користувача, його обліковий запис, ідентифікатор входу, статус, ім'я комп'ютера, з якого прийшов користувач (якщо він використовував віддалений вхід);
- дозволяє проводити деякі операції над користувачами;
- може допомогти запустити додаток;
- може перейти в якесь певне вікно додатка;
- може здійснити вихід із системи.

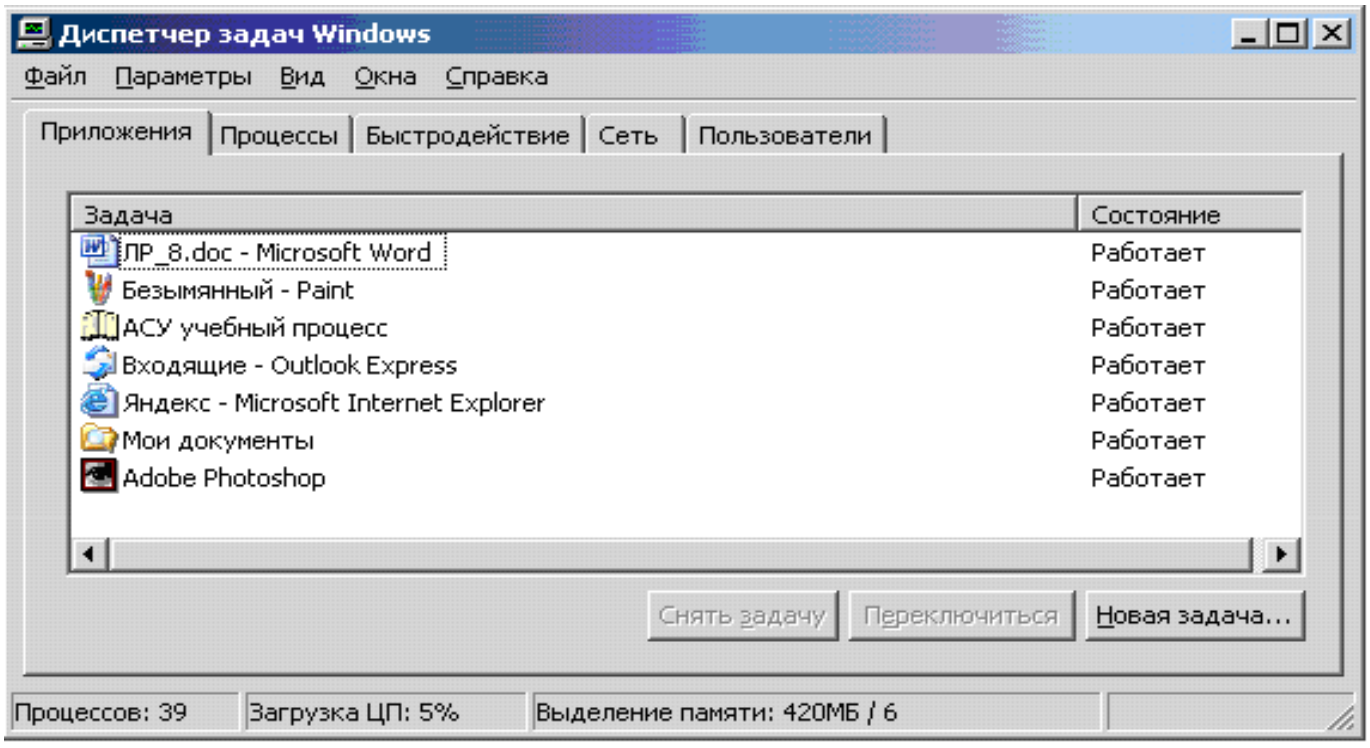


Рис. 9 Вікно *Диспетчера завдань*

Основні команди пунктів операційного меню *Диспетчера завдань*.

Меню *Файл* команда *Нове завдання* (*Виконати*) запускає новий додаток.

Меню *Вид* містить команди, відповідальні за вивід на екран різної інформації, відображуваної у вікні *Диспетчера завдань* і команди відповідальні за частоту відновлення інформації, відображуваної додатком (рис. 10). Якщо *Диспетчер завдань* буде постійно обновлювати інформацію у всіх своїх вікнах, прикріплених до відповідних закладок, то на це витратиться багато часу роботи центрального процесора й продуктивність системи понизиться. Щоб цього не трапилося, розроблювачі пішли на компроміс, і тепер інформація у вікнах даної програми обновлюється через певні проміжки часу. Таким чином, будь-яка інформація, відображувана у вікні *Диспетчера завдань*, є, фактично, завжди на момент відновлення інформації у вікні, а зараз уже стала історією. Але оскільки інтервали відновлення інформації у вікні досить малі, то можна з великою ймовірністю вважати, що дана інформація відображає поточний стан системи.

Команда *Обновити* (рис. 10) призначена для відновлення всіх вікон диспетчера завдань, з метою показу поточного стану системи.

Команда *Швидкість відновлення* (рис. 10) дозволяє встановити, як відносно часто буде обновлятися інформація у всіх вікнах *Диспетчера завдань*, для цього встановлені наступні режими:

- режим *Висока* – призначений для максимально швидкого відновлення інформації;
- режим *Звичайна* – призначений для відновлення інформації зі швидкістю, яка вважається достатньою розроблювачами ОС (використовується за замовчуванням);
- режим *Низька* – призначений для рідкого відновлення інформації;
- режим *Призупинити* – призначений для заборони відновлення інформації; означає паузу, яку варто вибирати, коли потрібно обміркувати значення параметрів, отриманих від системи (фактично буде зберігатися інформаційний зліпок системи, який існував на момент зупинки збору інформації).

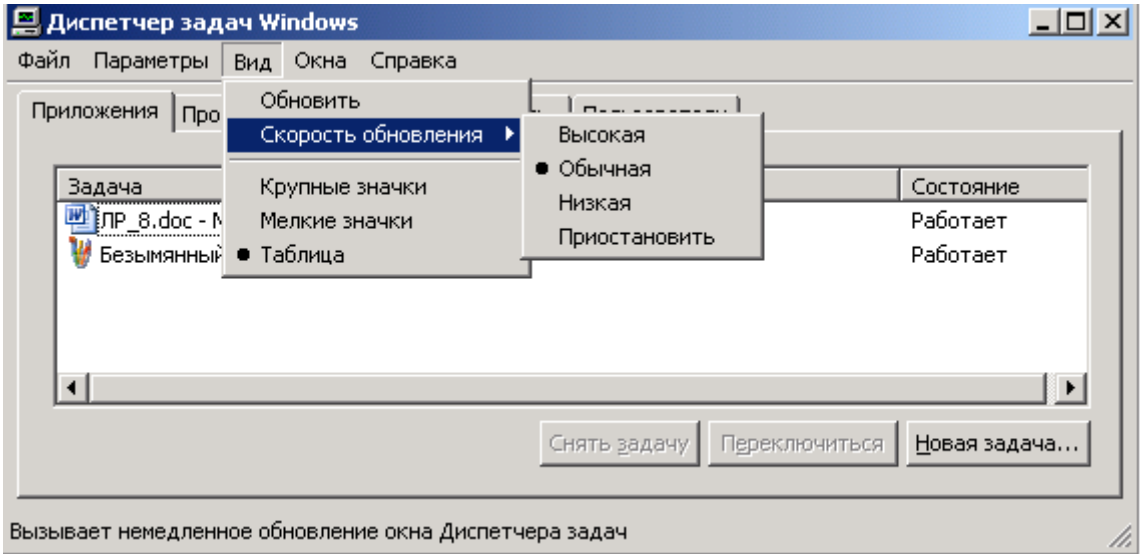


Рис. 10 Меню Вид *Диспетчера завдань*

3.Команда *Завершення роботи* дозволяє перевести комп'ютер в режим що чекає або сплячий режими, виключити або запустити знову його, завершити сеанс поточного користувача або перемкнутися на іншого користувача системи. У режимі, що чекає, усі запущені програми залишаються в оперативній пам'яті, подача енергії до якої зберігається. У випадку сплячого режиму всі програми записуються на жорсткий диск і система повністю знеструмлюється. Режим енергозбереження й гібернації (*лат. hibernatio* – спячка) буде коректно працювати тільки тоді, коли встаткування й програмне забезпечення підтримують його й налагоджені відповідним чином. При

виборі пункту меню, яке перезапускає або виключає комп'ютер усі користувачі, що працюють у системі, будуть відключені й усі працюючі програми зупинені.

Диспетчер завдань містить наступні закладки: *Додатка*, *Процеси*, *Швидкодія*, *Користувачі*.

1.3.1. Закладка Додатки

Закладка *Додатка* відображає в системі всі працюючі в цей момент додатки (рис. 9). Унизу вікна під списком активних додатків перебувають кнопки, що дозволяють завершити додатки, перемкнутися на додаток і запустити новий додаток. Кнопка *Зняти завдання* завершить будь-який додаток. Якщо додаток не відповідає на запити системи, коли вона намагається його закрити, то *Windows* запитає, чи дійсно користувач прагне його завершити, тому що є ризик втрати незбереженої інформації. Натискання кнопки *Завершити зараз*, розташованої в цьому вікні, аварійно завершить додаток. При аварійнім закритті додатків усі незбережені в них дані можуть бути безповоротно загублені.

Якщо часто доводиться мати справу із завислими завданнями, послідовне натискання на кнопку *Завершити зараз* у вікнах, що відкриваються системою, з питаннями про завершення обраного додатка є досить стомлюючою справою. Для запобігання даної процедури можна відредагувати значення ключа *Hungapptimeout* у реєстрі за адресою:

HKEY_CURRENT_USER\Control Panel\ Desktop

Ключ визначає час у мілісекундах, через яке *Windows* буде вважати додаток завислим. За замовчуванням це значення рівне 5000 (п'ять секунд). Якщо через цей інтервал часу додаток не буде реагувати на запити системи, він буде вважатися завислим. У цих же галузях реєстру втримується ключ *Waittokillapplicatioiitimeout,* який задає час перед закриттям завислого додатка. За замовчуванням це значення рівне 20000 (двадцять секунд). У підсумку, після того як система протягом п'яти секунд переконається, що додаток завис, вона буде чекати на нього завершення протягом ще двадцяти секунд. Разом, сумарний час очікування системи, перед закриттям завислого додатка рівно 25 секундам.

Для того щоб завислі додатки закривалися автоматично, у тій же вітці реєстру є ключ *Autoend-tasks*. При установці його значення рівне одиниці, система автоматично буде знищувати завислі додатки. Однак занадто малі значення змін, що визначають очікування системи, можуть привести до того, що нормально працюючі, але довго думаючі процеси будуть уважатися системою повислими й можуть бути закриті, що приведе до нестабільної роботи системи. Автоматичне знищення завислих процесів може виявитися корисною функцією. Якщо в системі існує більше завантаження додатками й сервісами, то завжди є достатня ймовірність появи завислих з якихось причин програм, які витрачають системні ресурси, включаючи найбільш важливі з них: системну пам'ять і час робота процесора, то їх закриття може бути життєво важливим для успішного продовження функціонування системи.

Клавіша *Перемкнутися* (рис. 9.) призначена для перемикання на обраний додаток у списку додатків. Після натискання цієї кнопки він з'явиться на екрані поверх усіх інших додатків.

1.3.2. Закладка Процеси

Будь-який додаток є процес, але не будь-який процес є додаток. Кількість процесів і додатків у системі може сильно відрізнятися. У закладці *Процеси* (рис. 11) під списком процесів перебуває опція *Відображати процеси всіх користувачів* у випадку включення якої, при наявності відповідних прав системного адміністратора, системою будуть відображатися всі процеси, які запущені всіма користувачами системи в цей момент часу. За допомогою кнопки *Завершити процес,* можна знищити обраний. В інформаційному рядку виводиться загальна кількість процесів завантаження, процесора, а також пам'яті, виділена процесам і операційній системі, і її сумарна ємність, включаючи файл підкачування.

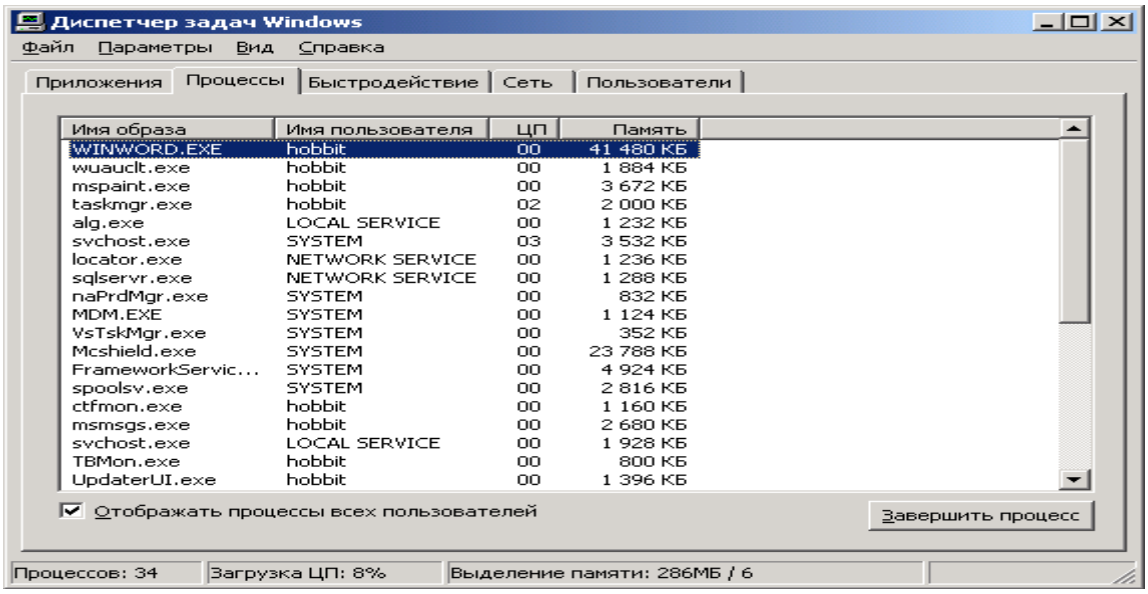


Рис. 11 Закладка *Процеси*

За замовчуванням для кожного процесу *Диспетчер завдань* показує ім'я файлу, що виконується, на основі якого був створений процес, або функцію процесу, якщо він належить системі й не перебуває в окремому файлі, що виконується, з якого міг би бути запущений. Після імені образа, файлу що виконується випливає ім'я користувача, під яким був запущений кожний конкретний процес. Якщо ж процес належить системі, то в цьому полі може втримуватися інформація про те, до якого типу сервісу системи він відноситься. Якщо ж процес є частиною системи, то про це буде сказано словом *SYSTEM*.

У поле *Завантаження ЦП* відображається інформація про завантаженість процесом центрального мікропроцесора системи. У випадку якщо в системі немає процесів потребуючих виконання, то буде виконуватися спеціальний процес, називаний «Бездіяльність системи», що належить ОС, про що говорить рядок *SYSTEM*. Наступне інформаційне поле відображає кількість пам'яті, споживаної процесом.

Дані характеристики процесів, наведені в *Диспетчерові завдань* за замовчуванням, є найважливішими. Імена образів, що виконуються, дозволять у будь-який момент часу контролювати процеси, що виконуються. Незважаючи на те, що існують методи приховання імені процесу, що виконується, від показу *в Диспетчерові* завдань, більшість процесів у ньому відображаються. Тому завжди можна переконатися в тому, що в системі виконуються тільки ті процеси, які повинні виконуватися відповідно до поставлених вимог.

Поле *Ім'я користувача* дозволить визначити від облікового запису якого користувача запущений відповідний процес, що зручно для з'ясування його механізму запуску. Якщо процес запущений під правами якого-небудь користувача, то за його запуск відповідальний прямо або побічно цей користувач. Якщо процес працює від імені системи або адміністратора, якщо це вірус або шпигунська програма, вона вже досить глибоко проникнула в систему і її автозапуск потрібно шукати під обліковим записом адміністратора системи в автозапуску або серед програм або у відповідних місцях у реєстрі, відповідальних за автозапуск програм.

Рівень використання мікропроцесора процесом визначає те, як багато він «думає». Якщо процес практично не споживає процесорного часу, то він, імовірно, перебуває в стані *очікування*. Якщо процес вантажить процесор роботою, то він перебуває в стані *виконання* або, можливо, завис.

Кількість споживаної оперативної пам'яті визначає ступінь її використання процесом. Якщо процес споживає занадто багато пам'яті під свої потреби, наприклад, до половини всієї доступної пам'яті, то це може негативно позначитися на працездатності системи й привести до її перезавантаження або зупинки. Також існують атаки зломщиків, засновані на споживанні всієї доступної оперативної пам'яті системи з метою її зупинки або порушення нормального функціонування. Тому якщо в системі дивно поводиться процес, який не був запущений користувачами системи, то слід його досліджувати, попередньо знайшовши, що виконується образ цього процесу.

Поряд з відображуваними за замовчуванням параметрами процесу (рис. 11.) *Диспетчер завдань* може на вимогу користувача показувати й інші параметри, що задаються в пункті меню *Вид* режимом *Вибрати стовпці*. При виборі цього режиму з'явиться вікно *Вибір стовпців* (рис. 12.).

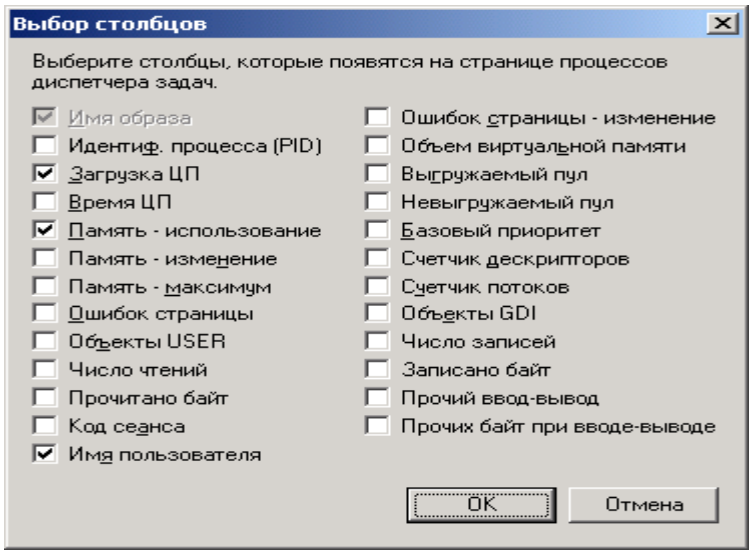


Рис. 12 Вікно пункту меню *Вид* режиму *Вибрати стовпці*

Крім параметрів *Завантаження ЦП*, *Ім'я користувача* й *Пам'ять* (використовуваних за замовчуванням) цікаві параметри *Ідентиф. процесу* (*PID*), *Час ЦП*, *Обсяг віртуальної пам'яті*, *Базовий пріоритет*, *Лічильник дескрипторів* і *Лічильник потоків*. Дані параметри викликають відображення в *Диспетчерові завдань*, відповідно, ідентифікатора процесу (*PID, Process ID*), часу роботи на центральному процесорі, розміру використовуваної віртуальної пам'яті, кількості використовуваних процесом дескрипторів, а також числа ниток у процесу. Після виходу з *Диспетчера завдань* усі його параметри налагодження будуть збережені й при його повторному виклику будуть враховані системою.

Опис параметрів.

1.Поле *Ідентифікатора процесу* (*PID, Process ID*) є найважливішим параметром, за яким можна знайти потрібний процес у системі й продовжити його дослідження іншими методами, наприклад, спеціальними налагоджувачами або зберігши на диску інтерактивними дизасемблерами.

2.Поле *Час ЦП* визначає ступінь використання процесом центрального процесора, чим вище його завантаженість, тем активніше працює відповідний додаток. Якщо ж завантаженість процесора додатком незначна або дорівнює нулю, то цей додаток більшу частину часу проводить у стані спокою. Дане поле подає інформацію про те, що відбувається усередині системи і які додатки проявляють ту або іншу активність.

Багато вірусів і троянські програми можуть проводити більшу частину часу свого життя, перебуваючи в стані очікування, мінімально використовуючи час роботи мікропроцесора. Якщо якийсь невідомий процес робить значну активність у системі, то це також є попереджувальним сигналом. Тому при необхідності завжди можна визначити коли, ким і як був запущений процес, що дасть можливість запобігти його повторному запуску.

3.Поле *Обсяг віртуальної пам'яті* визначає ступінь використання віртуальної пам'яті процесом. Більші запити до віртуальної пам'яті можу означати також і помилки в процесі або його націлювання на руйнування системи шляхом захвата всієї доступної віртуальної пам'яті.

4.Поле *Базовий пріоритет* визначає значення пріоритету, під яким запущений даний процес. Рівень пріоритету *Середній* має переважна більшість процесів користувача; деякі процеси, що вимагають більших обчислювальних ресурсів комп'ютера, можуть мати пріоритети *Вище за середнє* або *Високий*. Існують і інші значення пріоритетів процесів, але вони використовуються рідко.

Виключенням є процес *Idle.exe*, який не враховується системою як процес, що вимагає виконання й тому не має пріоритету. Він виконується лише у випадку, коли в теперішній момент часу в системі немає інших процесів, які необхідно було б виконувати на процесорі. У середньому процеси, що мають більший пріоритет, виконуються в операційній системі швидше, тому що їм для їхнього виконання операційною системою надається більше часу роботи мікропроцесора.

Велика кількість користувацьких процесів із пріоритетами вище ніж *Середній* можуть сильно гальмувати роботу системи, зробити її нестабільної, або привести до перезавантаження. Тому якщо невідомий процес має пріоритет вище пріоритету *Середній*, то слід визначити, що це за процес і звідки він узявся в системі.

5.Поле *Лічильник дескрипторів* визначає кількість використовуваних процесом дескрипторів – ідентифікаторів, які визначають використовувані процесом системні ресурси, наприклад, файли. Чим більше дескрипторів використовує процес, тем більшою активність він має.

Дана ситуація може служити непрямою інформацією про внутрішню діяльність процесу. Наприклад, якщо невідомий процес, що займає порівняно мало оперативної пам'яті й ресурсів центрального процесора, має число дескрипторів за тисячу, те це привід задуматися над тем, навіщо всі вони йому потрібні. Імовірно, що він намагається таємно аналізувати вміст файлів системи, заразити або зруйнувати їхній уміст. Існує й інший варіант: багато мережевих атак на систему ґрунтуються на побудові до неї надлишкової кількості запитів, які вона не може обслужити й, як наслідок, припиняє нормальне функціонування. Наявність великої кількості дескрипторів або постійне збільшення їх числа в процесу, вказує на користь такого припущення й вимагає негайного втручання. Якщо невідомий процес має дуже мало відкритих дескрипторів, то він так само є кандидатом на дослідження або знищення.

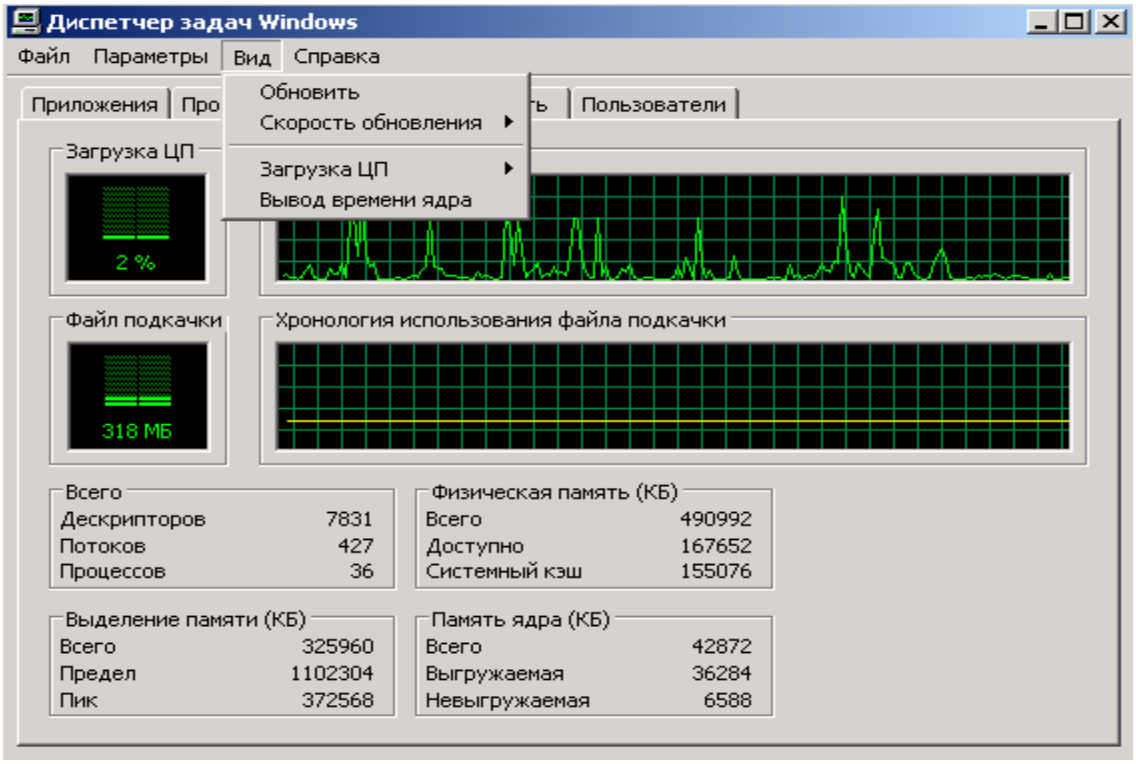
6.Поле *Лічильник потоків* визначає число ниток у процесу. *Нитками* називаються, процеси, які виконуються в рамках одного процесу, що є для них материнським. Багато процесів мають кілька ниток, це значно спрощує їхню розробку для програміста. Однак велика кількість потоків в одного процесу (більш сотні) є підозрілим і може вказувати на застосування проти системи атаки відмови в обслуговуванні (як у випадку із числом дескрипторів у процесу). В атаці відмови в обслуговуванні процес, який перевантажує систему запитами на ресурси, може бути звичайною програмою, але інша програма або зломщик віддалено по мережі роблять так, що вона починає усе більше й більше запитувати в системи обчислювальних ресурсів.

Єдиною можливістю запобігти таким атакам є періодичне відновлення версій використовуваного програмного забезпечення. З метою профілактики або пошуку причин виникнення таких атак слід періодично проводити перевірку працюючих процесів операційної системи за допомогою *Диспетчера завдань, Total Commandera* або інших засобів.

Рекомендується дотримувати наступного правила: якщо в *Диспетчерові завдань* перебуває невідомий процес і його поведінка є дивною, хоча б по одному з вище наведених параметрів, то, якщо немає інших ідей, слід його завершити за допомогою кнопки *Завершити процес* або повідомити про процес системного адміністратора.

1.3.3. Закладка Швидкодія

Закладка *Швидкодія* відображає параметри продуктивності системи (рис. 13).



Рис/ 13 Вкладка *Швидкодія*

На індикаторах *Завантаження ЦП* і *Хронологія завантаження ЦП* виводиться інформація, відповідно, про поточну завантаженість мікропроцесора й про його використання в минулому. В ідеалі, у випадку бездіяльності системи, завантаженість повинна бути в діапазоні від нуля до одного або двох відсотків. Це не виключає періодичні різкі підвищення навантаження на процесор, аж до ста відсотків, наприклад, у випадку операцій із зовнішніми пристроями (жорстким диском або принтером).

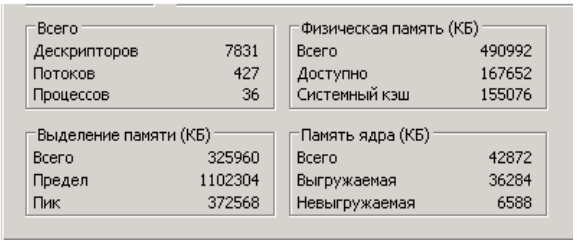
Якщо ж середнє завантаження системи становить більш п'яти відсотків, то це значить, що в ній постійно виконується якийсь процес, що має порівняно більше навантаження на систему. Для з'ясування цього процесу слід звернутися до закладки *Процеси* або до закладки *Мережа*, щоб переконатися в тому, що цей процес нічого не робить у локальній мережі або Інтернеті. Багато мережевих вірусів і хропаків мають тенденцію перебувати постійно в системі, виконуючи деяку внутрішню роботу, періодично працюючи з мережею. І якщо це так, постійне невелике завантаження системи й використання достатньо великої кількості пам'яті, а також мережний трафік будуть їх демаскувати.

Якщо в системі є більш одного мікропроцесора, то для кожного із цих процесорів на *Диспетчерові завдань* з'являться свої індикатори *Завантаження ЦП* і *Хронологія завантаження ЦП*.

За допомогою пункту меню *Вид \ Вивід часу ядра* (рис. 13) можна конкретизувати яка саме продуктивність відбивається на індикаторах *Диспетчера завдань*: сумарне завантаження системи або окрема інформація із завантаження мікропроцесора операційною системою й користувацькими програмами. Цей режим дозволяє одержати додаткову інформацію про те, де саме відбувається підвищене завантаження мікропроцесора.

Індикатори *Файл підкачування* й *Хронологія використання файлу підкачування* показують, відповідно використання, файлу підкачування і його використання системою в минулому. Це дуже важливий показник. Якщо файл підкачування використовується більше ніж на половину за умови, що не були запущені більші програми (текстові або графічні редактори, компілятори, плеєри та ін.), то це вірна ознака того, що в системі щось відбувається. Це може бути помилка в програмнім забезпеченні або атака типу відмови в обслуговуванні. Для з'ясувань причин, що відбувається слід звернутися до закладки *Процеси*, звернувши особливу увагу на те, як процеси використовують пам'ять. Також варто звернути увагу на закладку *Мережа*, щоб переконатися в тому, що процеси нічого не роблять у локальній мережі або Інтернеті.

Параметри системи *Всього* відображають загальне число дескрипторів (у рядку *Дескрипторів*), ниток (у рядку *Потоків*) і процесів (у рядку *Процесів*). Якщо кількість дескрипторів, потоків і процесів буде занадто великим, то можливо, що хтось проти системи використовує мережеву або локальну атаку відмови в обслуговуванні. Система може стати нестабільною або перестане функціонувати нормально, а вся інформація, що втримується в користувацьких програмах, буде загублена. Слід терміново знайти процес, який використовує велику кількість ресурсів і його закрити. Після чого зробити пошук локальної або віддаленої причини, що викликала дану атаку.



У групі параметрів продуктивності системи *Фізична пам'ять (КБ)* відбивається сумарний обсяг оперативної пам'яті (рядок *Усього*), доступної пам'яті (рядок *Доступно*) і обсяг пам'яті, зайнятому під кеш (рядок *Системний кеш*). Усі обсяги наведені в кілобайтах. Якщо виявлене, що в системі без запуску яких-небудь програм занадто мало доступної пам'яті (менше сотні мегабайт), то слід установити додаткову оперативну пам'ять або розібратися із процесами, які її споживають.

Група параметрів *Виділення пам'яті (КБ)* визначає використання пам'яті додатками в системі:

- рядок *Усього* описує поточне використання пам'яті;
- рядок *Межа* показує максимальну ємність пам'яті, яка може бути використана додатками (сума ємностей файлу підкачування й оперативної пам'яті);
- рядок *Пік* показує максимальний обсяг пам'яті, який використовувався додатками в системі.

Якщо значення *Пік* або *Всього* наближається до значення *Межа*, то за умови, що в системі не завантажені більші додатки, можливо відбувається локальна або віддалена атака.

Група параметрів *Пам'ять ядра (КБ)* показує обсяг пам'яті, використовуваної ядром операційної системи *Windows XP*:

- рядок *Усього* показує сумарний обсяг пам'яті, доступний ядру;
- рядок, Що *Вивантажується* показує розмір пам'яті, який може бути витиснутий у файл

підкачування спеціальними засобами ОС;

- рядок, Що *Не вивантажується* показує розмір пам'яті, яка використовується ядром системи, що не може бути витіснена в файл підкачки і знаходится постійно в оперативній.

Залежно від поточної ситуації в роботі операційної системи, ці значення можуть мінятися в ту або іншу сторону. Якщо ці значення міняються різко, наприклад, у два рази, то це ознака того, що в системі щось не так. Тому слід з'ясувати причину таких коливання в пам'яті, використовуваної ядром операційної системи. Рекомендується перезавантажити систему тому що в деяких випадках це пояснюється помилками в операційній системі, які зникнуть після перезавантаження.

Для діагностики системи можна використовувати зовнішні антивірусні програми, зовнішні програми перевірки системи або вбудовані засоби ОС. Наприклад, для перевірки ідентичності файлів можна використовувати програму установки *Windows XP* з відповідним ключем. Довідку про ключі можна одержати, запустивши файл *Winnt32.exe* із ключем *"/?"*, який перебуває в дистрибутиві операційної системи, у папці 1386.

1.3.4. Закладка Мережа

У закладці *Мережа* відображається моніторинг мережевих або модемних з'єднань (рис. 14)

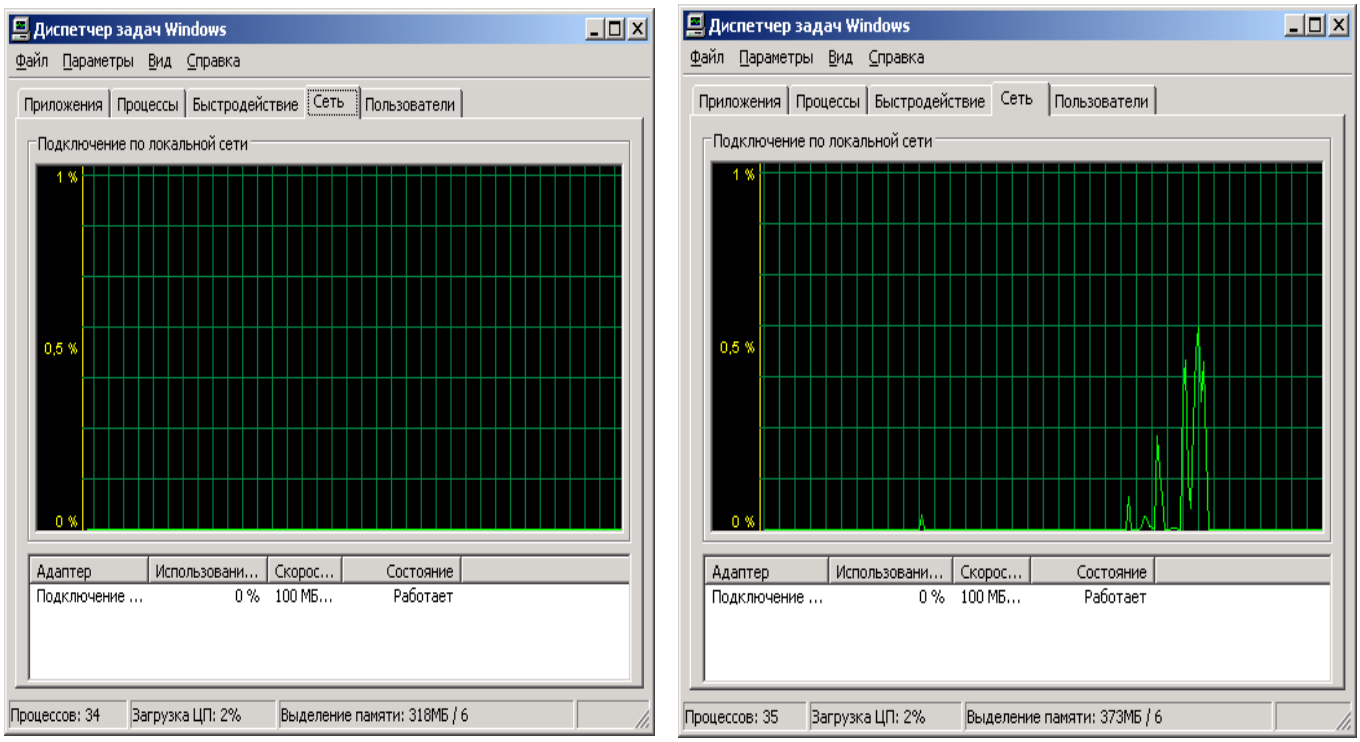


Рис. 14. Закладка *Мережа*

Якщо немає мережевих підключень, то на екрані з'явиться вікно ідентичне лівому вікну зображеному на рис. 14. Якщо ж комп'ютер підключений до комп'ютерної мережі й був зроблений вихід в Інтернет або була завантажена мережна програма, то на екрані з'явиться вікно ідентичне правому вікну зображеному на рис. 1.14.

У верхній частині вікна відображається графічна частина завантаження мережевого з'єднання. Завантаження виміряється від нуля до ста відсотків. У нижній частині вікна вказується для кожного мережевого адаптера системи його ім'я мережеве завантаження, швидкість й стан з'єднання.

Можна доповнити відображувані характеристики мережевих з'єднань (рис. 15):

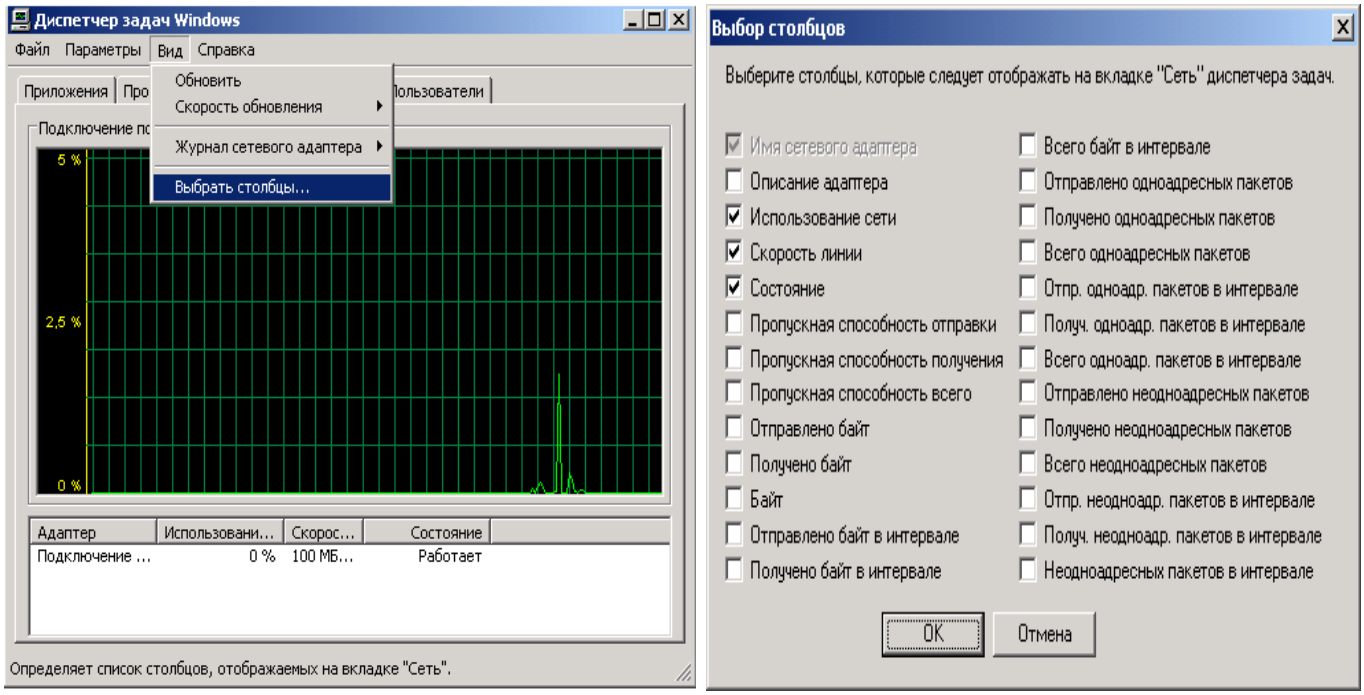
Меню *Вид* \ *Вибрати стовпці*

З метою підвищення поінформованості про процеси, що відбуваються в мережевих з'єднаннях, можна встановити ряд додаткових опцій:

- опція *Опис адаптера* дозволяє подивитися опис адаптерів, які використовуються в системі;
- опції *Пропускна здатність відправлення* й *Пропускна здатність одержання* дозволяють, відповідно, визначити кількість у відсотках переданих і одержуваних байт, які проходять через мережеве з'єднання в теперішній момент часу;
- опція *Пропускна здатність усього* показує у відсотках сумарну кількість інформації, що протікає через мережеве з'єднання, у теперішній момент часу;
- опції *Відправлено байт* і *Отримано байт* дозволяють, відповідно, визначити в байтах сумарна кількість переданих і отриманих даних через мережеве з'єднання за весь час його існування.

Усі мережеві програми, що працюють у системі, вносять свій внесок у завантаження певних мережевих інтерфейсів, якщо дійсно працюють із ними. Їхня активність відображається на вікні моніторингу мережевих з'єднань *Диспетчера завдань*.

Рис. 15 Опції, що дозволяють відображати у вікні моніторингу мережевих з'єднань додаткові параметри



Уміст закладки *Мережа* надає додаткову можливість пошуку сторонніх програм. Наприклад, якщо у вікні моніторингу існує постійне завантаження каналу, рівна певному значенню (за умови, що не були запущені мережеві програми й відновлення операційної системи виключене), то тоді із упевненістю можна сказати, що в системі зручно влаштувався вірус, троянська програма або програма-шпигун. Отже, необхідно перевірити систему антивірусним сканером і переконатися в коректності налагодження мережевого екрана. На відміну від інших засобів *Диспетчера завдань*, дана закладка може практично гарантовано виявити деструктивне програмне забезпечення.

1.3.5. Закладка Користувачі

Закладка *Користувачі* відображає користувачів, що працюють у теперішній момент у системі (рис.16).

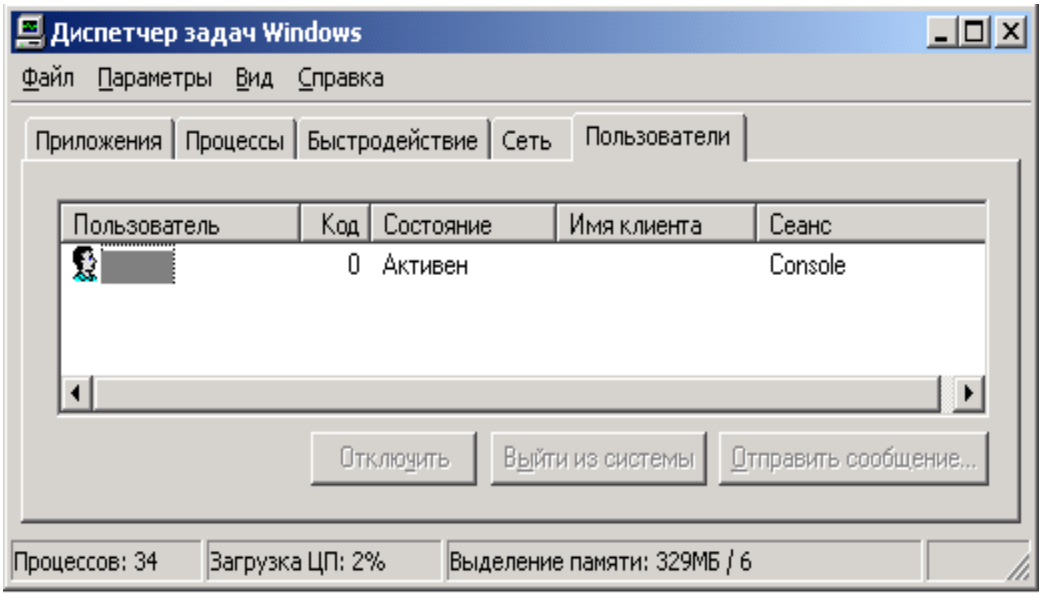


Рис. 16 Закладка *Користувачі*

У данім вікні можете вибрати користувача й подивитися його параметри у відповідних стовпцях:

- стовпець *Код* відображає ідентифікатор сесії користувача в системі;
- стовпець *Стан* – відображає статус користувача;
- стовпець *Ім'я клієнта* – відображає ім'я машини, з якої прийшов користувач, якщо він працює в мережі;
- стовпець *Сеанс* – відображає ім'я сесії користувача на комп'ютері.

За допомогою кнопок, розташованих унизу вікна, можна виконувати ряд системних дій по керуванню користувачами:

- кнопка *Відключити* – відключає обраного користувача від комп'ютера;
- кнопка *Вийти із системи* – змушує користувача вийти із системи;
- кнопка *Відправити повідомлення* – посилає іншому користувачеві повідомлення.

Вікно перегляду активних користувачів у системі зручне тим, що завжди можна контролювати користувачів або програми, які працюють у системі під відповідними обліковими записами. При виявленні підозрілого користувача можете його відключити або послати йому відповідне повідомлення. Крім того, у випадку виявлення яких-небудь проблем, завжди можна знати, хто працює в системі, і, як наслідок, почати адміністративні або інші заходи, у випадку виявлення причин цих проблем.

2. Хід роботи

Виконати завдання згідно п.1. Представити звіт з лабораторної роботи у вигляді пояснювального тексту та рисунків. Зробити висновки по роботі.

3. Контрольні питання

1. Що собою представляє механізм *Windows XP*, називаний *аудитом системи*?
2. Перелічіть функції, виконувані вищевказаним механізмом ОС.
3. Яким чином зробити налагодження *аудита локальної системи*?

4. Що собою представляють налагодження *аудита подій*?
5. Комплекс яких дій потрібно виконати для визначення того, коли буде відбуватися запис тої або іншої події, певної відповідним рядком списку політики аудита?
6. Перелічіть види аудита подій (зробіть копію вікна налагодження аудита з видами аудита подій).
7. Які характерні риси має політика аудита?
8. Яким чином зробити запис усіх спроб входу користувачів у систему?
9. Які дані політики аудита можуть придатися у випадку, якщо в системі буде відбуватися щось дивне й необхідно з'ясувати причини виниклих ситуацій?
10. Яка політика аудита дозволяє проводити аудит системних подій перезавантаження, вимикання комп'ютера й інших важливих повідомлень, що стосуються безпеки системи?:
11. Перелічіть особливості аудита системи.
12. Яким чином переглянути події, що відбуваються в системі?
13. Визначите призначення програми *Event Viewer*.
14. Яким чином завантажить програму *Event Viewer*?
15. Яким чином переглянути властивості конкретного повідомлення?
16. Перелічіть й опишіть інформаційні поля в описі події *Even*.
17. На яких типах подій слід сконцентрувати свою увагу?
18. З якими подіями (діями) можуть бути зв'язані повідомлення системи безпеки *Аудит відмов*?
19. Які дії слід почати при переповненні розділів безпеки системи?
20. Яким чином переглянути збережені події?
21. Визначите призначення *Диспетчера завдань*.
22. Перелічить функції *Диспетчера завдань*.
23. Які неприємності доставляють операційній системі завислі програми, як їх визначити і як з ними боротися?
24. Яким чином ідентифікувати процес, що відбувається в системі?
25. Що дозволить у будь-який момент часу контролювати процеси, що виконуються?
26. Поясните термін «ім'я образа, що виконується, ».
27. Яким чином у *Диспетчерові завдань* можна визначити можливі атаки на систему (перелічить всі можливості *Диспетчера завдань*)?
28. Яким чином визначити в *Диспетчерові завдань*, у якому стані перебуває процес (у стані очікування, у стані виконання або завис)?
29. За якими ознаками у Диспетчерові завдань можна визначити, що процес завис?
30. За якими ознаками за допомогою *Диспетчера завдань* можна визначити, що процес, запущений у системі спрямований на заподіяння збитку системи?
31. Перелічить Ваші дії у випадку виявлення невідомого Вам і системі процесу.
32. За допомогою якого параметра можна знайти потрібний процес у системі (при використанні програми *Диспетчер завдань*)?
33. За допомогою яких параметрів у *Диспетчерові завдань* можна визначити ступінь використання процесом центрального процесора?
34. Що можуть означати «більші запити до віртуальної пам'яті» і за допомогою якого параметра *в Диспетчерові завдань* можна визначити ступінь використання віртуальної пам'яті?
35. Який пріоритет має процес *Idle.exe* і як визначити в *Диспетчерові завдань* рівень пріоритету процесів?

36. Які неприємності ОС можуть заподіяти велика кількість процесів з рівнем пріоритету *Середній*?
37. Як визначити за допомогою *Диспетчера завдань* яку активність має процес? Для якої мети потрібна дана інформація?
38. На що вказує велика кількість потоків (>100) у процесу? Як визначити кількість потоків у процесу за допомогою Диспетчера завдань?
39. Як запобігти можливим атакам на систему? Які профілактичні дії слід проводити для цих цілей?
40. Що може означати ситуація, коли середнє завантаження системи становить більш п'яти відсотків? Які програми мають тенденцію перебувати постійно в системі?
41. Яка завантаженість мікропроцесора повинна бути в ідеалі? Як визначити завантаження системи за допомогою *Диспетчера завдань*?
42. Що означає ситуація, коли файл підкачування використовується більше ніж на половину за умови, що не були запущені інші програми?
43. Яка ситуація може відбутися якщо кількість дескрипторів, потоків і процесів буде занадто великим? Як визначити ці параметри за допомогою Диспетчера завдань?
44. Що може означати ситуація, коли група параметрів *Виділення пам'яті* різко змінюються (разів у два). Які дії слід робити в цьому випадку?
45. Яким чином можна доповнити відображувані характеристики мережевих з'єднань у *Диспетчерові завдань*?
46. Що відбувається, якщо у вікні моніторингу мережевих з'єднань існує постійне завантаження каналу, рівне певному значенню (за умови, що не були запущені мережеві програми й відновлення операційної системи виключене)?
47. Яким чином можна за допомогою *Диспетчера завдань* ідентифікувати користувача в системі? Які дії можна почати, якщо виявлений невідомий користувач?

48.

Лабораторна робота 4

Захист інформації під час застосування операційної системи Windows 7

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в операційній системі Windows 7.

Ознайомитись з рівнями захисту комп'ютера встановленням, зміною, зберіганням паролів, встановлення їх параметрів, захистом від вірусів, шпигунських і інших шкідливих програм, управління роботою брандмауера, захисника.

План

1. Теорія

1.1 Захист комп'ютера за допомогою пароля

Використання надійного пароля є одним з найбільш важливих факторів захисту комп'ютера від зловмисників і інших небажаних користувачів.

Пароль можна встановити при установці операційної системи на комп'ютер, з BIOS та змінити в процесі роботи.

В BIOS існує декілька можливостей установлення паролю з вкладки **Security: Supervisor Password (пароль на вхід до BIOS), User Password (пароль на операційну систему), HDD Password (пароль на доступ до жорсткого диску)** – це комплексний захист комп'ютера, дисків, розділів і конфіденційної інформації від несанкціонованого доступу. Захистіть ваші диски й розділи паролем, сховайте й захистіть свою інформацію від сторонніх осіб, обмежте перегляд і запуск файлів, це дозволить підвищити надійність захисту комп'ютера. Захист функціонує на низькому рівні, працює безпосередньо з диском і не

залежить від операційних систем, програм, іншого встаткування. Паролі шифруються й зберігаються в захищених областях диску. Маючи оригінальний, простий інтерфейс і покроковий майстер, програма дозволяє працювати із захистом користувачам будь – якої кваліфікації. Програма призначена для захисту завантаження комп'ютера з вінчестера шляхом установки пароля на вінчестер (у завантажувальний сектор). Пароль запитується відразу після ініціалізації BIOS і перед завантаженням операційної системи. Підтримка дисків до 127 Гігабайт. Працює у всіх операційних системах від Microsoft, крім ядер Winnt, тому що в них вбудований захист від прямого доступу до вінчестера.), Password on boot (пароль на доступ до завантаження, перезавантаження комп'ютера або перед зверненням до BIOS).

Пароль являє собою послідовність знаків, яка дозволяє користувачам входити в комп'ютер, одержувати доступ до файлів, програм і інших ресурсів. Паролі дозволяють бути впевненим у тому, що ніхто не буде мати доступу до комп'ютера доти, поки не одержить відповідного дозволу. В ОС Windows пароль може складатися з букв, цифр, символів, а також пробілів. В Windows у паролях ураховується регістр знаків. Щоб забезпечити безпеку комп'ютера, рекомендується завжди використовувати надійні паролі (табл. 1,2).

Таблиця 1

Надійні паролі й парольні фрази містять знаки, що належать кожній з наступних категорій:

Категорія знаків	Приклади
Букви верхнього регістру	A, B, C...
Букви нижнього регістру	a, b, c ...
Цифри	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Інші знаки на клавіатурі (усі знаки, що не є буквами або цифрами) і пробіли	` ~ . @ # $ % & * ( ) _ — + = { } [ ] \ | : ; " ' < >, . ? /

Таблиця 2

Ознаки надійних паролів і парольних фраз

Надійний пароль:	Надійна парольна фраза:
• Містить як мінімум вісім знаків. • Не містить імені користувача, дійсного імені або назви компанії. • Не містить повного слова. • Значно відрізняється від паролів, що використовувалися раніше.	• Значно відрізняється від паролів і парольних фраз, що використовувалися раніше. • Являє собою послідовність слів, що утворюють фразу. • Не містить загальних фраз, що зустрічаються в літературі або музичних додатках. • Не містить слів, що зустрічаються в словниках. • Має довжину від 20 до 30 знаків. • Не містить імені користувача, дійсного імені або назви компанії.

Пароль або парольна фраза, що відповідають усім описаним вище умовам, як і раніше можуть бути ненадійними. Наприклад, пароль виду Suna56K# задовольняє всім вимогам до надійності, але є ненадійним, тому що містить повне слово. S7na 56 K# надійніше

попереднього, тому що деякі букви в слові заміщені цифрами, і, крім того, пароль містить пробіли.

Паролі Windows можуть містити набагато більше восьми символів, рекомендованих раніше. Допускається створення паролів довжиною до 127 знаків. Однак у мережі, у якій також працюють комп'ютери під керуванням ОС Windows 95 або Windows 98, рекомендується застосовувати паролі не довші 14 символів. Якщо пароль містить більш 14 знаків, вхід у мережу з комп'ютерів під керуванням зазначених вище операційних систем може бути неможливий.

1.2 Зміна (встановлення) пароля Windows

Пароль Windows використовується для входу в систему. Щоб ваш комп'ютер був більш захищеним, рекомендується регулярно міняти пароль Windows і використовувати надійний пароль.

1. Натисніть клавіші **Ctrl+Alt+Delete** і виберіть команду **Сменить пароль**.
2. Уведіть старий пароль, новий пароль, а потім повторіть введення нового пароля для підтвердження, після цього натисніть клавішу з стрілкою та **ОК**.

Примітка:

- при вході в систему з правами адміністратора, можна створювати й міняти паролі для всіх облікових записів користувачів на комп'ютері;
- при зміні пароля іншого облікового запису з використанням облікового запису адміністратора всі зашифровані файли або повідомлення електронної пошти, створені користувачем, що використовує цей обліковий запис, більше не будуть йому доступні.

1.3 Створення диску скидання пароля

Якщо пароль Windows загублений, можна створити новий за допомогою диску скидання пароля. Щоб не втратити доступ до файлів і інформації, рекомендується створити диск скидання пароля відразу після створення пароля.

Для створення диску знадобиться з'ємний носій, такий як USB – устрій флеш – пам'ять або дискета.

1. Встановіть з'ємний носій.
2. Зайдіть у **Панель управления** в **Учетные записи пользователей**. Розкрийте вказаний список команд (клацніть по піктограмі лівою клавішею миші).
3. У лівій області вікна (рис. 1) уведіть команду **Создание дискететы сброса пароля** й додержуйтеся інструкцій майстра (рис. 2 –5). Зберігайте диск скидання пароля в надійному місці.

В результаті роботи майстра на з'ємному диску з'являється файл, наприклад, userkey.psw

Примітка. Можна створити дискету скидання пароля натиснувши клавіші **Ctrl+Alt+Delete** і відібравши команду **Создание дискететы сброса пароля**.

1.4 Створення або зміна підказки для пароля

При створенні пароля для входу в Windows можна створити підказку, що допомагає запам'ятати його. Якщо пароль уже був створений, то для створення підказки необхідно його змінити.

1. Відкрийте компонент **Учетные записи пользователей**.
2. Уведіть команду **Смена своего пароля**.
3. Уведіть поточний пароль, новий пароль, і підтвердження нового пароля.
4. Уведіть підказку для нового пароля. Слід пам'ятати, що кожний, хто має доступ до комп'ютера, зможе бачити підказку.
5. Уведіть команду **Сменить пароль**.

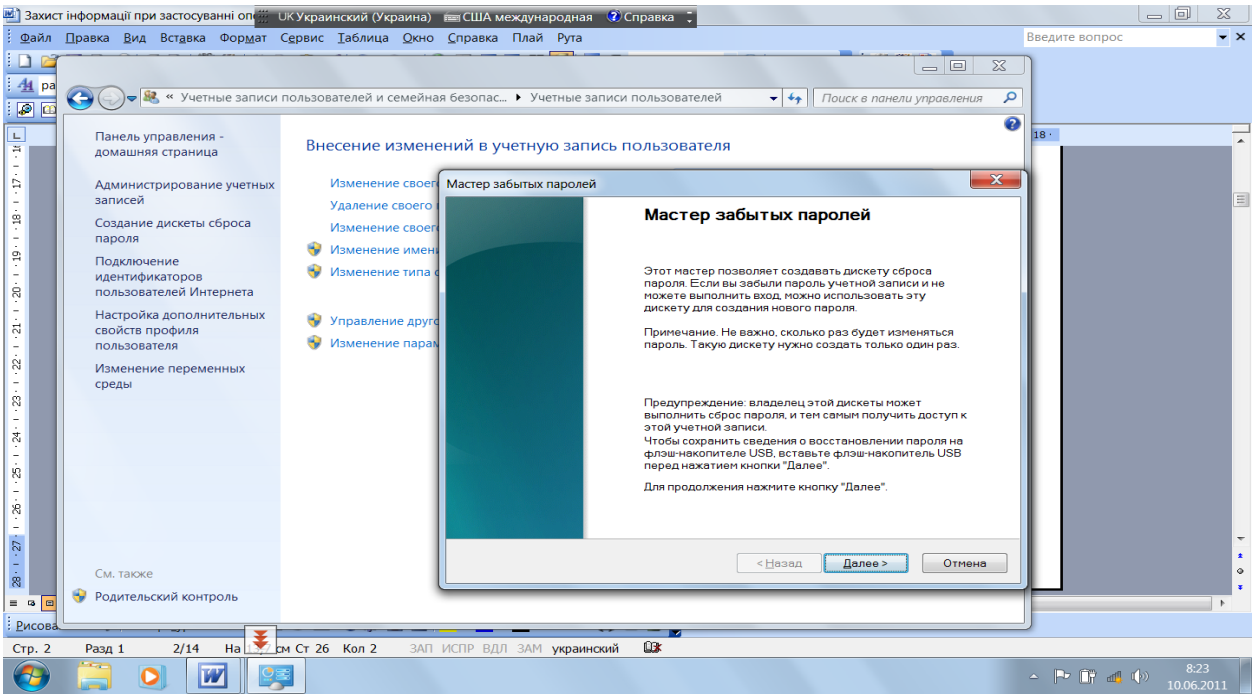


Рис. 1 Вікно майстра створення диску скидання паролів

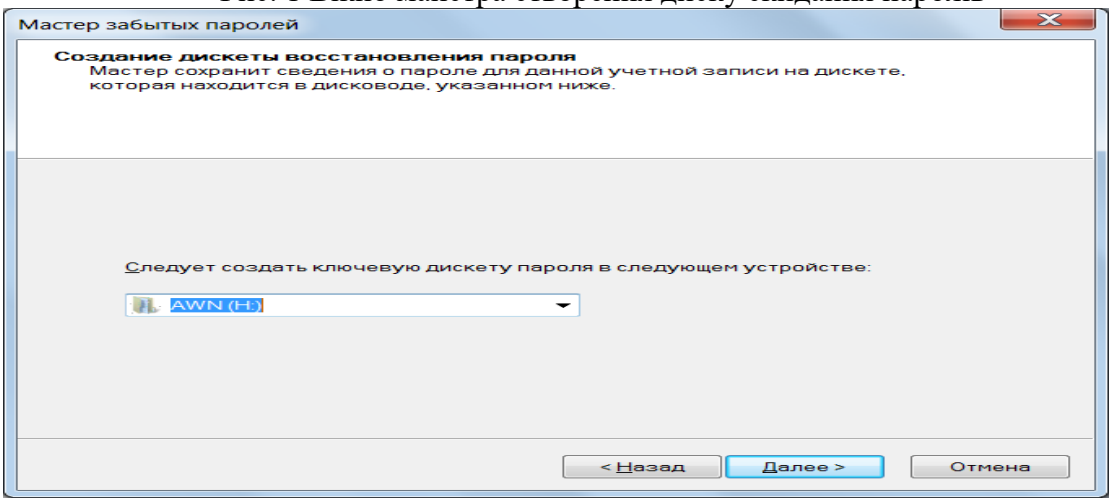


Рис. 2 Вікно вказівки диску збереження

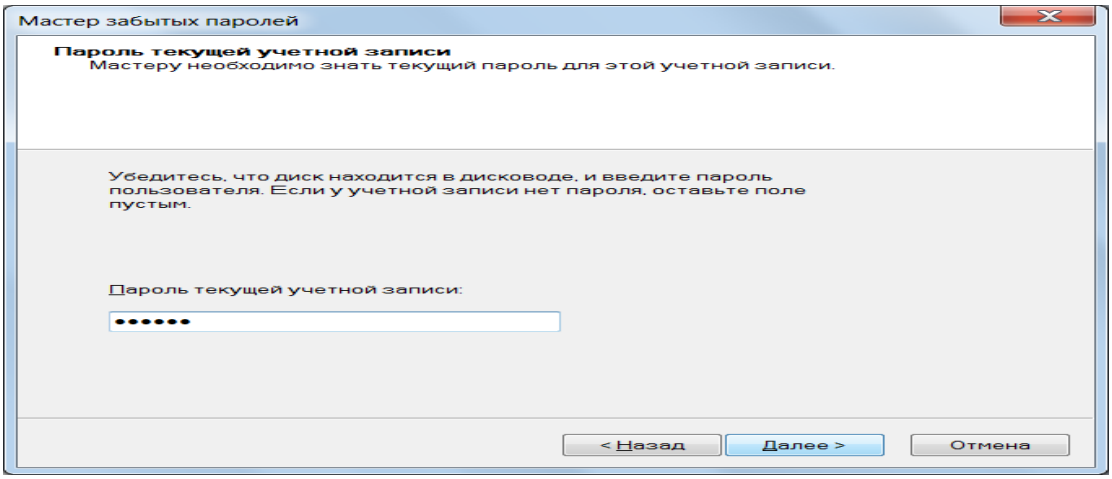


Рис. 3 Вікно робочого пароля

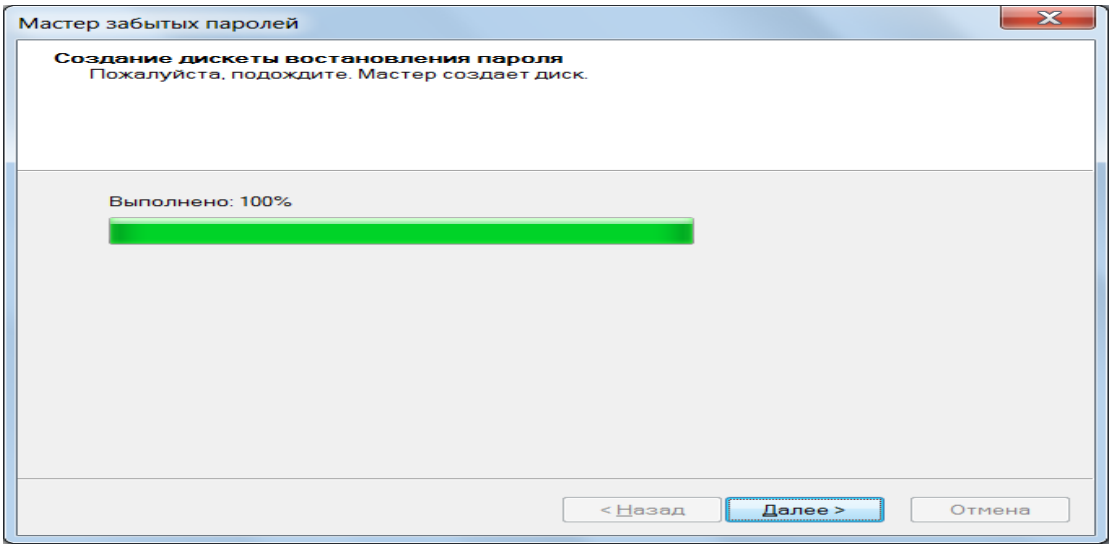


Рис. 4 Вікно процесу створення файлу

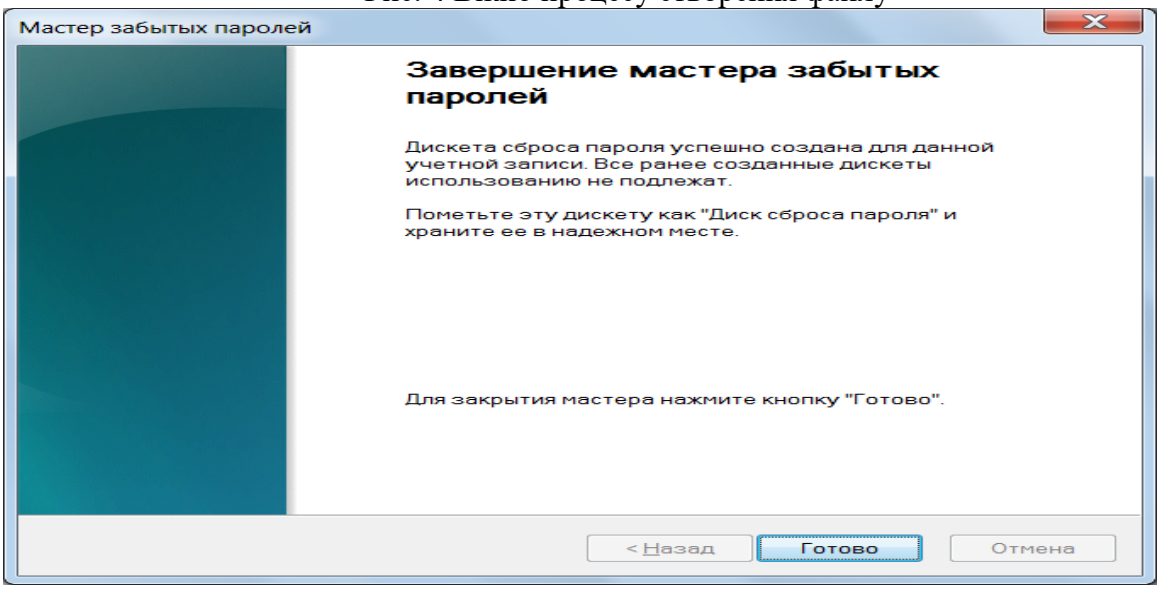


Рис. 5 Заключне вікно роботи майстра

1.5 Зміна способу запиту пароля при виході комп'ютера зі сплячого режиму

Для захисту комп'ютера операційна система Windows запитує пароль для розблокування комп'ютера при виході зі сплячого режиму за умовчанням. Запит пароля при виході зі сплячого режиму дозволяє захистити дані, що особливо актуально при зберіганні на комп'ютері конфіденційної інформації. Однак, якщо комп'ютер установлений удома й на ньому працює тільки один користувач, то можна змінити цей параметр, тоді при виході зі сплячого режиму операційна система не буде запитувати пароль.

1. Відкрийте компонент **Учетные записи пользователей**.
2. Уведіть команду **Система и безопасность.**
3. Уведіть команду **Электропитание**.
4. Уведіть команду **Запрос пароля при пробуждении** (рис. 6).
5. Відберіть потрібні параметри.
6. Уведіть команду **Сохранить изменения**.

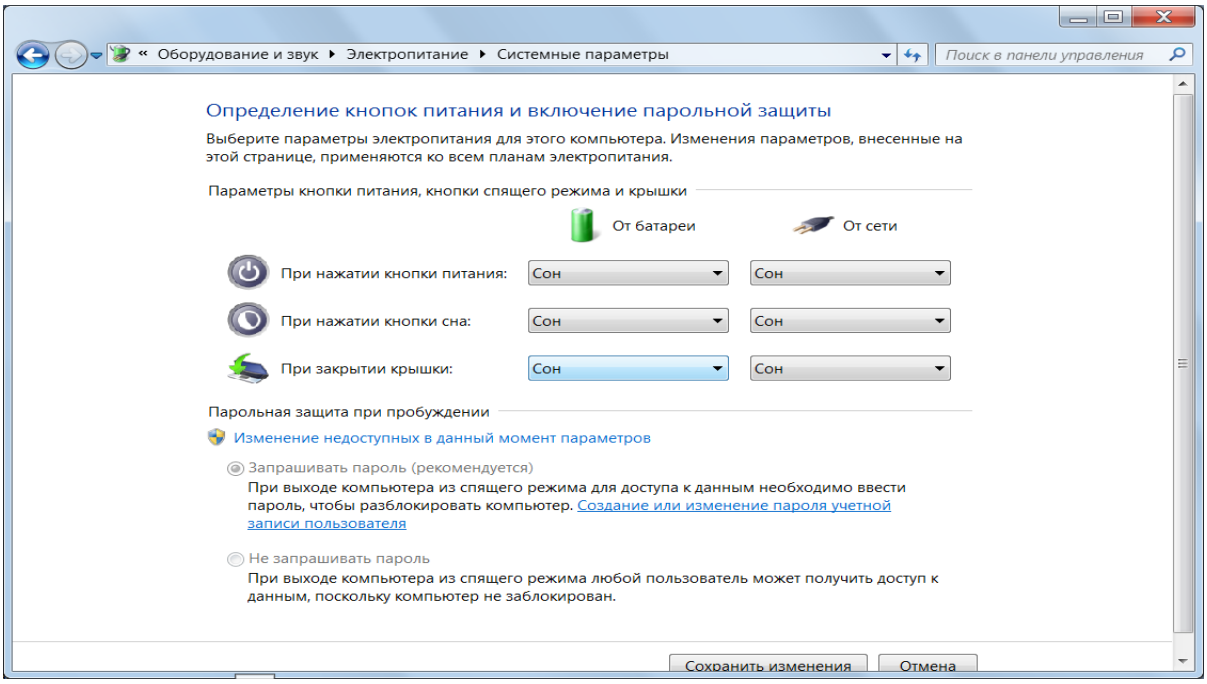


Рис. 6 Вікно відбору параметрів при пробудженні комп'ютера

2. Використання брандмауера.

Брандмауер – це програмне або апаратне забезпечення, яке перевіряє інформацію, що входить в комп'ютер з локальної мережі або Інтернету, а потім або відхиляє її, або пропускає в комп'ютер, залежно від параметрів брандмауера. Таким чином, брандмауер допомагає запобігти доступу хакерів і шкідливих програм до комп'ютера. Брандмауер Windows вбудований в Windows і включається автоматично.

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 запитує користувача про блокування або дозвіл підключення. Якщо користувач дозволяє підключення, брандмауер Windows створює виключення.

2.1 Включення і виключення брандмауера Windows

1.Відкрийте **Панель управления** (рис. 7).

2. Клацніть по значку розділу **Система и безопасность**.

3. Відберіть команду **Брандмауэр Windows** (рис. 8).

3. У лівій області виберіть **Включение и отключение брандмауэра Windows** .

При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

4. Клацніть **Включение брандмауэра Windows** під кожним мережевим розміщенням, яке слід захистити, і натисніть кнопку **ОК**.

Якщо брандмауер повинен блокувати все, включаючи програми, яким раніше було дозволено встановлювати зв'язок через брандмауер, встановіть прапорець **Блокирование всех входящих подключений**. Такий вибір включає навіть підключення, вказані в списку дозволених програм.

2.2 Включення і виключення мережевого виявлення

Мережеве виявлення – це налагодження мережі, яке визначає, чи може комп'ютер користувача бачити інші комп'ютери і пристрої в мережі, а також чи видимий він іншим комп'ютерам мережі. За умовчанням брандмауер Windows блокує мережеве виявлення, але можна надати цю можливість.

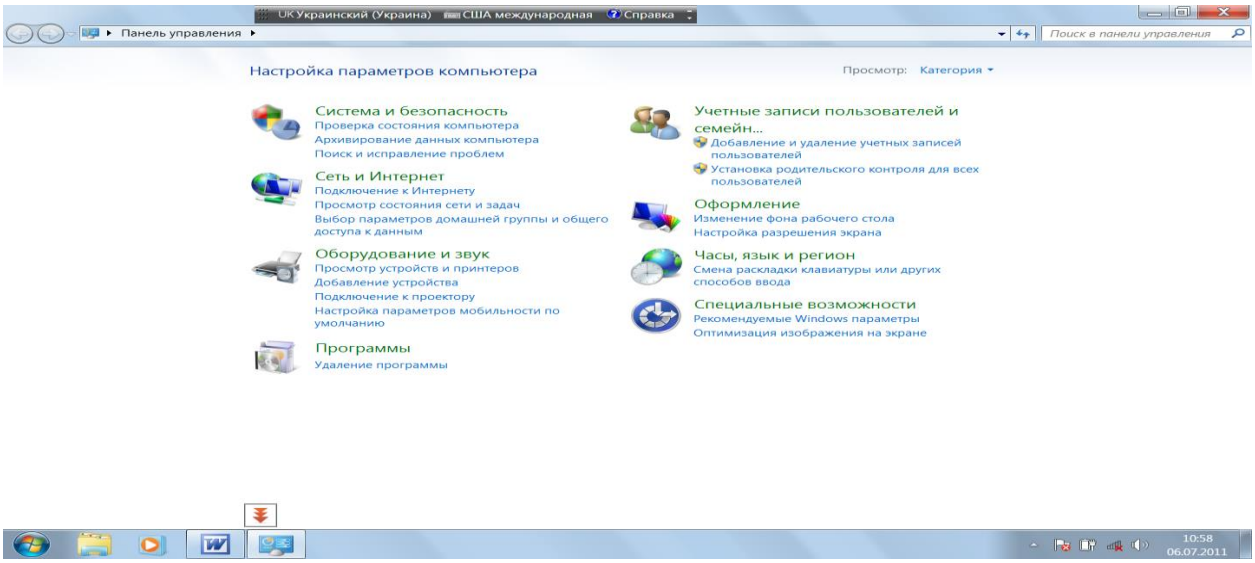


Рис. 7 Панель управления

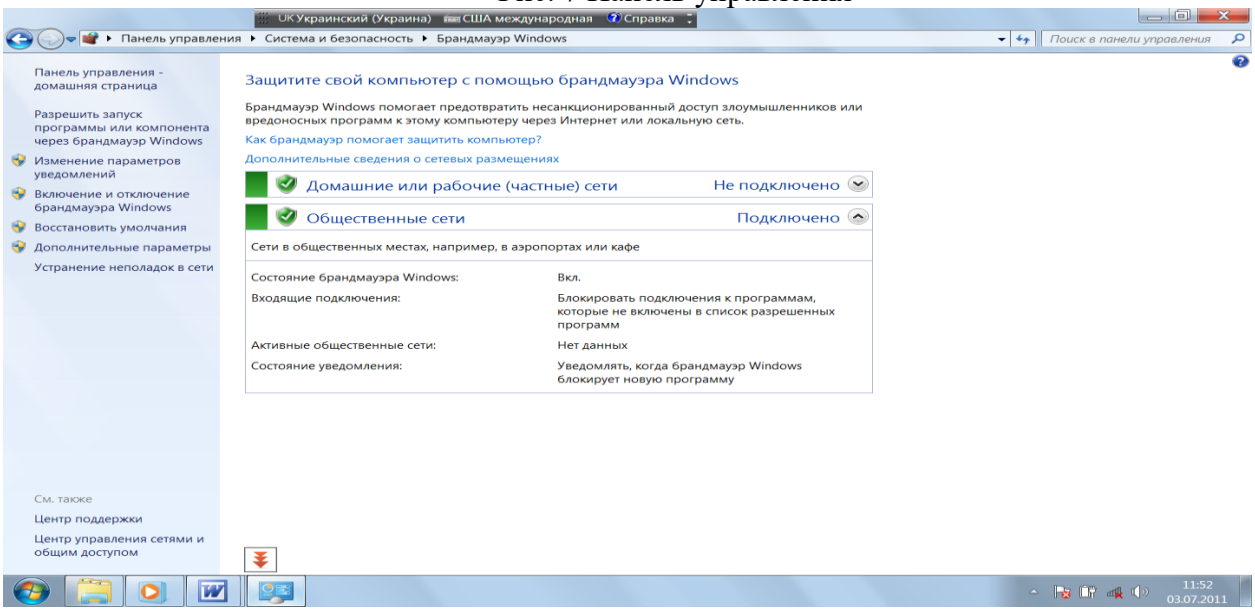


Рис. 8 Вікно брандмауер Windows

1. В вікні брандмауера Windows відберіть команду **Дополнительные параметры общего подключения.**

2. Клацніть значок у вигляді подвійних лапок, щоб розвернути поточний мережевий профіль.

3. У меню **Включить сетевое выявление** виберіть пункт **Сохранить изменения.** При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

2.3 Відновлення параметрів брандмауера Windows

Якщо деякі параметри брандмауера були змінені, і потрібно відмінити ці зміни, можна відновити параметри брандмауера до початкового стану (значенням за умовчанням).

1. Відкрийте брандмауер Windows.

2. У лівій області клацніть **Восстановить умолчание**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

3. У діалоговому вікні натисніть кнопку **Восстановить умолчание** (рис. 9). У вікні підтвердження натисніть кнопку **ОК**.

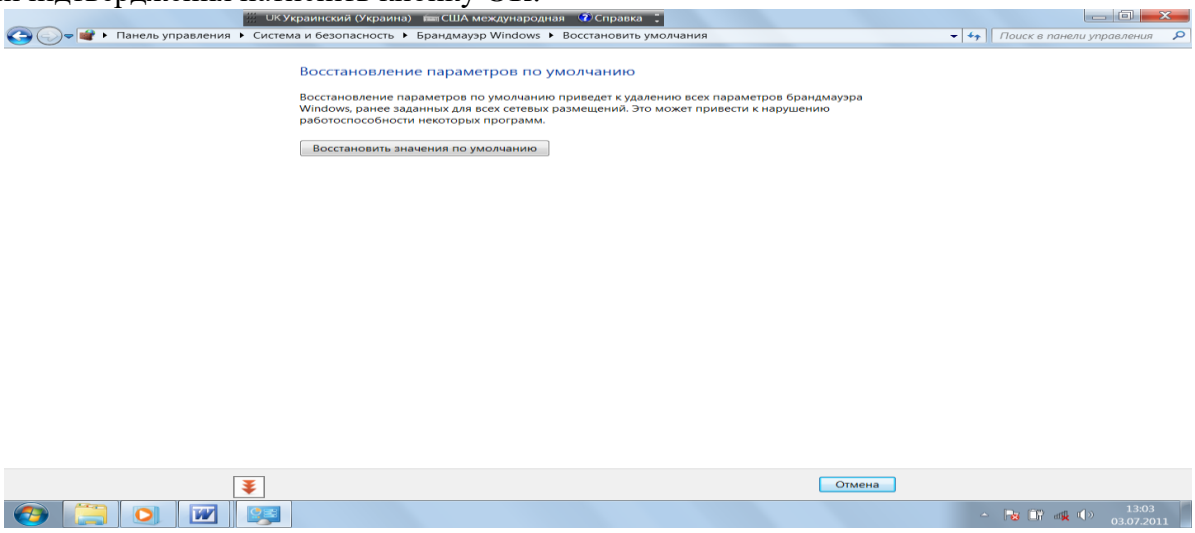


Рис. 9 Відновлення параметрів брандмауера

Примітка. Відновлення значень за умовчанням видаляє всі значення параметрів брандмауера Windows, які були налагоджені для всіх типів мережевих з'єднань. Це може стати причиною того, що деякі програми, яким було дозволено встановлювати зв'язок через брандмауер, будуть зупинені.

2.4 Дозвіл програмі встановлювати зв'язок через брандмауер Windows

За умовчанням більшість програм блокуються брандмауером Windows, що сприяє забезпеченню більш високого рівня безпеки комп'ютера. Деяким програмам для правильної роботи потрібен дозвіл встановлювати зв'язок через брандмауер. Це робиться таким чином:

1. Відкрийте вікно брандмауер Windows

2.У лівій області виберіть **Разрешить запуск программы или компоненту через брандмауэр Windows** (рис. 10).

3. Клацніть **Изменить параметры**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

4.Встановіть прапорець напроти програми, параметри доступу якої треба змінити, виберіть мережеві розміщення, з якими слід дозволити встановлювати з'єднання, і натисніть кнопку **ОК**.

Примітка. Перш ніж дозволяти програмі встановлювати зв'язок через брандмауер, користувач повинен усвідомлювати всі ризики, пов'язані з даним з'єднанням.

2. Іншим програмам для надання параметрів доступу введіть команду **Разрешить другую программу** (рис. 11). Виберіть потрібну програму введіть команду **Добавить** та потрібні параметри доступу (рис. 12).

Якщо необхідно блокувати всі підключення то – в вікні Брандмауер Windows відібрати команду **Изменение параметров уведомлений** (рис. 13) та поставити прапорець біля команди **Блокирование всех входящих подключений, включая подключение, указанные в списке разрешенных программ.**

Цей параметр блокує всі неочікувані спроби підключення до комп'ютера. Він служить для максимального захисту комп'ютера, наприклад при підключенні до загальнодоступної мережі в готелі або аеропорту або в періоди розповсюдження через Інтернет особливо небезпечних вірусів — черв'яків. При використанні цього параметру ви не будете повідомлені про блокування програм брандмауером Windows, і всі програми із списку

дозволених програм будуть проігноровані. При блокуванні всіх вхідних підключень можна проглядати більшість web – сторінок, відправляти і приймати електронну пошту, а також відправляти і приймати миттєві повідомлення. Команда **Сообщать, когда брандмауэр**

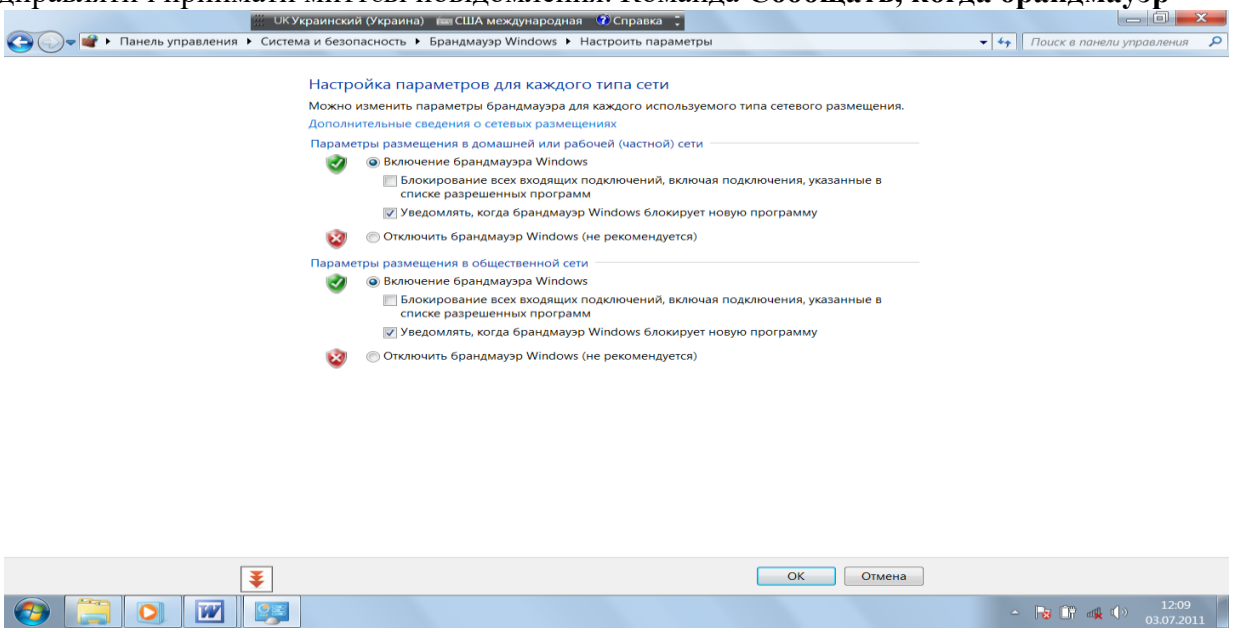


Рис. 10 Відбір параметрів включення\виключення Брандмауер Windows

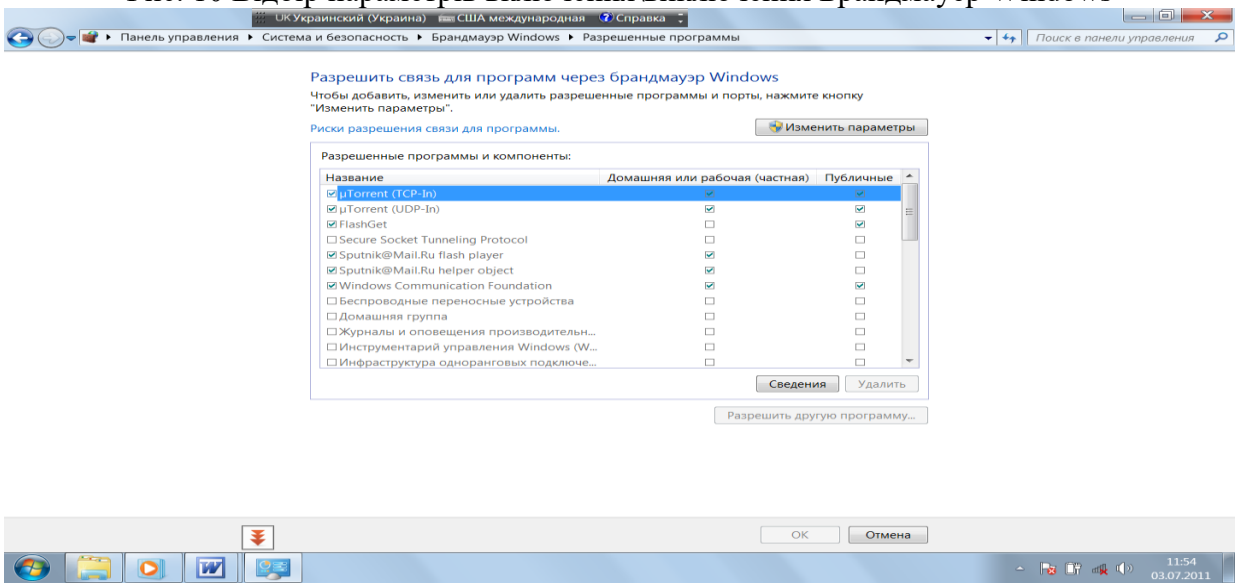


Рис. 11 Вікно дозволу роботи програмам

Windows блокує новую программу повідомляє користувача при блокуванні нової програми і надає можливість відмінити блокування.

2.5 Відкриття порту в брандмауері Windows

Якщо брандмауер Windows блокує програму, але необхідно дозволити цій програмі встановлювати зв'язок через брандмауер, ви повинні вибрати цю програму в списку дозволених програм (список виключень) в брандмауері Windows. Проте, якщо програми немає в списку, можливо, потрібно буде відкрити порт. Наприклад, щоб грати з друзями в мережі в багатокористувацьку гру, необхідно відкрити порт для цієї гри так, щоб брандмауер дозволив відповідним даним увійти до комп'ютера. Порт залишається відкритим постійно, тому закривайте порти, якщо вони більше не потрібні.

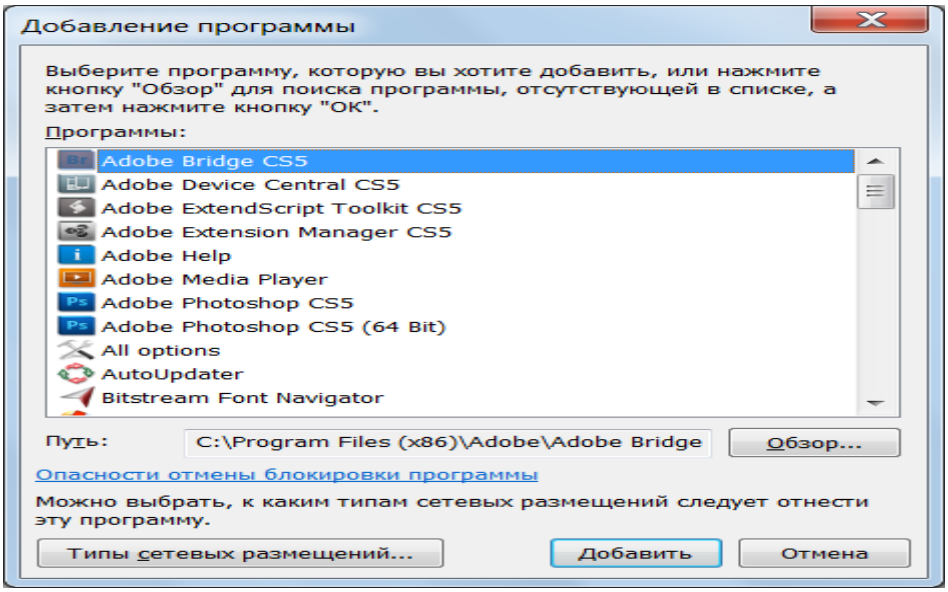


Рис. 12 Вікно відбору програм

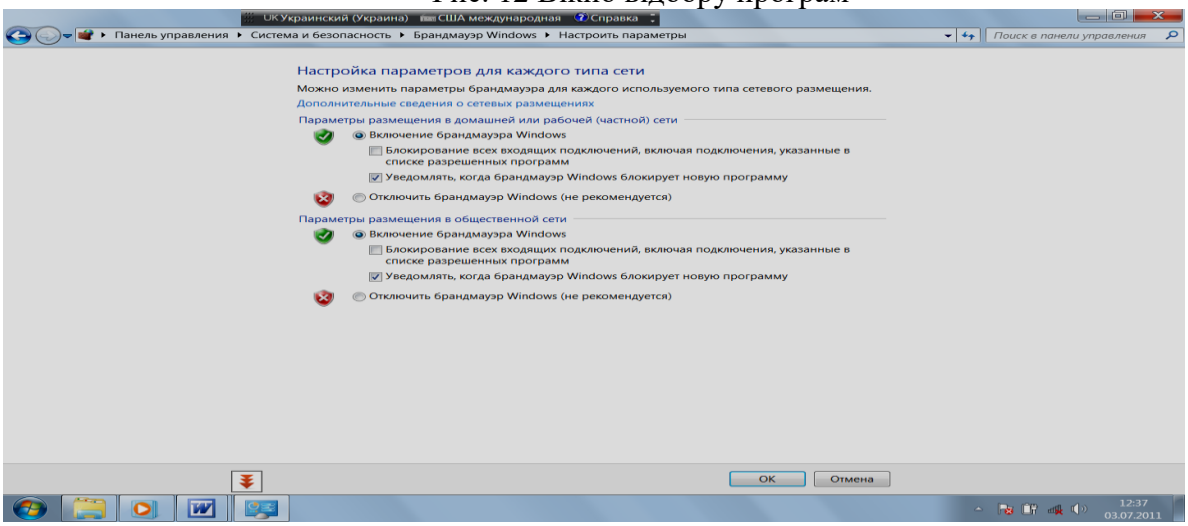


Рис. 13 Вікно блокування підключень

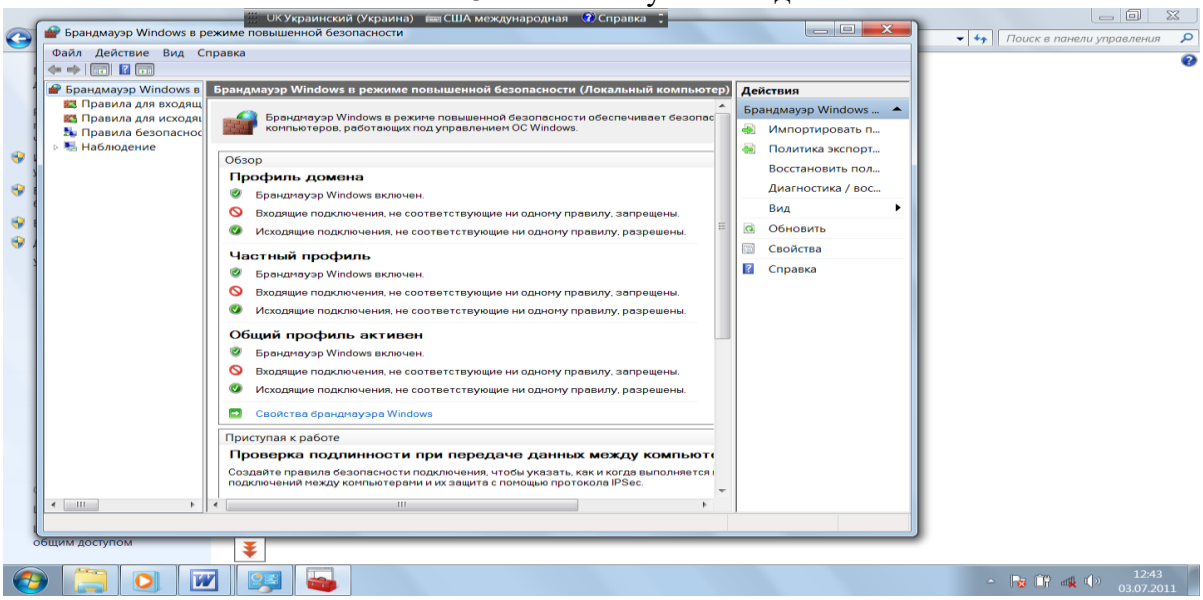


Рис. 14 Вікно додаткових параметрів

1. Відкрийте брандмауер Windows.
2. У лівій області виберіть **Дополнительные параметры** (рис. 14).

(При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження).

3. У діалоговому вікні Брандмауер Windows в режимі підвищеної безпеки в лівій області клацніть **Правила для входящих подключений** (рис. 15) і потім в правій області клацніть **Создать правило** (рис. 16).
4. Слідуйте інструкціям майстра створення правила для нового вхідного підключення.

Кожного разу, коли відкривається порт або програмі дозволяється зв'язок через брандмауер, комп'ютер стає менш безпечним. Чим більше дозволених програм або відкритих портів має брандмауер, тим більше можливостей з'являється у хакерів і шкідливих програм для запуску черв'яків, діставання доступу до файлів або використання комп'ютера для розповсюдження шкідливих програм на інші комп'ютери.

Зазвичай безпечніше додати програму в список виключень замість відкриття порту. Якщо відкритий порт, то він залишається відкритим до тих пір, поки не буде закритий, незалежно від того, використовує його програма чи ні. При додаванні програми в список дозволених програм, отвір відкривається тільки при необхідності для певного з'єднання.

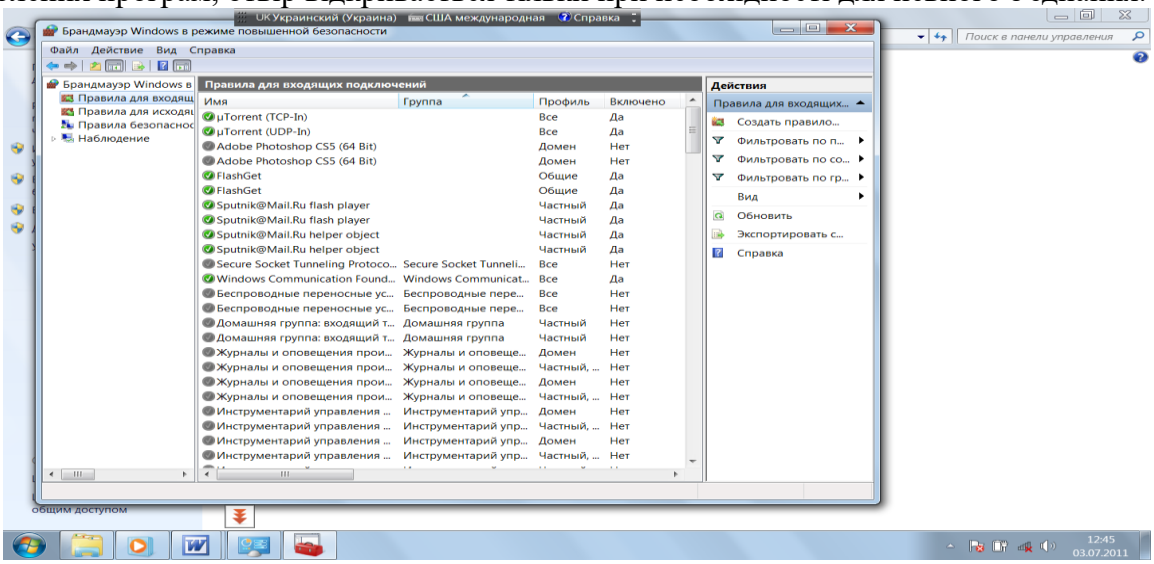


Рис. 15 Правила для вхідних підключень

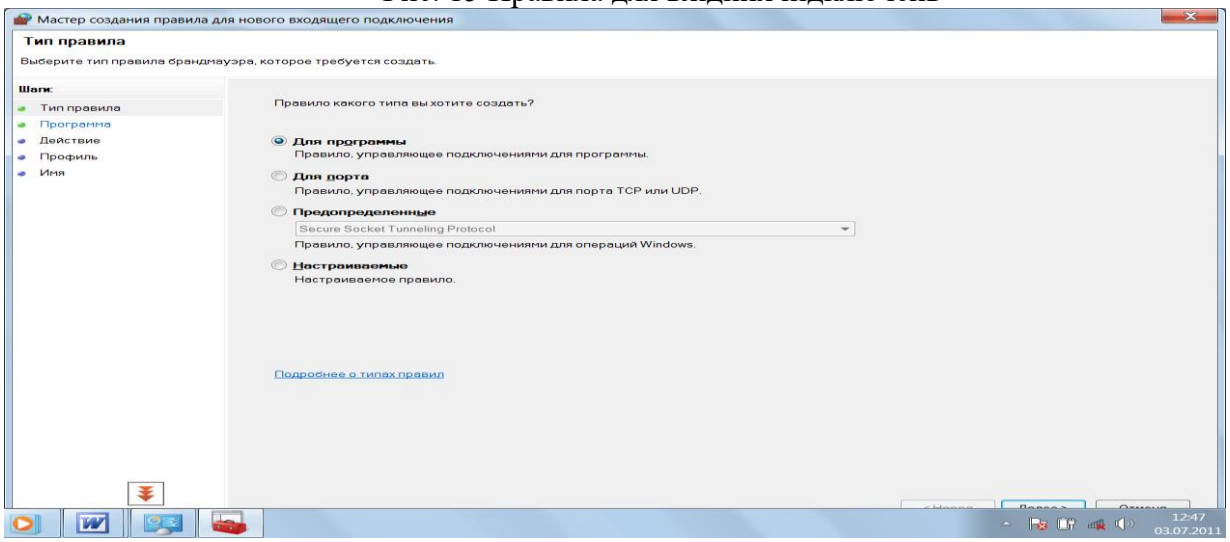


Рис. 16 Майстер створення правила

3 Захист від вірусів

Віруси, черв'яки і троянські коні – це програми, створені хакерами, що використовують Інтернет для зараження уразливих комп'ютерів. Віруси і черв'яки можуть розмножуватися від комп'ютера до комп'ютера, тоді як троянські коні потрапляють в комп'ютер, ховаючись в імовірно легальних програмах, таких як, наприклад, заставки. Деструктивні віруси, черв'яки і троянські програми можуть стерти інформацію з жорсткого диску або повністю вивести комп'ютер з ладу. Інші програми не наносять пряму утрату, але погіршують швидкодію і стабільність комп'ютера.

Антивірусні програми перевіряють електронну пошту і інші файли комп'ютера на наявність вірусів, черв'яків і троянських програм. При виявленні шкідливої програми антивірусна програма або відправляє вірус в карантин (ізолює), або повністю видаляє його до нанесення збитку комп'ютеру і файлам.

Windows не має вбудованої антивірусної програми, але виробник комп'ютера може встановити таку. Оскільки нові віруси виявляються щодня, дуже важливо вибрати антивірусну програму з можливістю автоматичного оновлення. При оновленні антивірусне програмне забезпечення додає нові віруси в список перевірки (базу), захищаючи комп'ютер від нових атак. Застарілий список вірусів залишає комп'ютер уразливим для нових погроз. Оновлення зазвичай вимагає сплати за щорічну підписку.

3.1 Оновлення антивірусного програмного забезпечення

Оновлення антивірусних програм для ефективного захисту від нових вірусів слід регулярно виконувати. Більшість антивірусних програм розроблена з можливістю автоматичного оновлення, але можна також оновлювати програму вручну.

Windows не поставляється з антивірусними програмами, але найчастіше може виявляти і відстежувати роботу тих антивірусних програм, які встановлені користувачем або виготівником комп'ютера. Стан антивірусної програми зазвичай відображається в центрі підтримки.

1. Відкрийте **Центр поддержки**.
2. Натисніть кнопку із стрілкою поряд з вузлом Бопасность, щоб розкрити розділ.

Якщо Windows може виявити встановлені антивірусні програми, то їх список буде відображений в розділі **Защита от вирусов** (рис. 17).

3. Клацніть **Восстановить**.

Примітка. Параметр **Восстановить** відображається тільки в тому випадку, якщо ОС Windows визначила необхідність оновлення антивірусної програми. Дані про стан надаються ОС Windows не всіма антивірусними програмами.

Якщо антивірусні програми не відображаються в центрі підтримки, перейдіть в розділ оновлень web – сайту постачальника антивірусного програмного забезпечення. Знайдіть оновлення для потрібної версії програми і операційної системи і встановіть його.

3.2 Захист від шпигунських і інших шкідливих програм.

Шпигунські програми можуть відображати рекламу, збирати особисті відомості і змінювати параметри комп'ютера, зазвичай без отримання на те дозволу. Наприклад, шпигунські програми можуть встановлювати небажані панелі інструментів, посилання або списки вибраного в браузер, змінювати стандартну домашню сторінку або часто відображати спливаючу рекламу. Деякі шпигунські програми не проявляють видимих симптомів, але таємно збирають важливі відомості, такі як відвідувані сайти або текст, що набирається. Більшість шпигунських програм встановлюються разом із безкоштовним програмним забезпеченням, але в деяких випадках до зараження може привести звичайні відвідини web – сайту.

Можливо, на комп'ютері встановлено яке – небудь шпигунське програмне забезпечення, якщо:

- з'являються нові панелі інструментів, посилання або об'єкти вибраного, які ви не додавали у браузер;
- несподівано змінюється домашня сторінка за умовчанням, покажчик миші або пошукова програма;
- при введенні адреси певного web – сайту (наприклад, пошукової системи) без попередження виконується перехід на інший web – сайт;
- відображаються спливаючі рекламні оголошення, навіть якщо немає підключення до Інтернету;
- комп'ютер раптово починає завантажуватися або працювати повільніше.

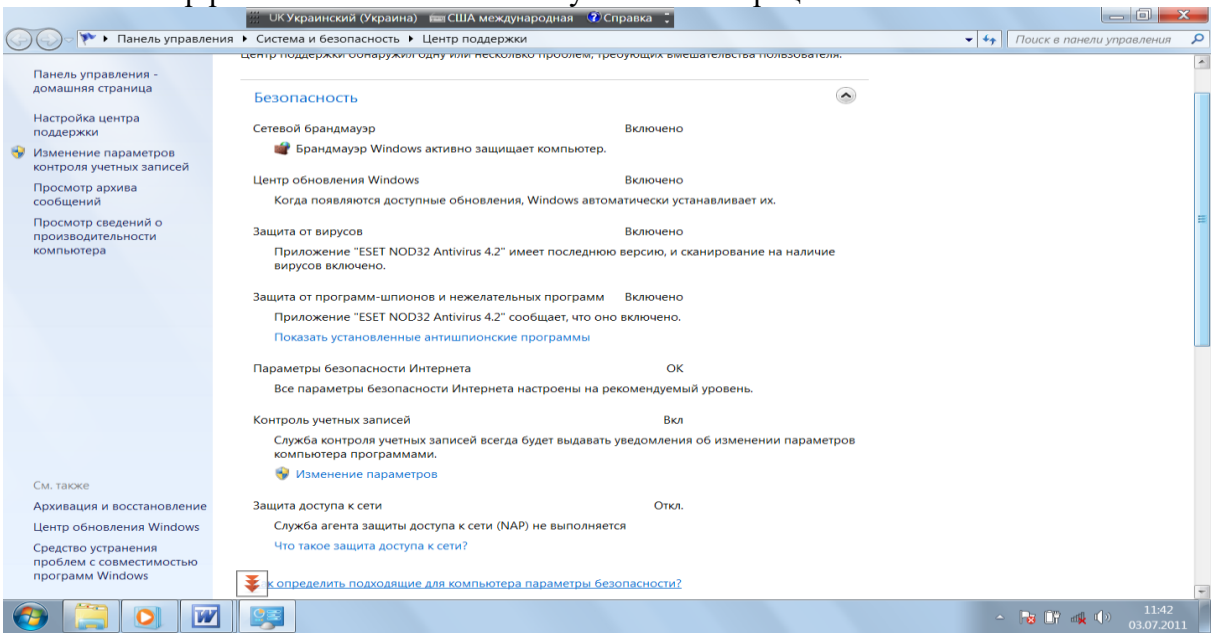


Рис. 17 Вікно команд безпека

Крім шпигунських програм треба відмітити віруси. 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, системного завантажувача 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 прогляданння 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 досягається 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 3apa3a), 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, 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.

Можливо, на комп'ютері є шпигунське програмне забезпечення, або віруси, навіть якщо ці симптоми відсутні. Запуск Захисника Windows під час роботи на комп'ютері може допомогти виявити і видалити таке програмне забезпечення.

Дана версія Windows містить вбудовану антишпигунську програму Захисник Windows, включену за умовчанням. Захисник Windows попереджає про спроби шпигунської програми встановити себе на комп'ютер. Захисник також може шукати на комп'ютері шпигунські програми і видаляти їх.

Оскільки нові шпигунські програми з'являються щодня, Захисник Windows повинен регулярно оновлюватися, щоб виявляти і захищати комп'ютер від новітніх погроз. Захисник Windows оновлюється в міру необхідності разом з оновленням Windows. Для найвищого рівня захисту включіть автоматичне оновлення Windows.

Захисник Windows забезпечує два способи запобігти зараженню комп'ютера шпигунськими програмами.

- захист в реальному часі. Захисник Windows оповіщає користувача про те, що шпигунська програма намагається встановитися або запуститися на комп'ютері. Користувач також отримає повідомлення, якщо яка – небудь програма спробує змінити важливі параметри Windows;
- параметри сканування. Захисник Windows можна використовувати для пошуку шпигунських програм, які могли встановитися на комп'ютері, для планування регулярних перевірок, а також для автоматичного видалення шкідливих програм, виявлених під час перевірки.

3.3 Включення і відключення захисника Windows|

1. З палелі задач відкрийте **Центр поддержки** (рис. 18).
2. Запустіть захисник Windows командою **Сканировать сейчас** (рис. 19). Вікно програми показано на рис. 20.
3. У меню **Программы** виберіть **Параметры**.
4. Виберіть пункт **Администратор**, встановіть або зніміть прапорець **Использовать эту программу,** а потім натисніть кнопку **Сохранить**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

3.4 Планування перевірок комп'ютера захисником Windows

Слід запланувати щоденну швидку перевірку, оскільки в цьому випадку перевіряються області комп'ютера, які найчастіше заражаються шпигунськими і іншими небажаними програмами. Щоб захисник Windows перевірив всі файли і програми на комп'ютері, запустіть повне сканування або заплануйте його.

Можна задати автоматичне видалення шпигунських і інших небажаних програм, виявлених під час сканування для підвищення безпеки комп'ютера

1. Запустіть захисник Windows .
2. У меню **Программы** виберіть **Параметры**.

2. У розділі **Автоматическая проверка** встановіть прапорець **Автоматически проверять компьютер (рекомендується)**, виберіть частоту, час і тип перевірки, а потім натисніть кнопку **Сохранить** (рис. 21).

3. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

4. Для автоматичного видалення шпигунських або інших потенційно небажаних програм після перевірки виберіть в лівій панелі **Действия по умолчанию**, вкажіть дію, яку слід застосувати до всіх об'єктів оповіщення, встановіть прапорець **Применить действия, которые рекомендуются**, і натисніть кнопку **Сохранить** (рис. 22).

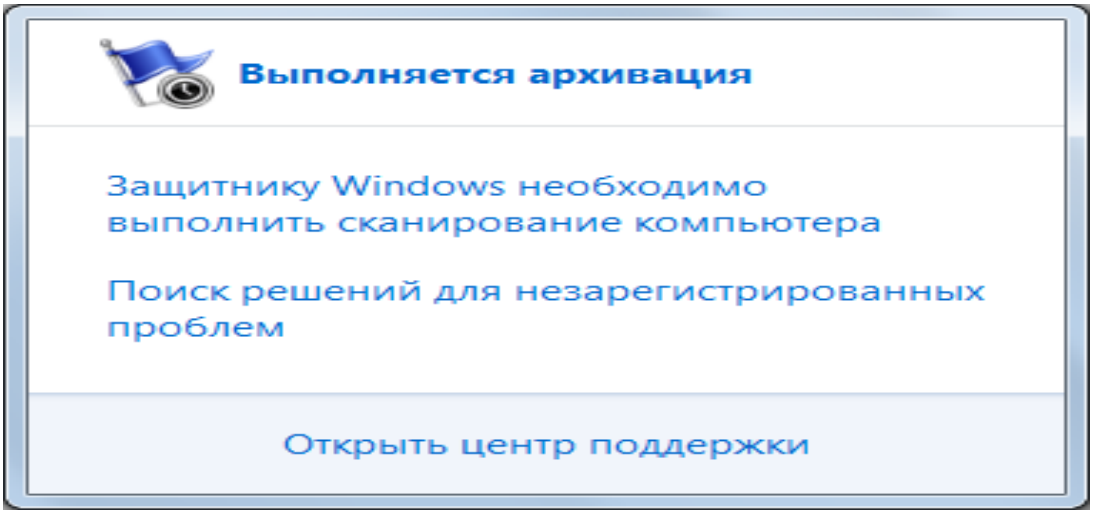


Рис 18 Відкриття центру підтримки

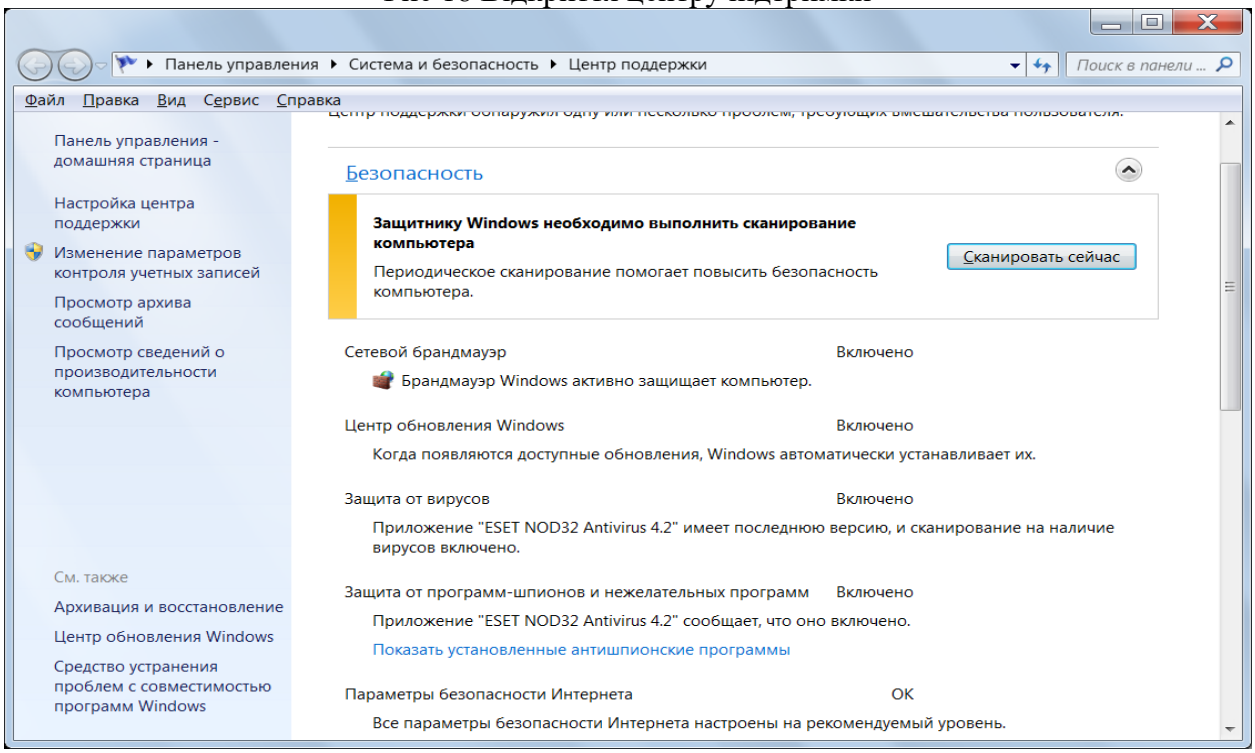


Рис. 19 Вікно запуску захисника Windows

5. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

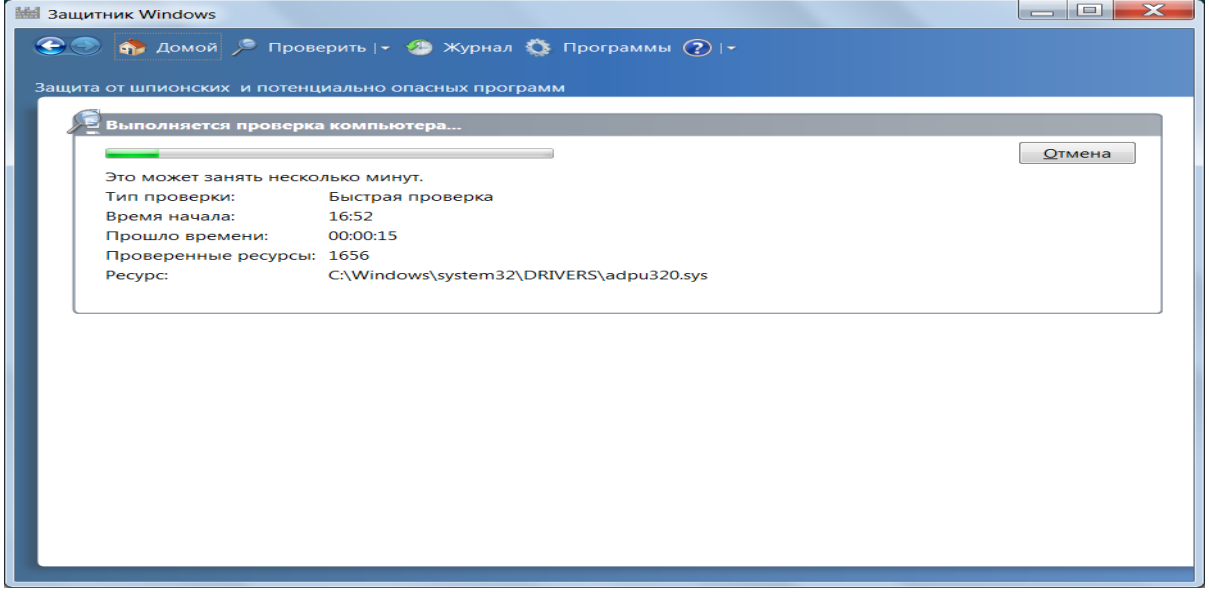


Рис. 20 Вікно захисника Windows

3.5 Видалення або відновлення об'єктів, поміщених в карантин Захисником Windows

Поміщаючи програму в карантин, захисник Windows переміщає її в інше місце на комп'ютері. Тим самим захисник Windows перешкоджає запуску програми (рис. 23), поки вона не буде відновлена або видалена.

1. У меню **Программы** виберіть пункт **Объекты в карантине**.
2. Виберіть команду **Просмотр** для проглядання всіх елементів. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

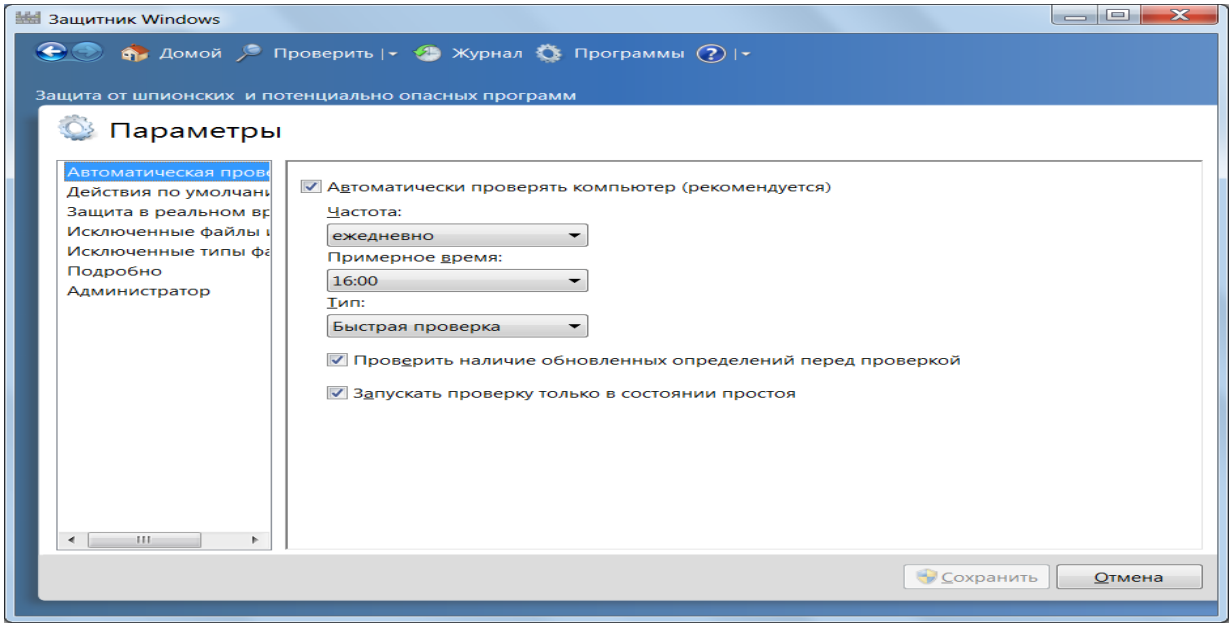


Рис. 21 Захисник Windows встановлення параметрів сканування

1. Проглянете всі об'єкти, а потім натисніть для кожного з них кнопку **Удалить** або кнопку **Восстановить**. Видалення всіх об'єктів, поміщених в карантин, проводиться при натисненні кнопки **Удалить все**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

Примітка. Не відновлюйте програми з критичним або високим рівнем сповіщень, оскільки це може поставити під загрозу конфіденційність і безпеку комп'ютера.

3.6 Додавання і видалення об'єктів із списку дозволених Захисника Windows

Якщо ви довіряєте виявленим захисником Windows програмам, оповіщення захисника Windows про потенційну загрозу конфіденційності або безпеці комп'ютера, яку можуть

представляти ці програми, можна відключити. Для цього відповідні програми слід додати в список дозволених захисника Windows. Щоб ці програми знову перевірялися, їх можна у будь — який час видалити із списку дозволених Захисника Windows командами: Додавання об'єкту в список дозволених, Видалення об'єкту із списку дозволених.

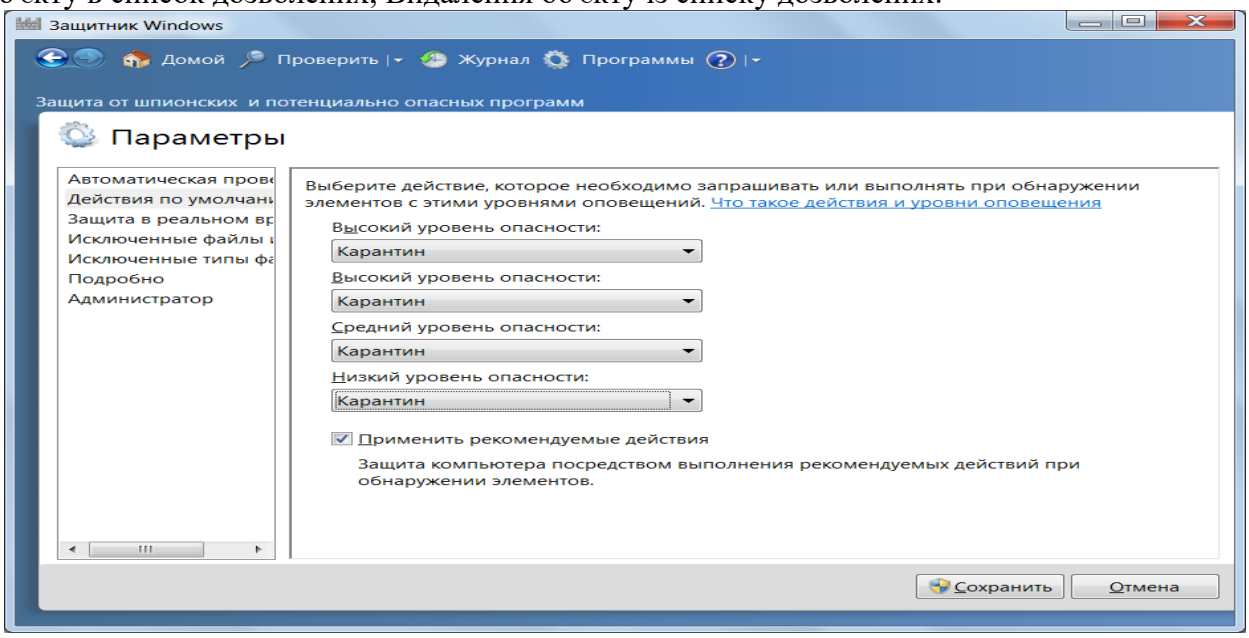


Рис. 22 Встановлення дій в захиснику Windows

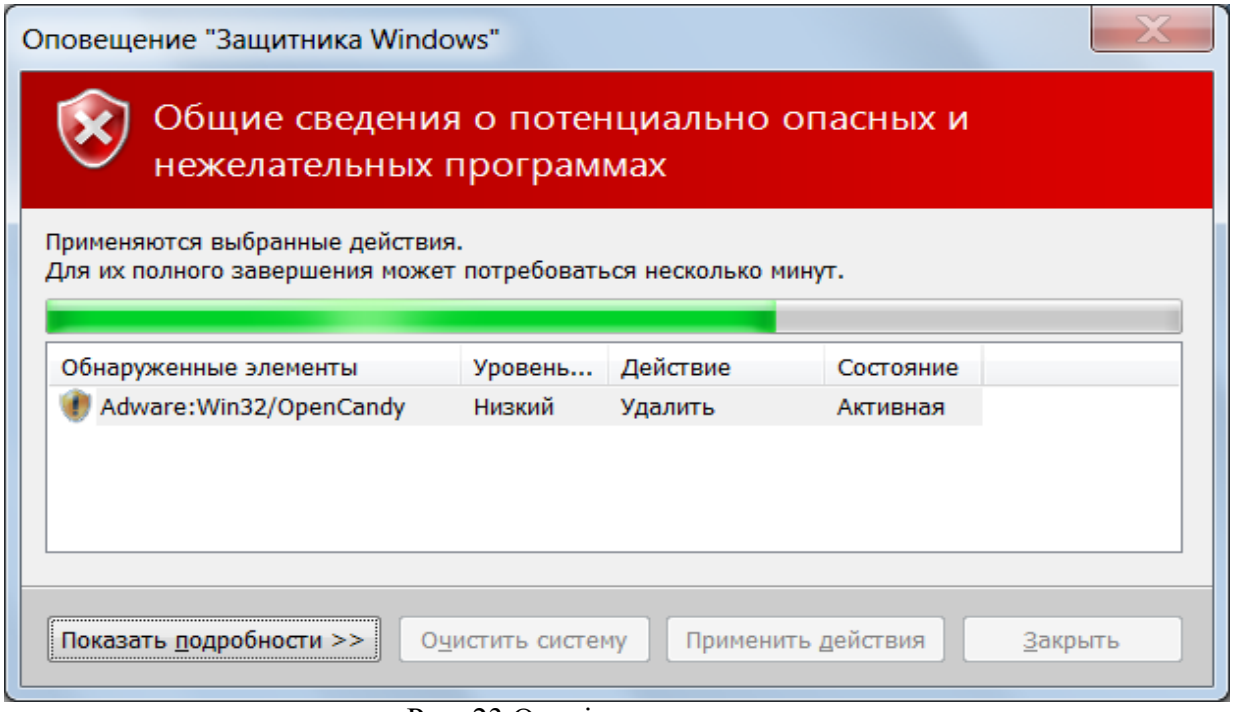


Рис. 23 Оповіщення захисника

3.7 Опис рівнів оповіщення захисника Windows

Рівні оповіщень дозволяють вибрати потрібну дію при виявленні шпигунської програми або потенційно небажаного програмного забезпечення. Хоча захисник Windows може рекомендувати видалити шпигунські програми, це не означає, що всі виявлені ним

програми є шкідливими або небажаними. Таблиця 3 допоможе вибрати потрібну дію при виявленні захисником Windows небажаної програми.

Таблиця 3

Опис рівнів оповіщень

Рівень оповіщення	Опис	Дії
Критичний або високий	Програми, які можуть виконувати збір особистих даних і негативно впливати на конфіденційність або можуть пошкодити комп'ютер, наприклад, шляхом збору інформації або зміни параметрів системи, зазвичай без вашого відома або згоди.	Негайно видаліть це програмне забезпечення.
Середній рівень	Програми, які можуть вплинути на конфіденційність і внести зміни, що можуть негативно позначитися на продуктивності системи, наприклад, шляхом збору особистих даних або зміни параметрів системи.	Ознайомтеся з описом причини, за якою ця програма була визнана сумнівною. Якщо вам не подобається, як працює ця програма, або ви не знаєте її видавця або не довіряєте йому, рекомендується заблокувати або видалити цю програму.
Низький рівень	Небажані програми, які можуть виконувати збір відомостей про користувача або комп'ютер змінювати характер роботи системи, але що працюють відповідно до ліцензійної угоди, яка відображалася під час їх установки.	Зазвичай такі програми не представляють небезпеку, якщо вони не були встановлені без вашого відома. Якщо ви не упевнені, видаляти певну програму чи ні, вивчіть докладну інформацію або перевірте, хто є її видавець.

3.8 Перегляд і очищення журналу Захисника Windows

У журналі відображається опис усіх дій, що застосовувалися до шпигунських інших потенційно небажаних програм, які захисник Windows виявив на комп'ютері.

Виберіть пункт **Журнал** і виконайте наступні дії:

Перегляд журналу проводиться командою **Осмотр**. З появою запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

Щоб вилучити всі елементи списку, натисніть кнопку **Очистить журнал**. З появою запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

4 Використання центру оновлення Windows.

Корпорація Microsoft регулярно пропонує важливі оновлення Windows для захисту комп'ютера від нових вірусів і інших погроз безпеці. Включіть автоматичне оновлення для

швидкого отримання оновлень. В цьому випадку не потрібно хвилюватися, що критичні оновлення Windows можуть бути пропущені.

Оновлення завантажуються у фоновому режимі при підключенні до Інтернету за умовчанням в 03:00, якщо не заданий інший час. Якщо користувач вимикає комп'ютер раніше, можна встановити оновлення перед виключенням. Інакше Windows встановить оновлення наступного разу при запуску комп'ютера.

Включення автоматичного оновлення

1. Зайдіть в **Панель управления**.

2. Клацніть по значку **Система и безопасность**. Відкриється вікно списку команд даного підрозділу (рис. 24).

3. Виберіть команду **Центр поддержки** (рис. 25).

4. Виберіть команду **Настройка центра поддержки** (рис. 26).

5. Виберіть команду **Параметры центра обновления** (рис. 27).

5.У групі **Важные сообщения** , відберіть потрібні параметри.

Центр підтримки повідомляє користувача про всі події, що вимагають його уваги. В центрі підтримки перераховані важливі повідомлення про параметри безпеки і обслуговування комп'ютера, які вимагають уваги користувача. Центр підтримки перевіряє декілька компонентів комп'ютера, пов'язаних з обслуговуванням і забезпеченням безпеки, які указують на загальну продуктивність комп'ютера.

При зміні стану компоненту (наприклад, закінчився термін дії антивірусної програми), що перевіряється, Центр підтримки відправляє користувачеві повідомлення, що відображається в області повідомлень на панелі завдань. Залежно від ступеня серйозності повідомлення міняється колір стану компоненту, і на підставі цього рекомендується зробити відповідні дії.

Червоним кольором помічені важливі повідомлення, що свідчать про значні проблеми, які необхідно усунути щонайшвидше. Як приклад можна привести антивірусну програму, що вимагає оновлення. Жовтим кольором позначені завдання, що рекомендуються, необхідність виконання яких потрібно розглянути користувачеві. Наприклад, завдання, що рекомендуються, з обслуговування.

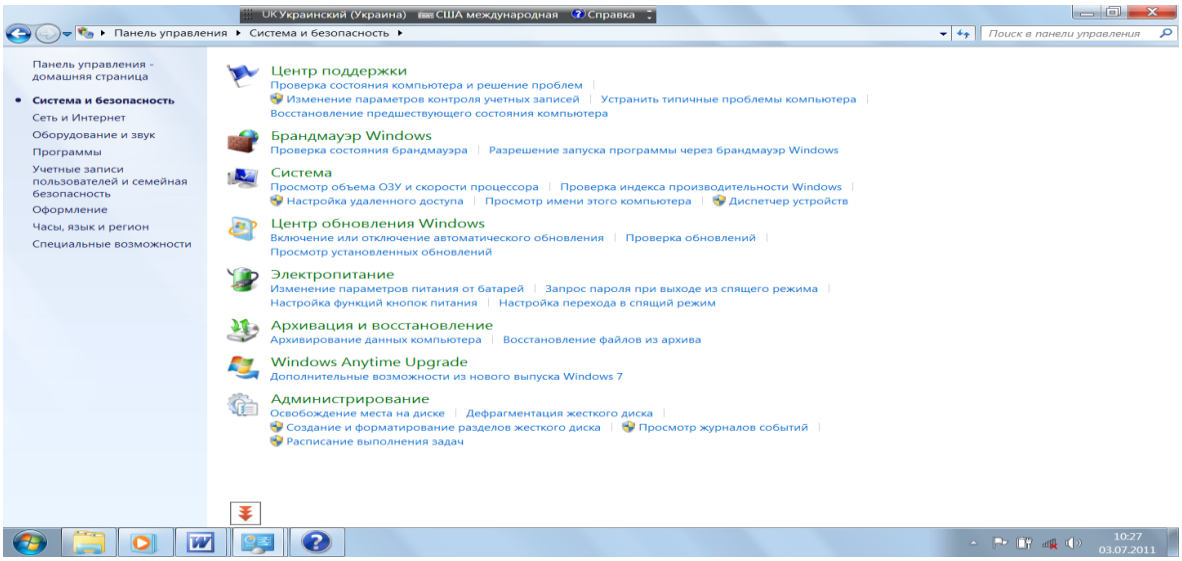


Рис. 24 Вікно списку команд

Рекомендується перевіряти стан всіх перерахованих в списку компонентів, оскільки при такому підході можна дізнатися про погрози безпеці завчасно.

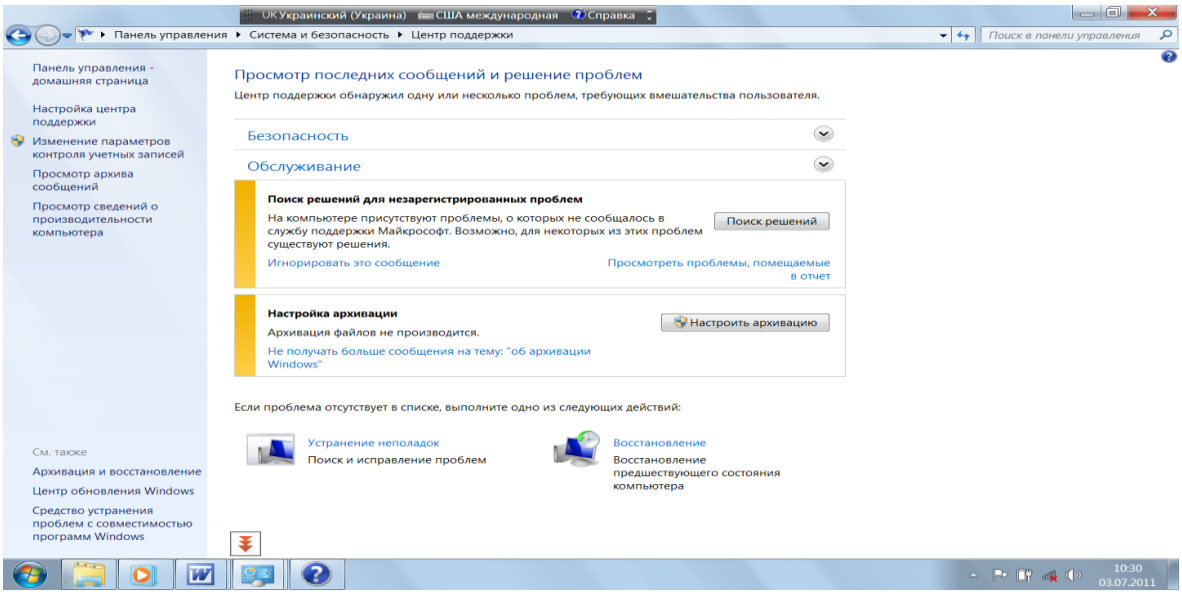


Рис. 25 Центр підтримки

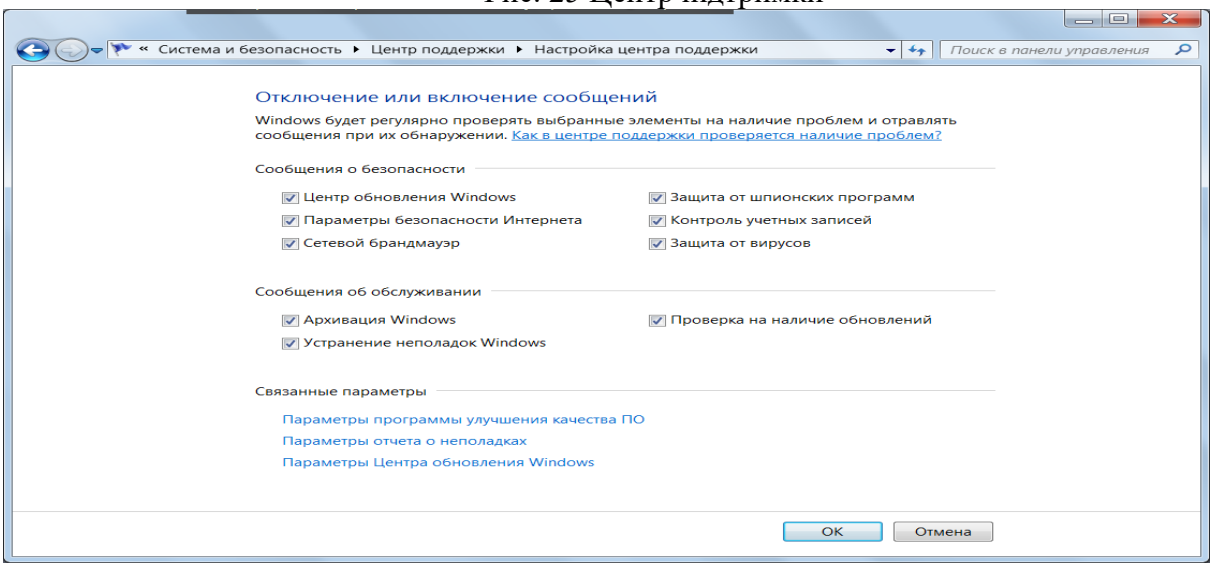


Рис. 26 Вікно налагодження центру підтримки

Якщо на сторінці **Изменение параметров Центра поддержки** прапорець для компоненту знятий, повідомлення відображатися не будуть і стан компоненту в центрі підтримки буде недоступний.

Щоб змінити вид проблем, які відображаються в центрі підтримки, клацніть **Изменить параметры Центра поддержки,** а потім – **Параметры отчетов о проблемах**. На сторінці **Изменения параметров отчетов о проблемах** виберіть об'єм даних, що відправляються, і встановіть періодичність перевірки на наявність нових рішень, а потім натисніть кнопку **ОК**.

Примітка. В центр підтримки можна зайти з панелі задач (рис. 28), клацнувши по ярлику **Устранение проблем**. Відібрати в цьому вікні команду **Центр поддержки**.

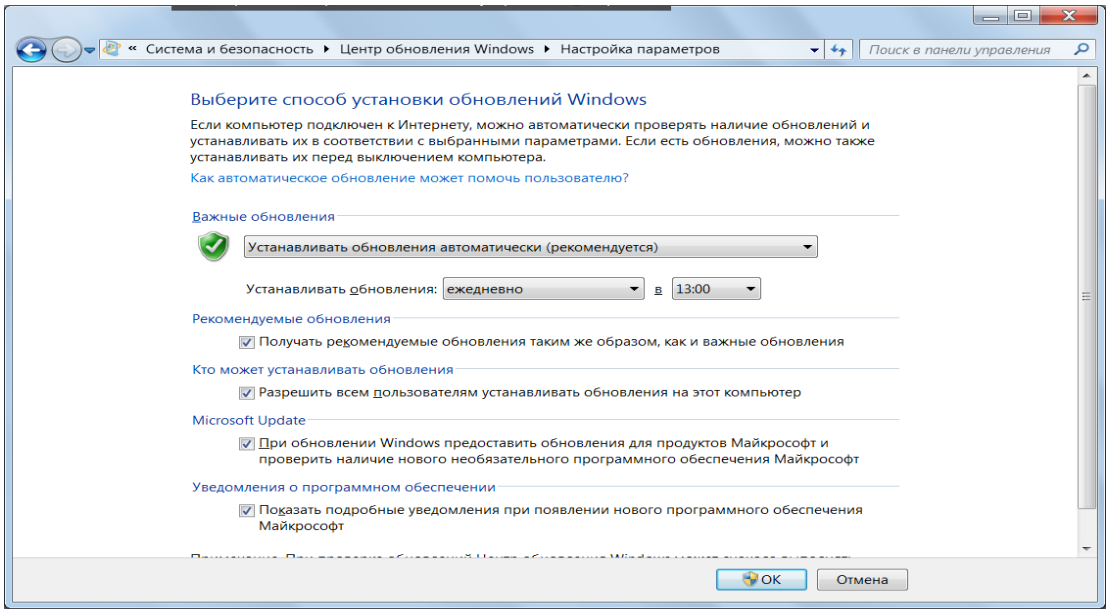


Рис. 27 Параметри центра оновлення

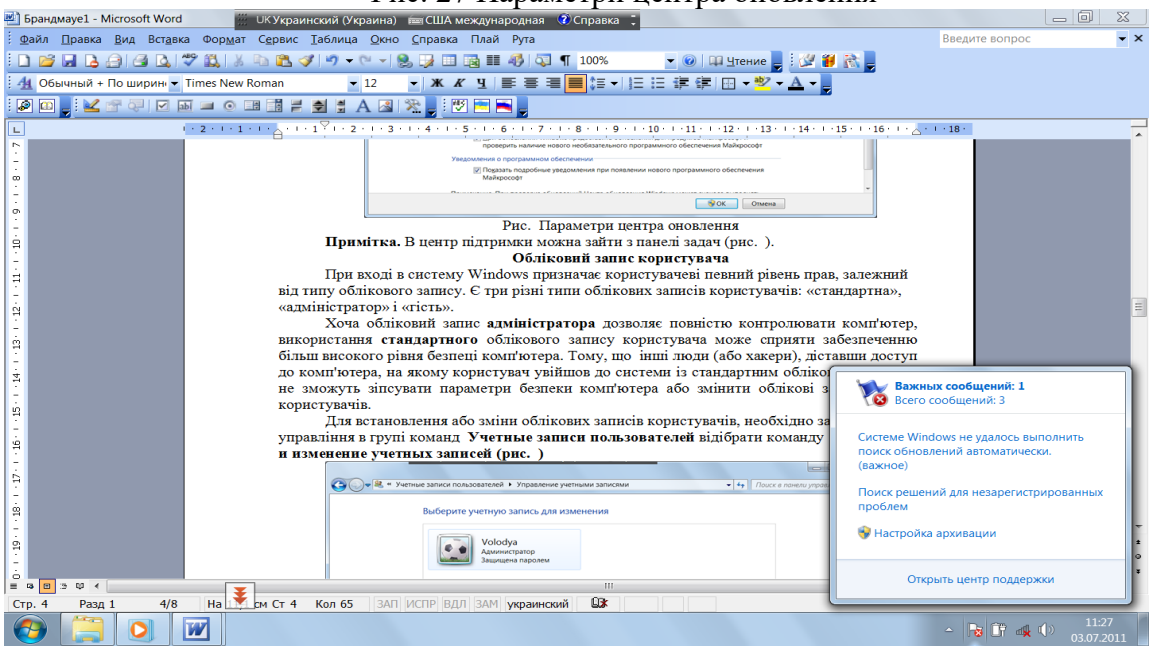


Рис. Параметри центра оновлення

Примітка. В центр підтримки можна зайти з панелі задач (рис.).

Обліковий запис користувача

При вході в систему Windows призначає користувачеві певний рівень прав, залежний від типу облікового запису. Є три різні типи облікових записів користувачів: «стандартна», «адміністратор» і «гість».

Хоча обліковий запис **адміністратора** дозволяє повністю контролювати комп'ютер, використання **стандартного** облікового запису користувача може сприяти забезпеченню більш високого рівня безпеці комп'ютера. Тому, що інші люди (або хакери), дістався доступ до комп'ютера, на якому користувач увійшов до системи із стандартним обліко не зможуть зіпсувати параметри безпеки комп'ютера або змінити облікові з користувачів.

Для встановлення або зміни облікових записів користувачів, необхідно за управління в групі команд **Учетные записи пользователей** відібрати команду **и изменение учетных записей (рис.)**

Рис. 28 Вікно усунення проблем

5. Хід роботи

1. Проведіть зміну пароля Windows
2. Проведіть створення диску скидання пароля
3. Проведіть зміну способу запиту пароля при виході комп'ютера зі сплячого режиму
4. Проведіть включення і виключення брандмауера Windows
5. Проведіть включення і виключення мережевого виявлення
6. Проведіть відновлення параметрів брандмауера Windows
7. Проведіть дозвіл програмі MS Word встановлювати зв'язок через брандмауер Windows
8. Проведіть оновлення антивірусного програмного забезпечення встановленого на комп’ютері
9. Проведіть сканування комп’ютера на наявність вірусів за допомогою антивірусного програмного забезпечення встановленого на комп’ютері

10. Проведіть включення і відключення захисника Windows
11. Проведіть сканування комп’ютера за допомогою захисника Windows
12. Проведіть перегляд і очищення журналу Захисника Windows
13. Проведіть оновлення Windows

6. Контрольні питання

1. Охарактеризуйте поняття надійного пароля.
2. Як проводиться зміна пароля Windows?
3. Як проводиться створення диску скидання пароля?
4. Як проводиться зміна способу запиту пароля при виході комп'ютера зі сплячого режиму?
5. Як проводиться включення і виключення брандмауера Windows?
6. Як проводиться включення і виключення мережевого виявлення?
7. Як проводиться відновлення параметрів брандмауера Windows?
8. Як проводиться дозвіл програмі встановлювати зв'язок через брандмауер Windows?
9. Як проводиться відкриття порту в брандмауері Windows?
10. Як проводиться оновлення антивірусного програмного забезпечення?
11. Як проводиться сканування комп’ютера на наявність вірусів за допомогою антивірусного програмного забезпечення встановленого на комп’ютері?
12. Як проводиться включення і відключення захисника Windows?
13. Як проводиться сканування комп’ютера за допомогою захисника Windows?
14. Як проводиться перегляд і очищення журналу Захисника Windows?
15. Як проводиться оновлення Windows?
16. Охарактеризуйте засоби захисту інформації в комп'ютері під час застосування операційної системи Windows 7.
17. Як проводиться захист комп'ютера за допомогою пароля?
18. Яке призначення брандмауера? Які параметри захисту можна налагодити?
19. Як провести захист від вірусів?
20. Як провести захист від шпигунських і інших шкідливих програм?
21. Як використати центр оновлення Windows?

Лабораторна робота 5
Захист інформації під час застосування операційної системи Windows 7

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в операційній системі Windows 7.

Ознайомитись з рівнями захисту комп'ютера, можливістю надання прав різним категоріям користувачів, використання фільтрів, встановлення їх параметрів, процесом шифрування, створенням сертифікату, архівацією системи та її відновленням, захистом дисків.

План

1. Теорія

1.1 Контроль облікових записів користувачів.

При вході в систему Windows призначає користувачеві певний рівень прав, залежний від типу облікового запису. Є три різні типи облікових записів користувачів: стандартний, адміністратор і гість.

Потрібно створити обліковий запис користувача для кожної людини, що користується комп'ютером, так щоб у кожного було індивідуальне оточення. Наприклад, кожна людина може встановити свій власний фон робочого столу і заставку. Облікові записи користувачів також можуть бути використані для визначення, до яких програм і файлів користувачі можуть дістати доступ і які зміни вони можуть провести на комп'ютері. Застосування облікових записів дозволяє декільком користувачам працювати на одному комп'ютері з використанням власних файлів, тек і параметрів. Доступ до облікового запису забезпечується використанням імені користувача і паролю.

Іноді групи користувачів називають групами безпеки. Обліковий запис може входити в одну або декілька груп. Двома найбільш поширеними групами користувачів є група стандартних користувачів і група адміністраторів. Обліковий запис часто називають на ім'я груп, в яку вона входить (наприклад, обліковий запис, що входить до групи звичайних користувачів, називається звичайний обліковий запис).

Використовуючи обліковий запис адміністратора, можна створювати нові групи користувачів, переміщувати облікові записи з однієї групи в іншу, додавати облікові записи в різні групи або видаляти їх. При створенні нової групи користувачів можна самостійно визначити, які права до неї будуть застосовані. Обліковий запис адміністратора є обліковим записом користувача, за допомогою якого можна вносити зміни, до записів інших користувачів комп'ютера. Адміністратори можуть міняти параметри безпеки, встановлювати програмне забезпечення і устаткування, а також вони мають доступ до всіх файлів на комп'ютері.

Хоча обліковий запис адміністратора дозволяє повністю контролювати комп'ютер, використання стандартного облікового запису користувача може сприяти забезпеченню більш високого рівня безпеці комп'ютера. Тому, що інші люди (або хакери), діставши доступ до комп'ютера, на якому користувач увійшов до системи із стандартним обліковим записом, не зможуть зіпсувати параметри безпеки комп'ютера або змінити облікові записи інших користувачів.

Контроль облікових записів (UAC) використовується для запобігання несанкціонованим змінам на комп'ютері. При спробі внесення змін, що вимагають прав адміністратора, виводиться відповідне повідомлення контролю облікових записів. Зміни такого роду можуть вплинути на безпеку комп'ютера і параметри інших користувачів комп'ютера. Щоб забезпечити максимальну безпеку комп'ютера, рекомендується включити контроль облікових записів.

1. Необхідно зайти в **Панель управления** в групі команд **Учетные записи пользователей** відібрати команду **Параметры контроля учетных записей**.

2. Виконати одну з наступних дій:

- щоб відключити контроль облікових записів, перемістіть повзунок в положення **Никогда не уведомлять** і натисніть кнопку **ОК**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження. Контроль облікових записів буде відключений після перезавантаження комп'ютера;
- щоб включити контроль облікових записів, перемістіть повзунок в положення, відповідне необхідній частоті повідомлення, і натисніть кнопку **ОК**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

Обліковий запис користувача не дозволяє іншим користувачам, що використовують звичайний обліковий запис, проглядати його файли. Проте при цьому користувачі з обліковим записом адміністратора можуть проглядати файли інших користувачів на комп'ютері. Якщо на комп'ютері є інші облікові записи адміністратора, то замість використання дозволів можна захищати файли, шифруючи їх за допомогою файлової системи (EFS).

Встановлення або зміни облікових записів користувачів виконуються шляхом виконання команд в панелі управління в групі команд **Учетные записи пользователей\Добавление и изменение учетных записей** (рис. 1).

Тип облікового запису відображається під ім'ям користувача.

Для створення нового облікового запису відберіть команду **Создание новой учетной записи** (рис. 2). Відберіть потрібні параметри та введіть назву облікового запису. Введіть команду **Создание учетной записи**. З'явиться відповідний обліковий запис (рис. 3).

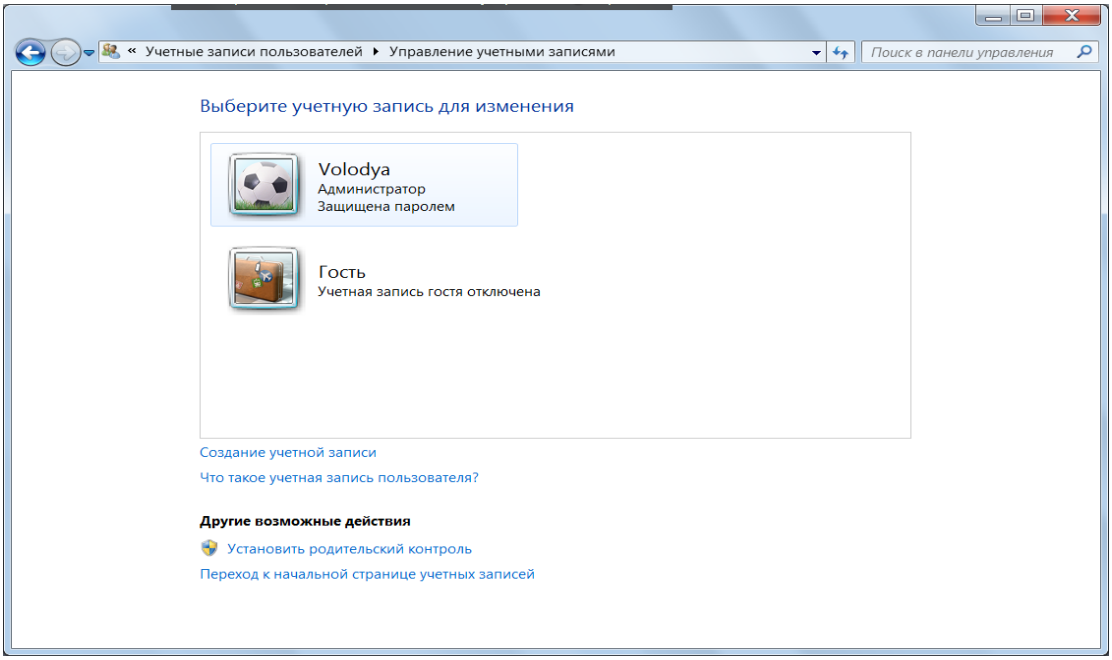


Рис. 1 Вікно зміни облікових записів користувачів

Зміна облікового запису виконується шляхом клацання основною клавішею миші по потрібному записі та відбором потрібної команди (рис. 4). В разі відбору команди, наприклад, **Удалить учетную запись** з'явиться вікно яке вимагає підтвердження команди (рис. 5).

1.1 Створення групи користувачів

1. Відкрийте **Панель управления.** Відберіть групу **Учетные записи пользователей**.
2. У лівій області виберіть компонент **Локальные пользователи и группы**.

Якщо компонент **Локальные пользователи и группы** не відображається

3. Двічі клацніть теку **Группы**.
4. Виберіть елемент **Действие**, а потім команду **Создать группу.**
5. Введіть **Имя группы и описание**.
6. Клацніть **Добавить** і введіть **Имя учетной записи**.
7. Клацніть **Проверить имя** і натисніть кнопку **ОК**.
8. Натисніть кнопку **Создать**.

Включення і відключення безпечного входу в систему

Важливо тримати комп'ютер настільки захищеним, наскільки це можливо. Одним із способів добитися цього є безпечний вхід в систему, при якому для входу в систему потрібно натиснути клавіші **Ctrl+Alt+Delete.** Використання безпечного входу в систему надає ще один рівень безпеки, що дозволяє упевнитися, що відображається справжній екран входу в Windows. Якщо безпечний вхід в систему включений, інші програми (такі як віруси або шпигунські програми) не можуть перехопити ім'я користувача і пароль під час їх введення.
Відкрийте компонент **Учетная запись опытного пользователя** . При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження. Виберіть вкладку **Дополнительно**, встановіть прапорець Требовать нажатия **Ctrl+Alt+Delete** і потімнатисніть кнопку **ОК**.

1.2 Використання фільтру Microsoft SmartScreen.

Фільтр Microsoft SmartScreen – це можливість в Internet Explorer, що допомагає виявляти підроблені web – вузли, а також web – вузли, які поширюють шкідливе програмне забезпечення. Підроблені web – вузли – це вузли, що підробляють надійні або відомі web – вузли, з метою обману користувачів

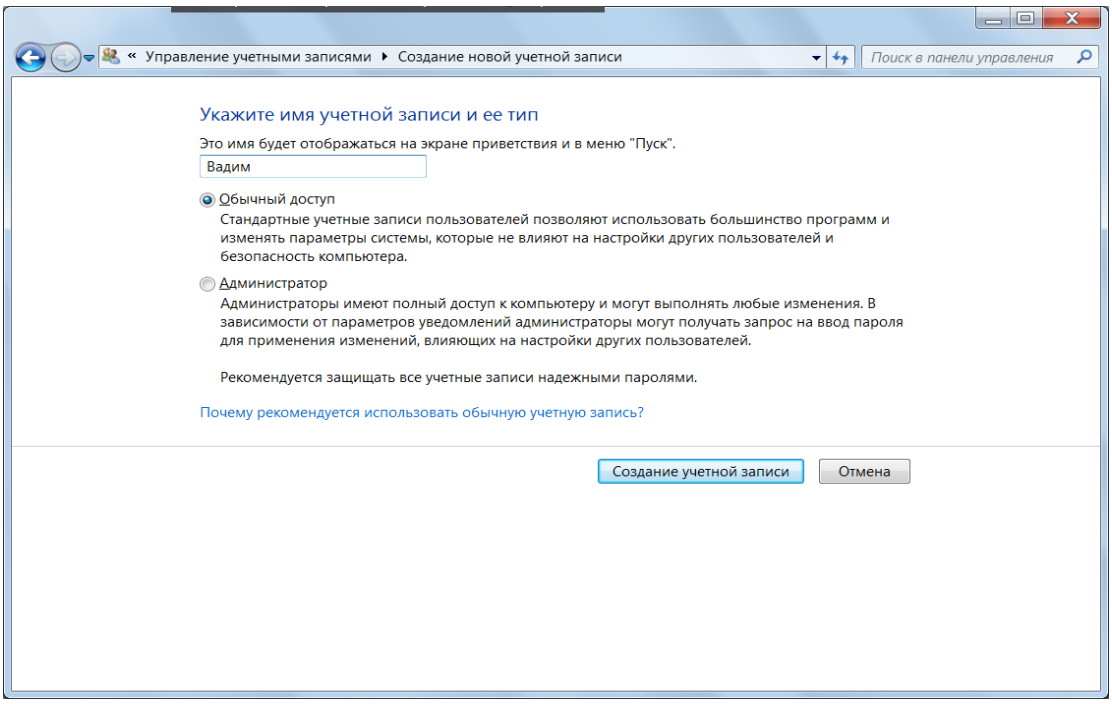


Рис. 2 Вікно відбору параметрів облікового запису

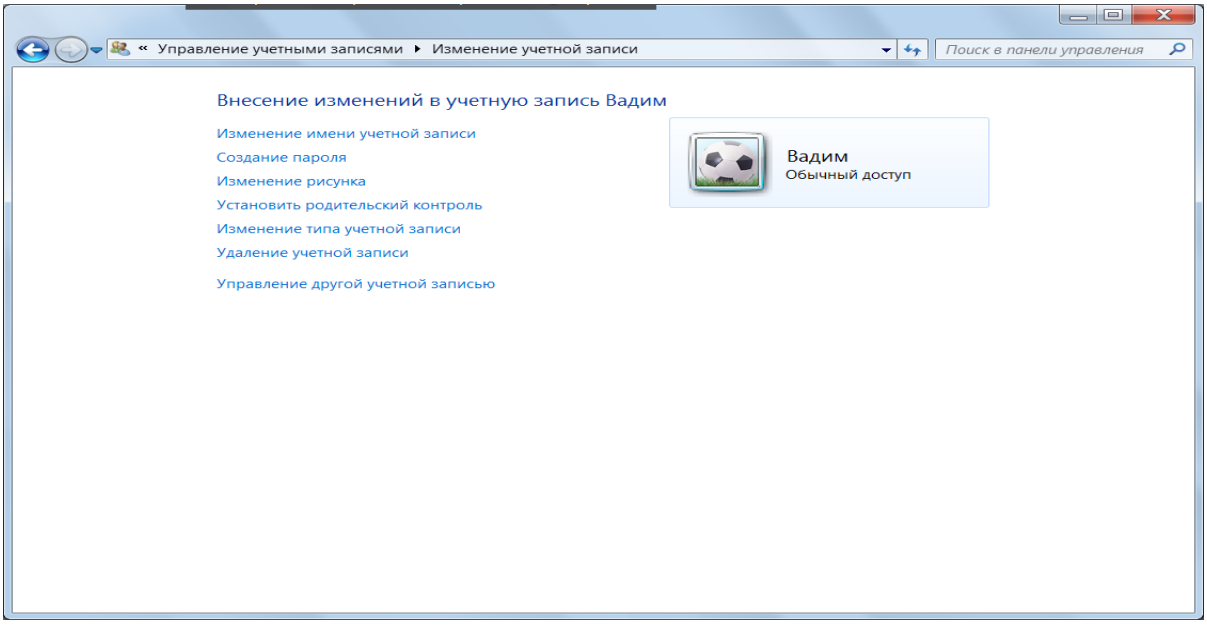


Рис. 3 Вікно з новим обліковим записом

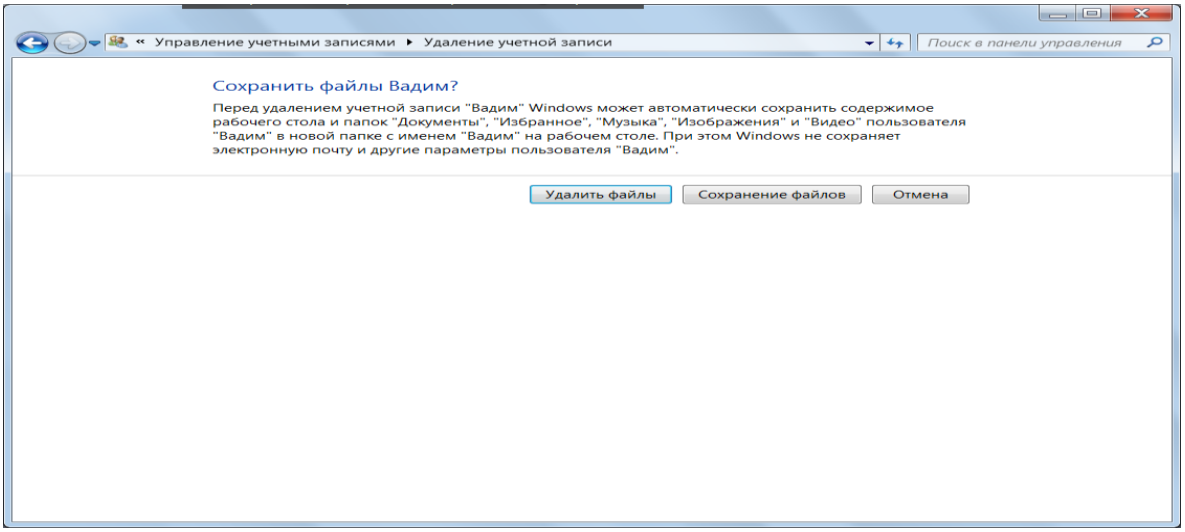


Рис. 4 Відбір потрібної команди для зміни облікового запису

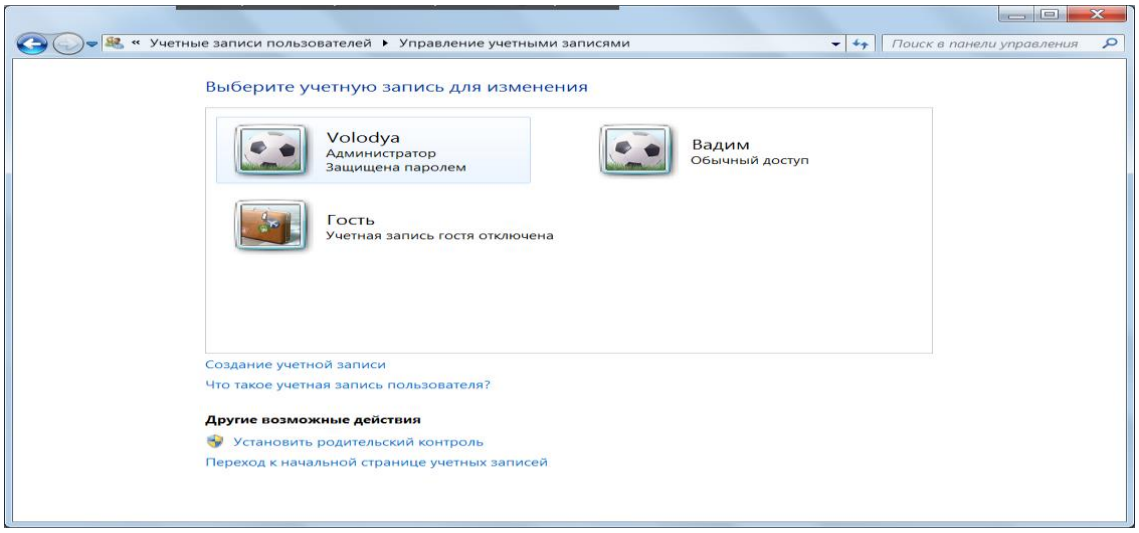


Рис. 5 Відбір облікового запису

комп'ютерів і розкриття особистої або фінансової інформації. Шкідливі web – вузли розповсюджують програмне забезпечення, яке може атакувати комп'ютер або викрасти особисті відомості.

Під час проглядання web – сторінок фільтр SmartScreen запускається у фоновому режимі і (з дозволу користувача) відправляє адреси відвіданих вузлів в службу Microsoft SmartScreen для порівняння із списками відомих підроблених і шкідливих вузлів. Якщо фільтр SmartScreen виявляє, що web – вузол, який проглядається, знаходиться в списку відомих підроблених або шкідливих web – вузлів, Internet Explorer відобразить web – сторінку блокування, а адресний рядок буде забарвлений в червоний колір. На сторінці блокування можна вибрати обхід заблокованого web – вузла і перейти на домашню сторінку або продовжити проглядання заблокованого вузла, хоча це і не рекомендується. Якщо ухвалено рішення продовжити проглядання заблокованого web – вузла, адресний рядок буде як і раніше забарвлений в червоний колір.

Для захисту конфіденційних відомостей інформація, що відправляється у web – сервер – службу SmartScreen, передається в зашифрованому форматі за захищеним протоколом HTTPS. Ці відомості не зберігають IP – адреси користувача або іншої особистої інформації, а

також не використовуватимуться для ідентифікації, зв'язку або відправки рекламних матеріалів користувачеві.

1.3 Відкриття файлу, якщо відмовлено в доступі

Якщо при спробі відкрити файл виводиться повідомлення про відмову в доступі, спробуйте виконати наступні дії.

Перевірте дозволи для файлу або теки, в якій зберігається файл. Це можна зробити таким чином.

1. Клацніть правою кнопкою миші файл або теку і виберіть команду **Свойства**.
2. Перейдіть на вкладку **Безопасность**.
3. У розділі **Группы или пользователи** клацніть ім'я для відображення наявних дозволів.

Відкриття файлу відбувається при наявності дозволу на читання.

2. Шифрування в Windows

Шифрування – це спосіб підвищення безпеки повідомлення або файлу, при якому їх вміст перетвориться так, що воно може бути прочитане тільки користувачем, з відповідним ключем шифрування для розшифрування вмісту. Наприклад, при здійсненні покупки в Інтернеті операції (такі як адреса, телефон, номер кредитної карти) зазвичай зашифровуються з метою безпеки.

Важливо регулярно архівувати файли і параметри, щоб мати можливість відновити їх у разі зараження комп'ютера вірусом або збою устаткування.

2. 1 Деякі ключові властивості системи шифрування EFS

- шифрування — проста дія; для його включення досить встановити прапорець у властивостях файлу або теки у вкладці **Общие** команда **Другие**;
- можна вказати, кому саме дозволяється читати ці файли;
- файли шифруються, коли вони закриваються, але при відкритті вони автоматично готові до використання;
- якщо шифрувати файл більше немає необхідності, зніміть прапорець у властивостях файлу.

Примітка. Файлова система EFS у випусках Windows 7 Початкова, Windows 7 Домашня базова і Windows 7 Домашня розширена підтримується частково. У цих випусках ОС Windows за наявності ключа шифрування або сертифікату можна виконувати наступні дії.

- дешифрувати файли, запускаючи файл Cipher.exe у вікні командного рядка (для досвідчених користувачів);
- змінювати зашифрований файл;
- копіювати зашифрований файл як розшифрований на жорсткий диск комп'ютера;
- імпортувати сертифікати і ключі системи EFS;
- створювати резервні копії EFS – сертифікатів і ключів, запускаючи файл Cipher.exe у вікні командного рядка (для досвідчених користувачів).

2. 2 Захист файлів за допомогою шифрування дисків BitLocker

Шифрування дисків BitLocker використовується для захисту всіх файлів, що зберігаються на диску зі встановленою ОС Windows (диск операційної системи) і на дисках, які не знімаються (наприклад, внутрішніх жорстких дисках), а також, для захисту всіх файлів, що зберігаються на дисках, які не знімаються (наприклад, зовнішніх жорстких дисках або USB – устроях, наприклад, флеш – пам'яті).

На відміну від шифрувальної файлової системи (EFS), що дозволяє зашифровувати окремі файли, BitLocker шифрує диск цілком. Користувач може входити в систему і працювати з файлами як завжди, а BitLocker заважатиме зловмисникам, що намагаються дістати доступ до системних файлів для пошуку паролів, а також до диску шляхом витягання його з даного комп'ютера і установлення в іншій.

BitLocker автоматично шифрує всі файли, що додаються на зашифрований диск. Файли будуть зашифровані тільки при зберіганні на зашифрованому диску. При їх копіюванні на інший диск вони будуть розшифровані. При наданні загального доступу до файлів за мережею вони будуть зашифровані на зашифрованому диску, але авторизовані користувачі зможуть діставати до них доступ звичайним способом.

При шифруванні диску з ОС BitLocker перевіряє комп'ютер при завантаженні на наявність можливих погроз безпеки (наприклад, змін в BIOS або файлах завантаження). При виявленні загрози безпеці BitLocker заблокує диск з ОС. Щоб розблоковувати його, буде потрібно спеціальний ключ відновлення BitLocker. Цей ключ та його копію треба створити при першому запуску BitLocker. Інакше доступ до файлів може бути втрачений. Якщо комп'ютер оснащений довіреним платформним модулем (TPM), BitLocker використовує його для запечатування ключів розблокування зашифрованого диску з ОС. При завантаженні комп'ютера BitLocker запрошує у довіреного платформного модуля ключі для доступу до диску і розблоковує його.

Зашифровані диски можна розблоковувати за допомогою пароля або смарт – карти – налагодити автоматичне розблокування дисків при вході в систему. BitLocker завжди можна відключити або тимчасово, або на постійній основі (розшифрувавши диск).

Примітка. Можливість шифрувати дані на дисках з використанням шифрування BitLocker доступна не у всіх випусках Windows.

Стандартом шифрування AES є алгоритм шифрування, прийнятий урядом США в 2001 році. AES забезпечує надійніше шифрування, ніж його попередник, стандарт шифрування даних DES. У даній версії Windows використовується стандарт – AES.

Що робити, якщо втрачений ключ шифрування файлу?

Якщо при спробі відкрити зашифрований файл з'являється повідомлення про те, що доступ до нього заборонений, це може свідчити про пошкодження або відсутність ключа шифрування. В цьому випадку слід використовувати резервну копію ключа шифрування або, якщо комп'ютер входить в домен, сертифікат відновлення, повинен бути присутнім у системного адміністратора. Якщо сертифікату відновлення або резервної копії ключа немає, доступ до файлів неможливий.

3 Архівація образу системи та файлів і тек

Програма архівації Windows дозволяє створювати копії файлів даних для всіх користувачів комп'ютера. Можна надати Windows вибір об'єктів для резервного копіювання або самостійно вибрати окремі теки, бібліотеки і диски для архівації. За умовчанням резервні копії створюються регулярно, відповідно до розкладу. Можна змінити цей розклад і уручну створити резервну копію у будь – який момент часу. Коли програма архівації Windows налагоджена, Windows відстежує нові і змінені файли і теки і додає їх в резервну копію.

Програма архівації Windows дозволяє створити образ системи, який є точним образом диску. Образ системи також містить Windows системні параметри, програми і файли. Образ системи можна використовувати для відновлення вмісту комп'ютера у разі відмови жорсткого диску або комп'ютера.

Хоча такий тип резервного копіювання включає особисті файли користувача, рекомендується регулярно створювати резервні копії файлів за допомогою програми

архівації Window, щоб при необхідності відновити окремі файли і теки. Налагодивши архівацію файлів за розкладом, можна вказати, чи потрібно включати образ системи. Цей образ системи містить тільки диски, необхідні для запуску Windows. Якщо потрібно включити додаткові диски даних, можна створити образ системи вручну.

1.Відкрийте **Панель управления**.

2. В списку команд **Система и безопасность** введіть команду **Архивация и восстановление** (рис. 6).

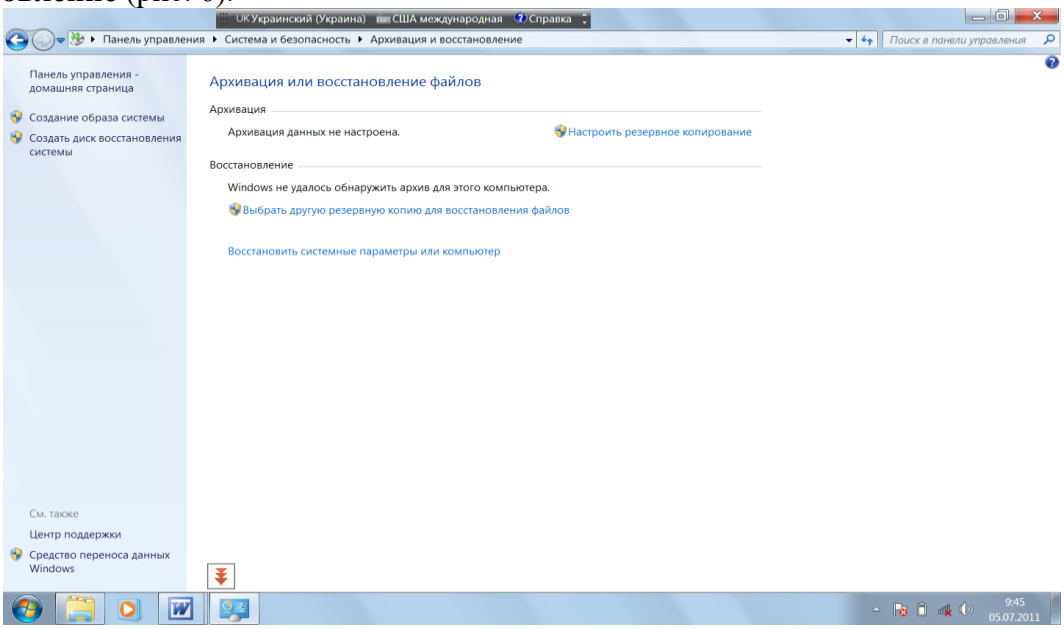


Рис. 6 Вікно архівації

2. Введіть команду **Настроить резервное копирование** (рис. 7).
3. Виберіть місце майбутнього розташування архівів (рис. 8).
4. Введіть команду **Далее** (рис. 9).
5. Відберіть потрібні параметри (параметр **Предоставить мне выбор** — для вибору об'єктів архівування).
6. Введіть команду **Далее** (рис. 10).
7. Відберіть потрібні параметри архівації, наприклад, час (рис. 11).
8. Введіть команду **Сохранить параметры и запустить архивацию** (рис. 12).

3.1 Видалення старих резервних копій файлів

Щоб видалити старі резервні копії файлів, в розділі Архів файлів даних виберіть команду **Просмотреть архивы**.

Потім можна вибрати резервні копії файлів, які потрібно видалити, щоб звільнити дисковий простір. Видалення запису в списку не вплине на інші резервні копії. Якщо потрібно, можна видалити всю резервну копію.

Щоб змінити об'єм простору, який використовується архівними образами системи, в розділі **Образ системы** виберіть **Изменить параметры**. Потім можна задати в Windows **Сохранение старих архивных образов системы** або тільки **Последнего образа**.

3.2 Проглядання вмісту резервної копії та відновлення файлів

Вміст резервної копії можна проглянути за допомогою майстра відновлення файлів.

1. Зайдіть в **Архивация и восстановление**.
2. Виконайте одну з наступних дій:

- для проглядання ваших файлів виберіть **Восстановить мои файлы**;

- для проглядання файлів всіх користувачів виберіть **Восстановить файлы всех пользователей.**

При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

Примітка. Відновити файли можна клацнувши по архіву та відібравши відповідні команди (рис. 13).

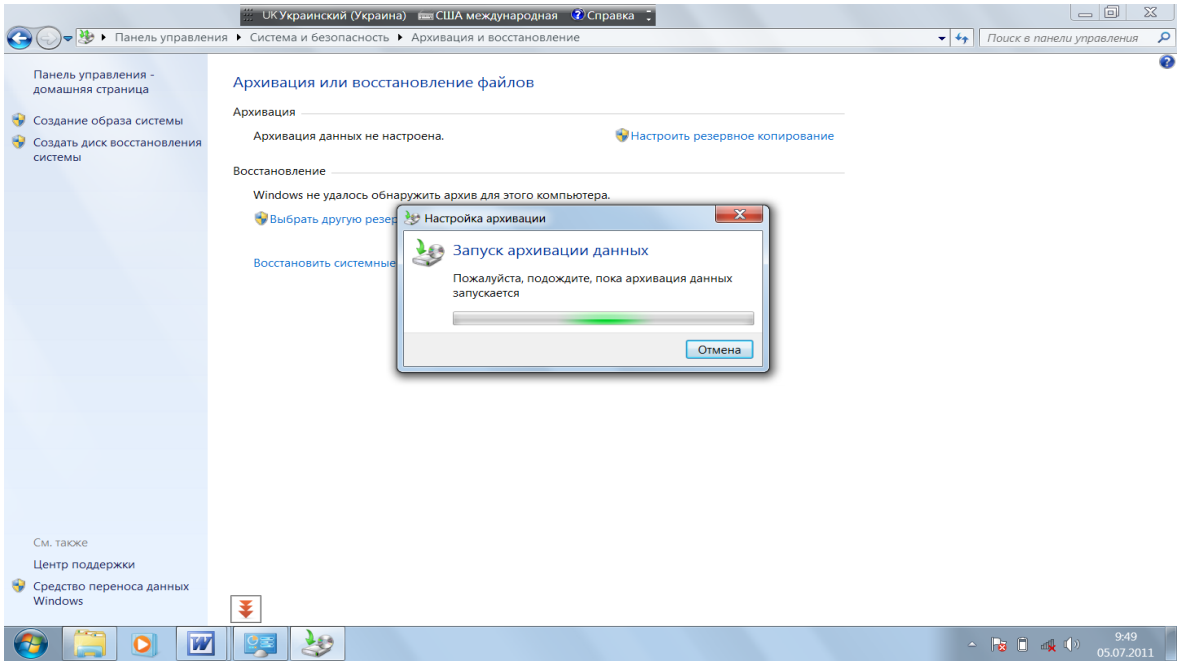


Рис. 7 Запуск майстра резервного копіювання

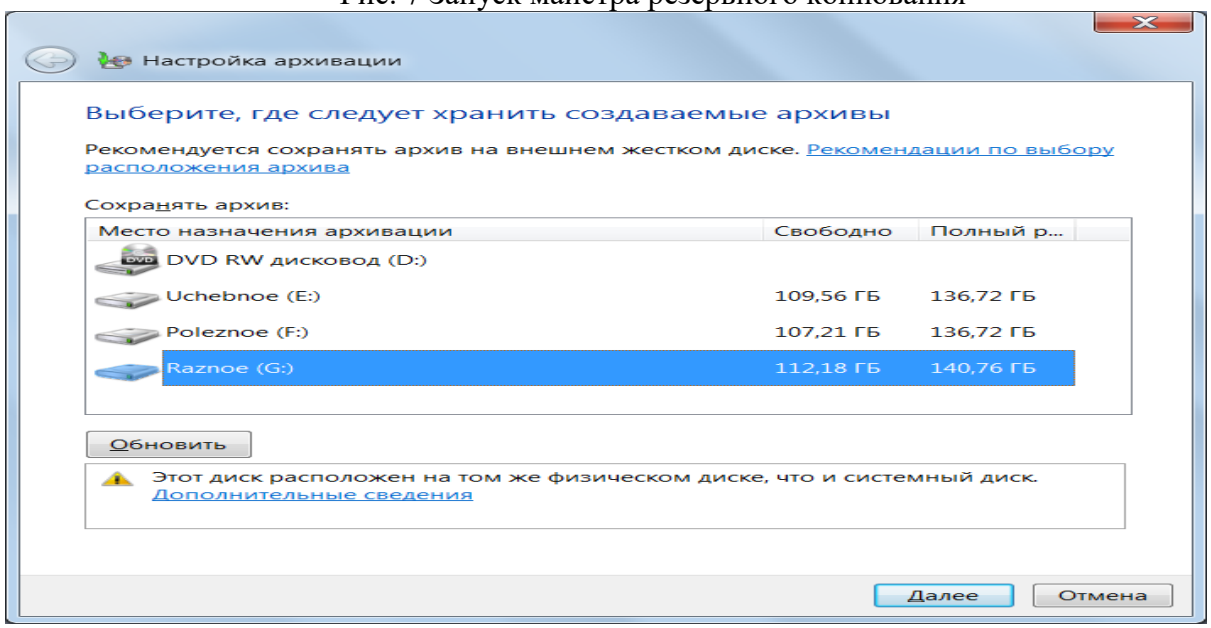


Рис. 8 Відбір місцезнаходження майбутнього архіву

Проглядання вмісту резервної копії відбувається шляхом введення команди **Просмотр файлов** або **Просмотр каталогов**.

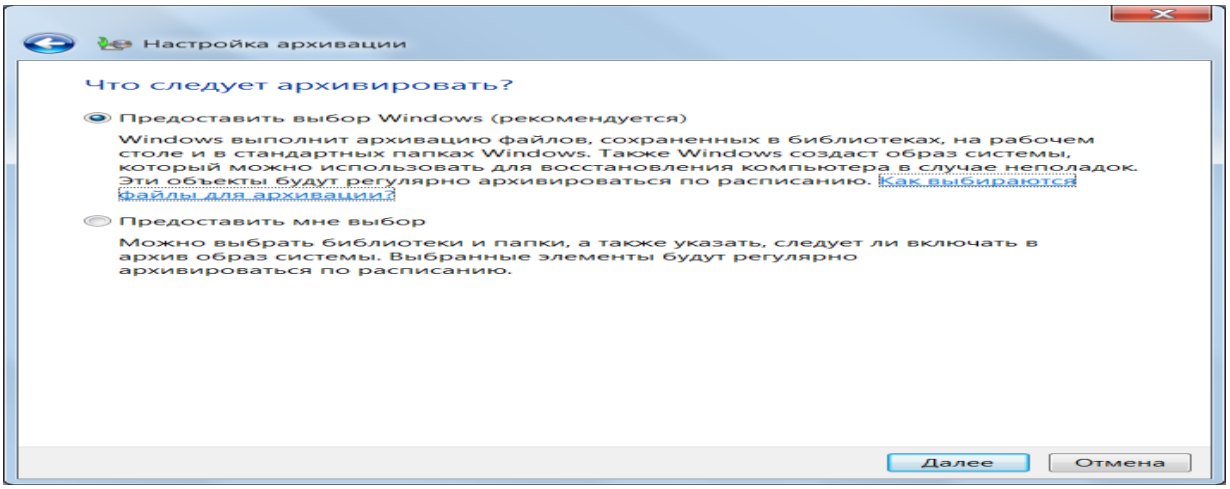


Рис. 9 Надання прав архівування

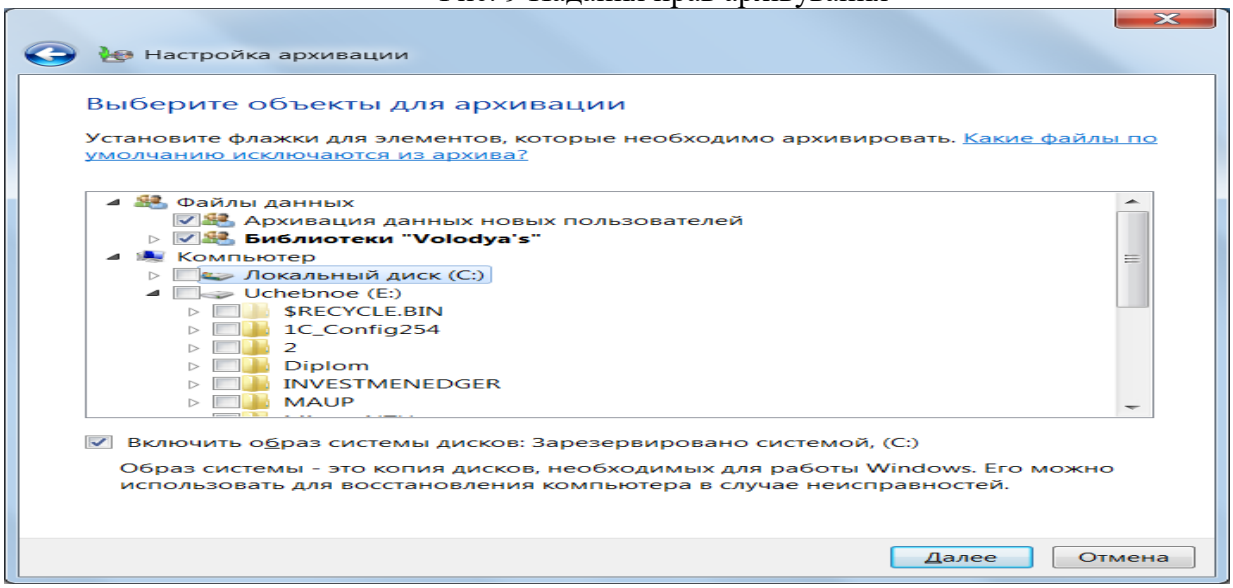


Рис. 10 Вікно відбору об'єктів архівування

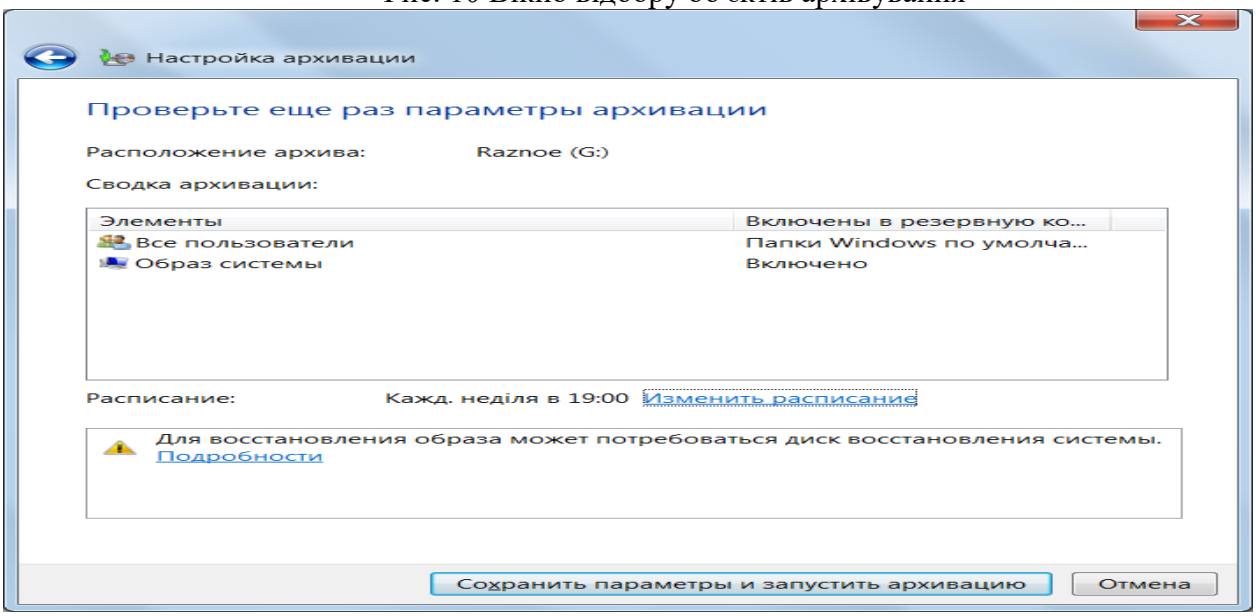


Рис. 11 Відбір параметрів архівації

Під час огляду тек окремі файли в теці не відображаються. Щоб проглянути окремі файли, скористайтеся командою **Просмотр файлов**.

Подавши команду **Управление местом на диске занимаемой этой копией** можна змінити параметри архіву (рис. 14).

Для пошуку у вмісті резервної копії виберіть **Поиск**, введіть ім'я файлу цілком або частково і натисніть кнопку **Найти**.

Існує два способи відновлення файлів.

- за наявності резервної копії, що містить файл, можна відновити файл з неї;
- якщо немає резервної копії, що містить файл, можна спробувати відновити попередню версію файлу. Windows автоматично зберігає копії змінених файлів (включаючи файли, що видаляються) з використанням крапок відновлення; ці файли називаються попередніми версіями.

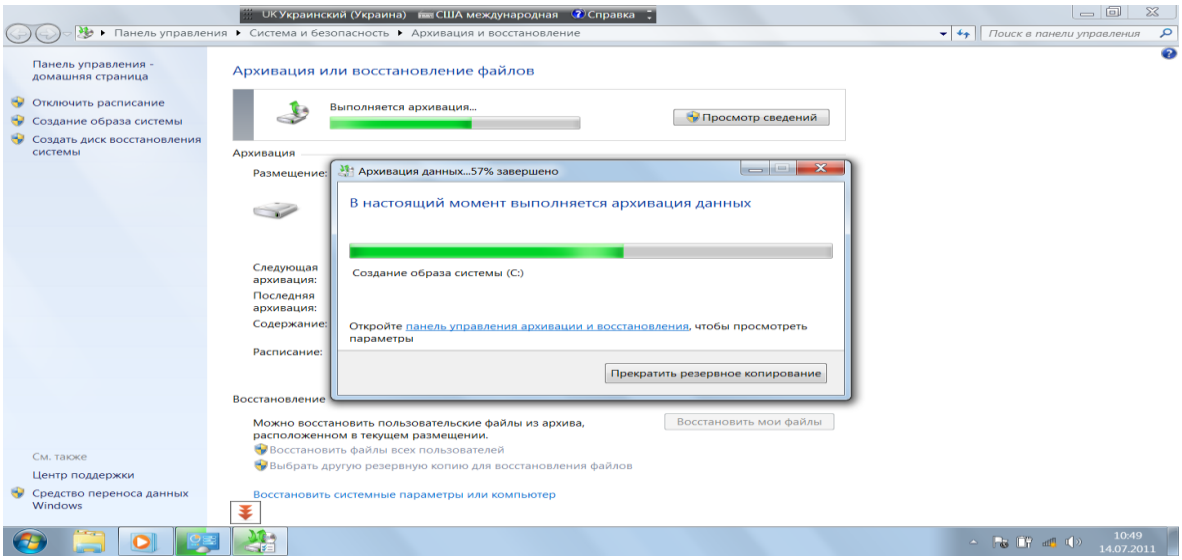


Рис. 12 Вікно процесу архівування

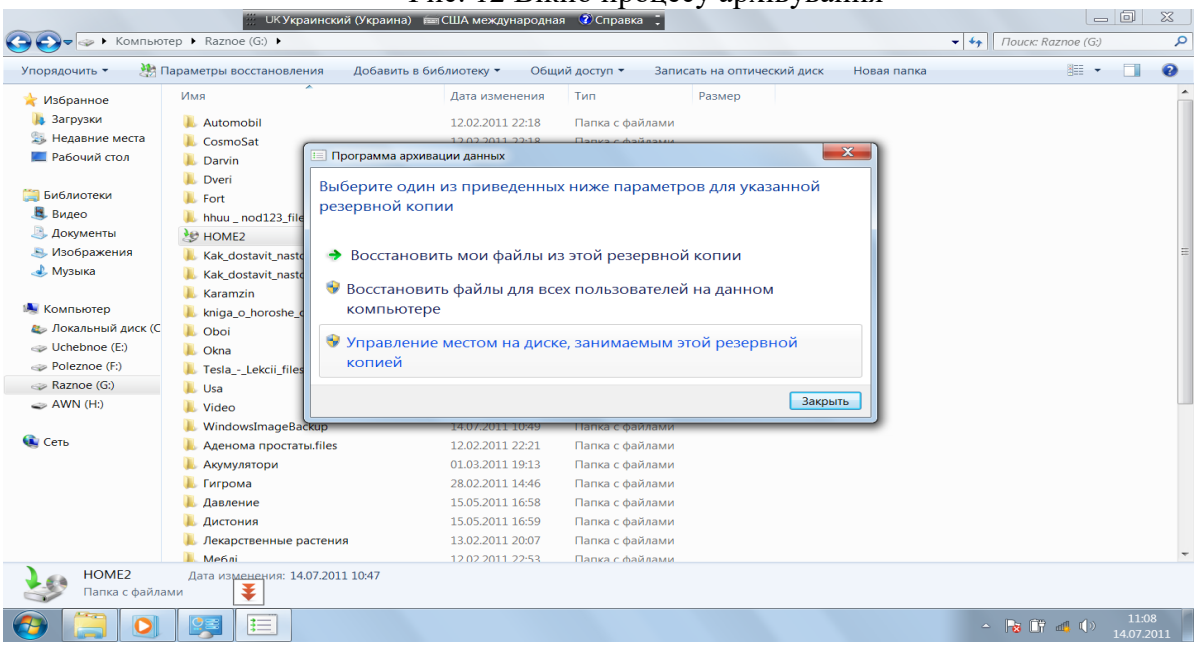


Рис. 13 Вікно відновлення файлів

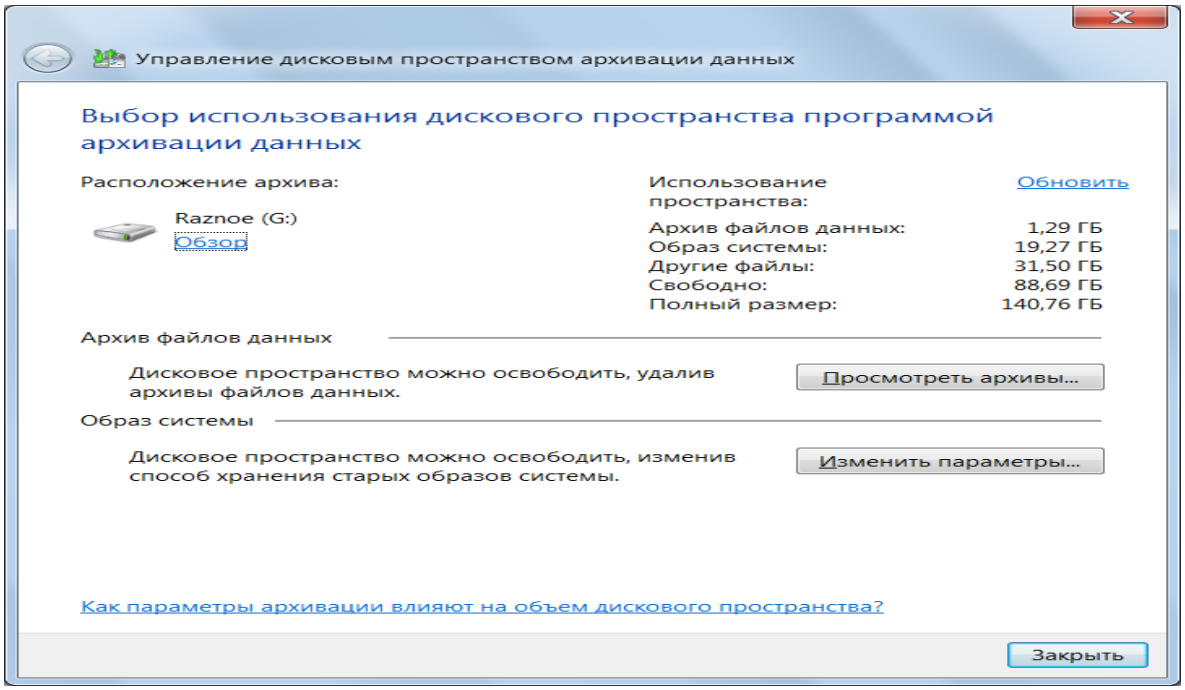


Рис. 14 Вікно зміни параметрів архіву

3.3 Створення крапки відновлення

Крапка відновлення – це представлення збереженого стану системних файлів комп'ютера. Крапку відновлення можна використовувати для відновлення системних файлів комп'ютера в стан, відповідний моменту часу у минулому. Крапки відновлення автоматично створюються засобом відновлення системи щонеділі (за умовчанням) і при виявленні засобом відновлення системи початку зміни конфігурації комп'ютера, наприклад при установці програми або драйвера.

Крапку відновлення у будь – який момент можна створити вручну, виконавши наступні дії.

1. Зайдіть в **Панель управления**, групу команд **Система и безопасность**.
2. Введіть команду **Система** (рис. 15).
2. У лівій області виберіть **Защита системы** (рис. 16). При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.
4. На вкладці **Защита системы** натисніть кнопку **Создать**.
4. У діалоговому вікні **Защита системы** введіть опис (рис. 17) натисніть кнопку **Создать**.

3.4 Створення образу системи для диску

Диск, на якому зберігається резервна копія, повинен бути відформатований під файлову систему NTFS.

1.Зайдіть в **Архивация и восстановление**

2.У лівій області виберіть **Создание образа системы** (рис. 18) і слідуйте інструкціям майстра. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

3. Відберіть параметри архівування за допомогою майстра.

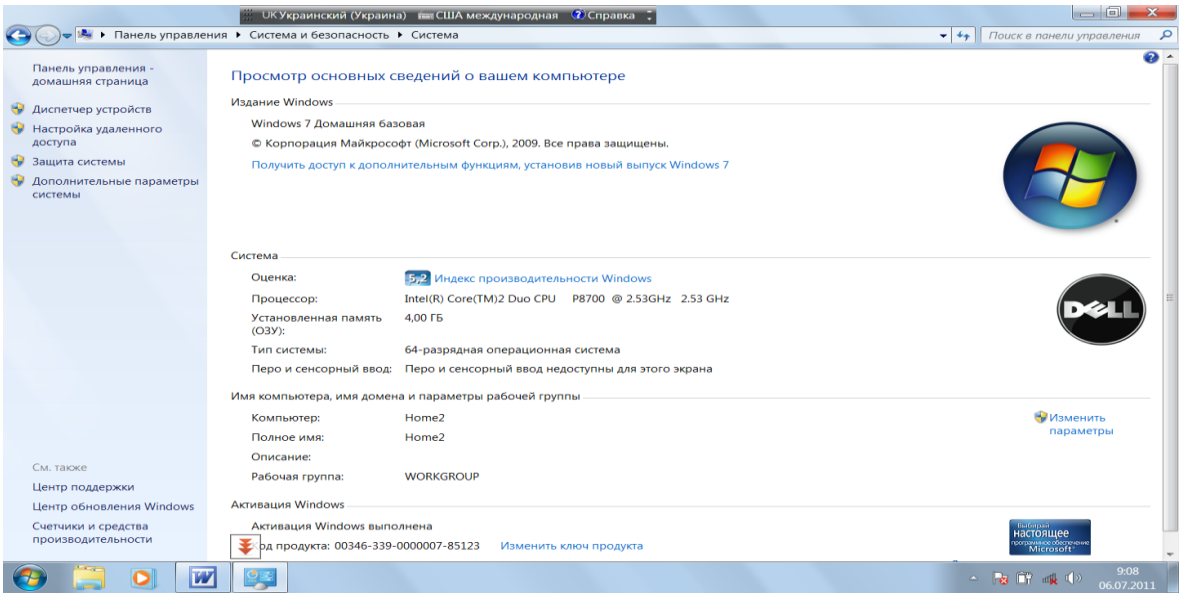


Рис. 15 Вікно системи

3.5 Створення резервної копії реєстру

Усі відомості про конфігурацію системи зберігаються в спеціальній базі даних, яка називається Реєстром, або Системним реєстром. Реєстр містить відомості, до яких Windows постійно звертається під час роботи, а саме:

- профілі усіх користувачів;
- дані про встановлені програми і типи документів, що створюються кожною програмою;
- значення властивостей для тек і значків програм;
- конфігурація устаткування, встановленого в операційній системі;
- дані про порти, які використовуються.

За допомогою реєстру можна модифікувати конфігурацію ОС. Проте перед внесенням змін до реєстру рекомендується зробити резервну копію своєї системи. Інструментальним засобом конфігурації системи являється програма – графічний редактор реєстру – Regedit.exe. Реєстр має ієрархічну деревовидну структуру.

Перш ніж вносити зміни в розділ реєстру або підрозділ, рекомендується виконати експорт або створити резервну копію відповідного розділу або підрозділу. Резервну копію можна зберегти в потрібному місці, наприклад, в теці на жорсткому диску або на з'ємному носієві. Потім цю резервну копію можна імпортувати, щоб відмінити внесені зміни.

1. Зайдіть в командний рядок та введіть команду **regedit** (рис. 19). При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

2. Знайдіть і виберіть розділ або підрозділ реєстру, резервну копію якого необхідно створити (рис. 20).

3. Відкрийте вкладку **Файл** і натисніть кнопку **Экспорт**.

4. У полі **Каталог** виберіть розташування, в яке слід зберегти резервну копію, і в ім'я файлу введіть ім'я файлу копії реєстру (рис. 21).

5. Клацніть **Сохранить**.

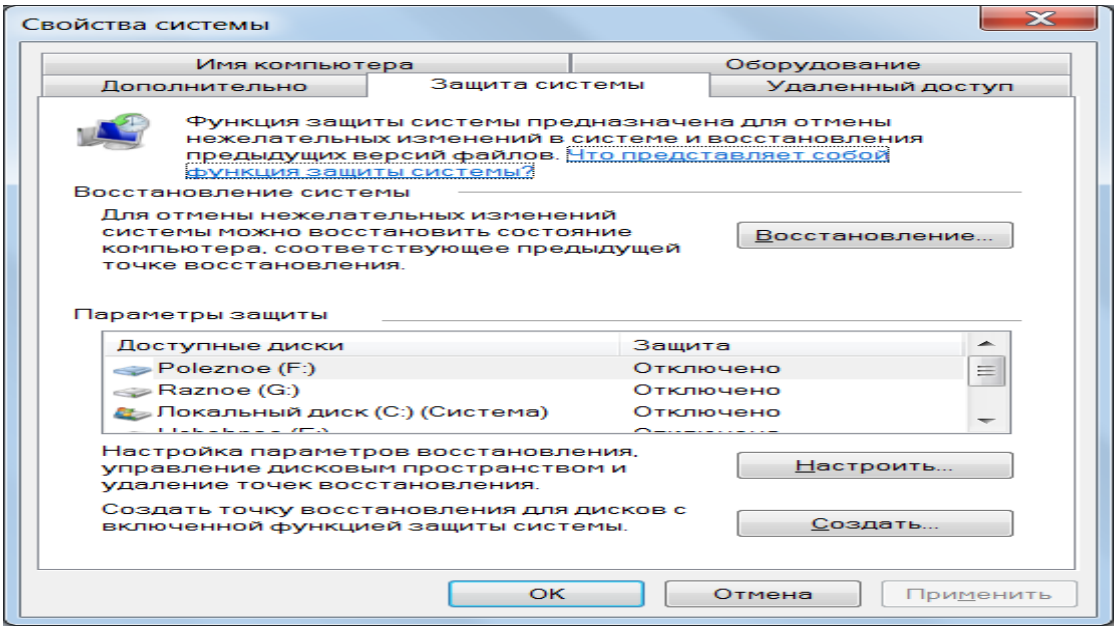


Рис. 16 Вікно захисту системи

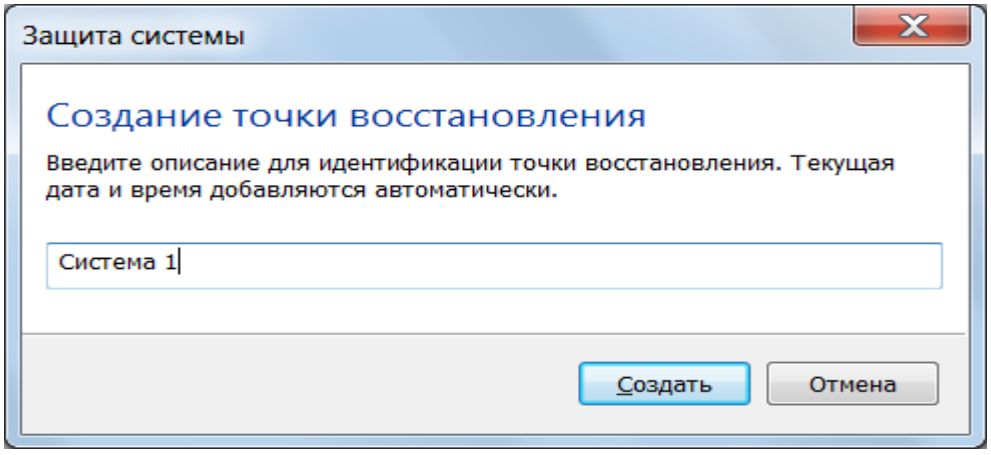


Рис. 17 Вікно опису крапки відновлення

Примітка. Перед внесенням змін до реєстру рекомендується створити крапку відновлення, використовуючи засіб Відновлення системи. Крапка відновлення містить дані про реєстр. Її можна використовувати для відміни змін системи.

4 Використання сертифікату

4.1 Оновлення або запит нового сертифікату

Насамперед сертифікати використовуються для ідентифікації користувачів або пристроїв, перевірки достовірності служб або шифрування файлів. Зазвичай сертифікати надаються автоматично. Наприклад, при здійсненні покупки через безпечний web – сайт в Інтернеті сертифікат використовується для шифрування даних кредитної карти. Сертифікат для особистого використання, наприклад, для включення цифрового підпису в електронні аркуші, може не надаватися автоматично. В цьому випадку необхідно запитати сертифікат в центрі сертифікації і імпортувати його.

Щоб запитати новий сертифікат:

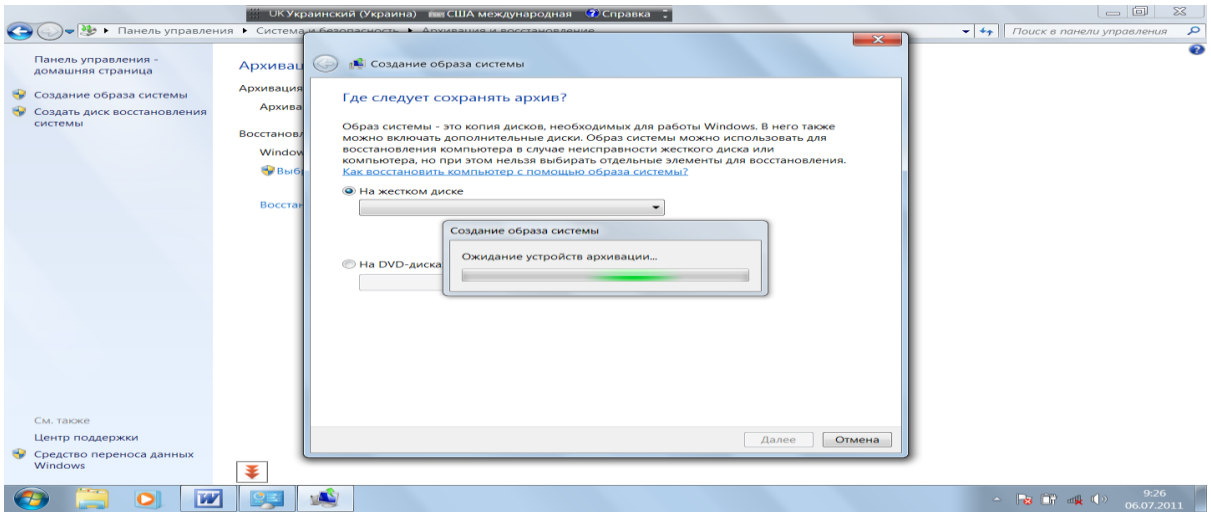


Рис. 18 Вікно підготовки до архівування

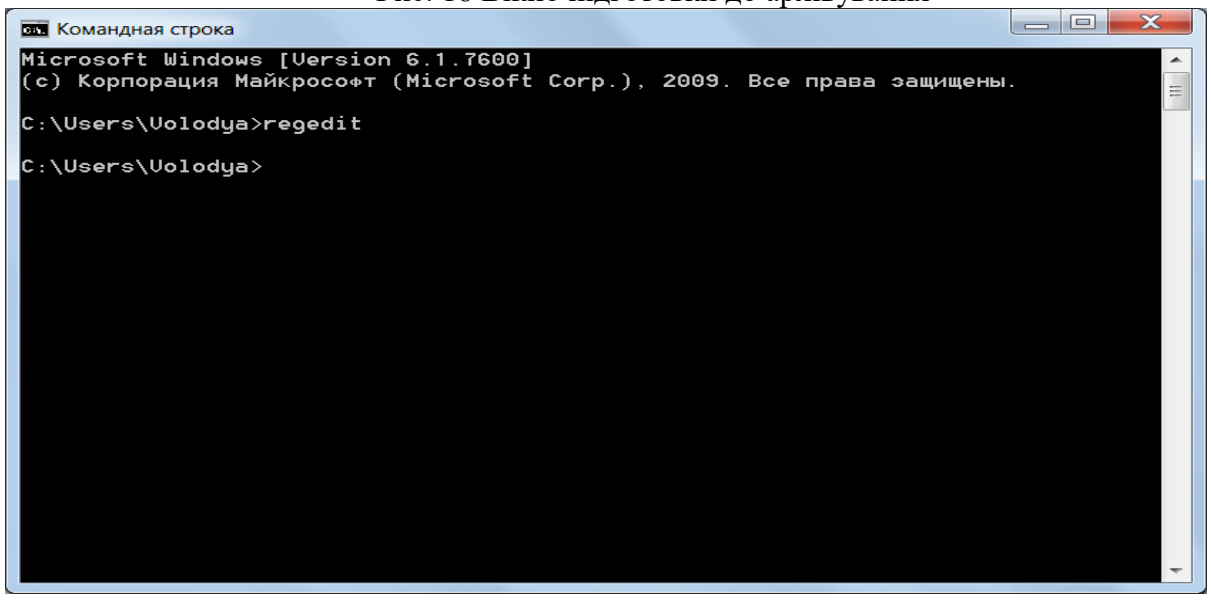


Рис. 19 Вікно командного рядка

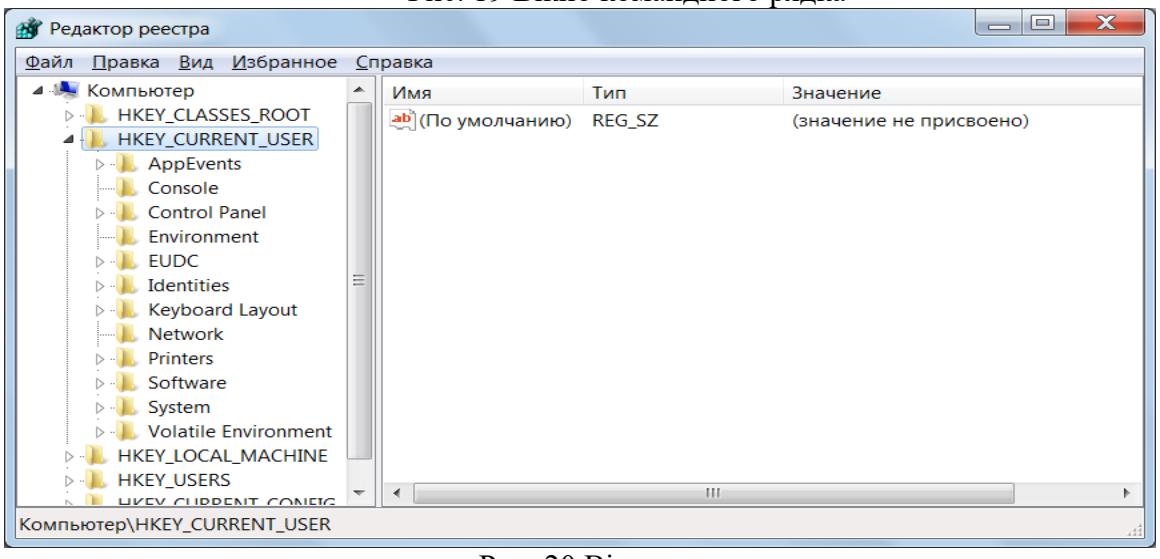


Рис. 20 Вікно реєстру

1. Зайдіть в **Панель управления**, відберіть групу команд **Сеть и Интернет**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

2. Відберіть команду **Свойства обозревателя**, вкладку **Содержание** (рис. 22).

3. Введіть команду **Сертификаты**.

4.Клацніть вкладку **Личные** (рис. 23).

5.Введіть команду **Импорт**.

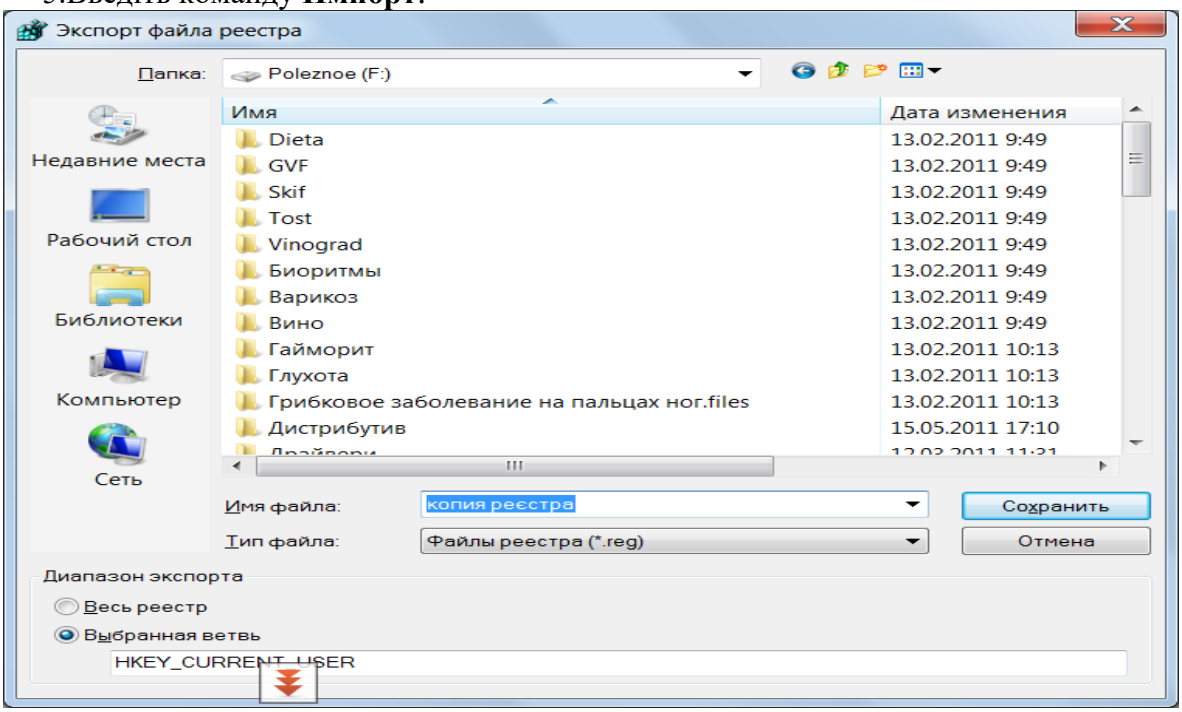


Рис. 21 Параметри збереження реєстру

6. З'явиться вікно майстра імпорту сертифікатів (рис. 24). Слідуйте вказівкам майстра.

Примітка. Запит сертифікатів для служб не підтримується. Щоб запитати сертифікат стандарту цифрового підпису (DSS) в центрі сертифікації, необхідно вибрати шаблон сертифікату **Только подпись пользователя** в майстру запиту сертифікату.

4.2 Проглядання сертифікатів і управління ними

Для проглядання відомостей про сертифікати, а також для їх зміни, видалення або запиту нових використовується диспетчер сертифікатів.

1. Відкрийте **Диспетчер сертифікатів**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.
2. Сертифікати зберігаються в теках **Сертификаты – текущий пользователь**
3. .Можливо, знадобиться проглядання тек, щоб знайти потрібний сертифікат.
4. При відкритті теки, що містить сертифікати, в правій області відображаються сертифікати і деякі відомості про них. Стовпець **Назначение** містить відомості про сферу застосування сертифікату.
5. Існує можливість запиту нового сертифікату з поточним або новим ключем, експорт і імпорт сертифікатів. Для виконання цих операцій виберіть **Сертификат**, в меню **Действие** виберіть пункт **Все задания**, а потім виберіть відповідну команду.

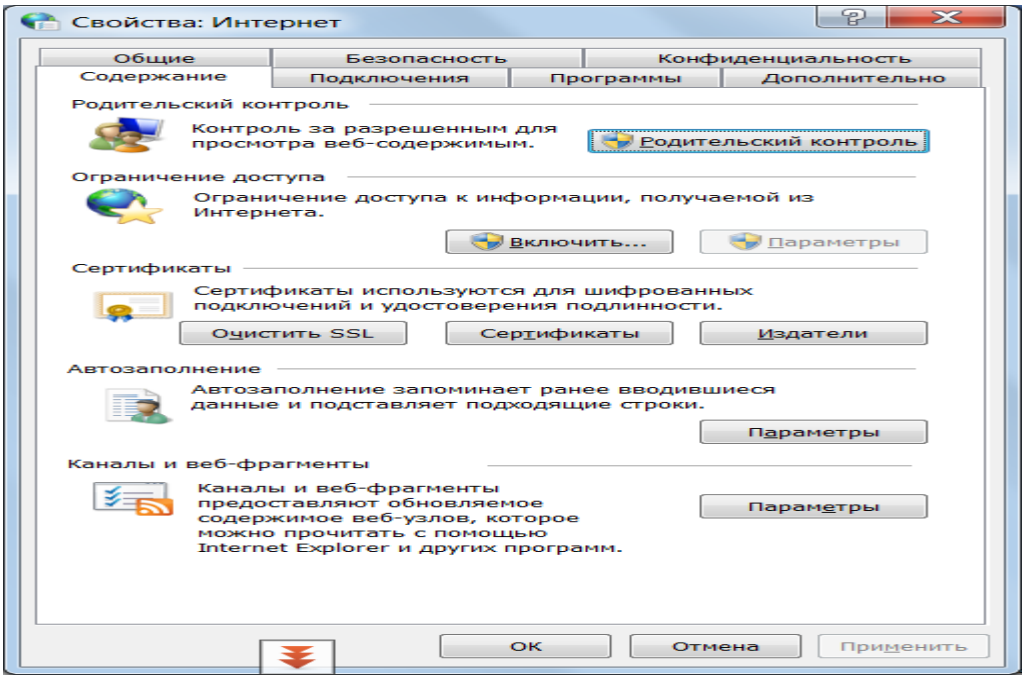


Рис. 22 Вкладка зміст

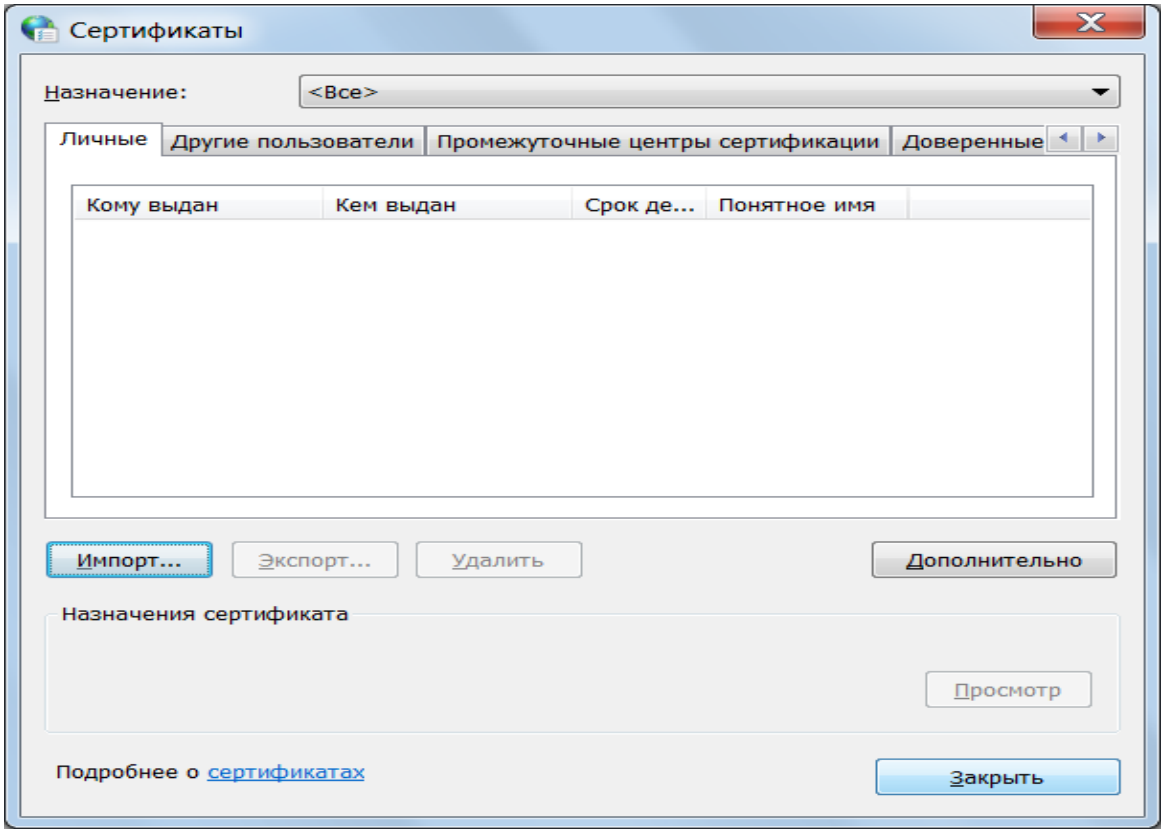


Рис. 23 Вікно сертифікатів

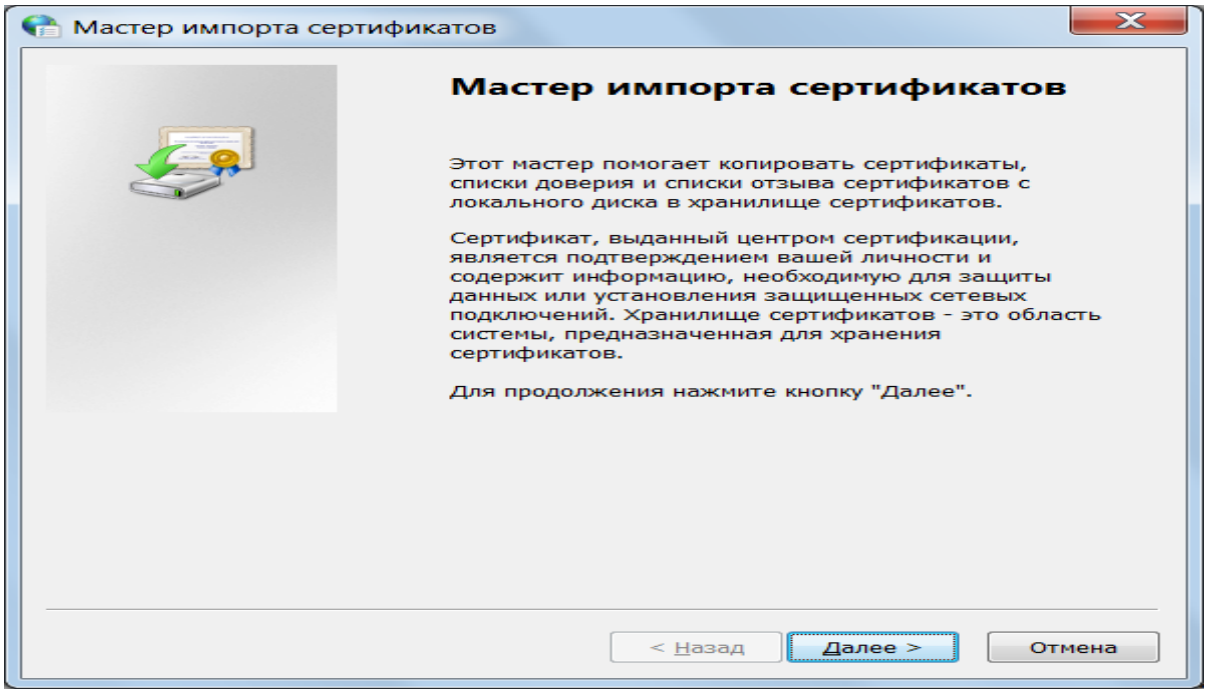


Рис. 24 Вікно майстра імпорту сертифікатів

4.3 Резервне копіювання сертифікату з шифрованої файлової системи (EFS)

При шифруванні даних на комп'ютері необхідно передбачити спосіб відновлення цих даних на випадок, якщо щось відбудеться з ключем шифрування. Якщо ключ шифрування втрачений або пошкоджений і спосіб відновлення даних відсутній, дані будуть втрачені. Дані будуть також втрачені, якщо пошкоджена або загублена смарт – карта, на якій зберігався ключ шифрування. Щоб гарантувати постійний доступ до зашифрованих даних, потрібно зробити резервні копії сертифікату і ключа шифрування. Якщо комп'ютером користуються декілька користувачів або якщо для шифрування файлів використовується смарт – карта, потрібно створити сертифікат відновлення файлу.

Примітка. Ці дії не можна виконати у випусках Windows 7 Початкова, Windows 7 Домашня базова і Windows 7 Домашня розширена.

4.4 Створення резервної копії EFS – сертифіката

1. Відкрийте **Диспетчер сертифікатів**. При появі запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.
2. У лівій області двічі клацніть теку **Личная**.
3. Клацніть **Сертификаты**.
4. У основній області клацніть сертифікат, що містить пункт **Шифрованая файловая система** в групі **Назначение**. Якщо є декілька EFS — сертифікатів, потрібно зробити резервне копіювання для всіх.
5. У меню **Действие** виберіть пункт **Все задания** і клацніть **Экспорт**.
6. У вікні майстра експорту сертифікатів натисніть кнопку **Далее**, виберіть параметр **ОК**, **Экспортировать закрытый ключ** і натисніть кнопку **Далее**.
7. Клацніть **Файл обмена личной информацией** і натисніть кнопку **Далее**.
8. Введіть пароль, який слід використовувати, підтвердіть його, а потім натисніть кнопку **Далее**. Процес експорту створить файл для збереження сертифікату.
9. Введіть ім'я файлу і його розташування (повний шлях) або натисніть кнопку **Осмотр**, перейдіть до потрібного місця, введіть ім'я файлу і натисніть кнопку **Сохранить**.

10. Послідовно натисніть кнопки **Далее** і **Готово**.

4.5 Захист диску

Такий захист встановлюється на логічний диск для захисту даних, програм; перешкоді їх видалення і т.п. На системний диск такий захист повинен бути встановлений обов'язково. Він встановлюється в такій послідовності:

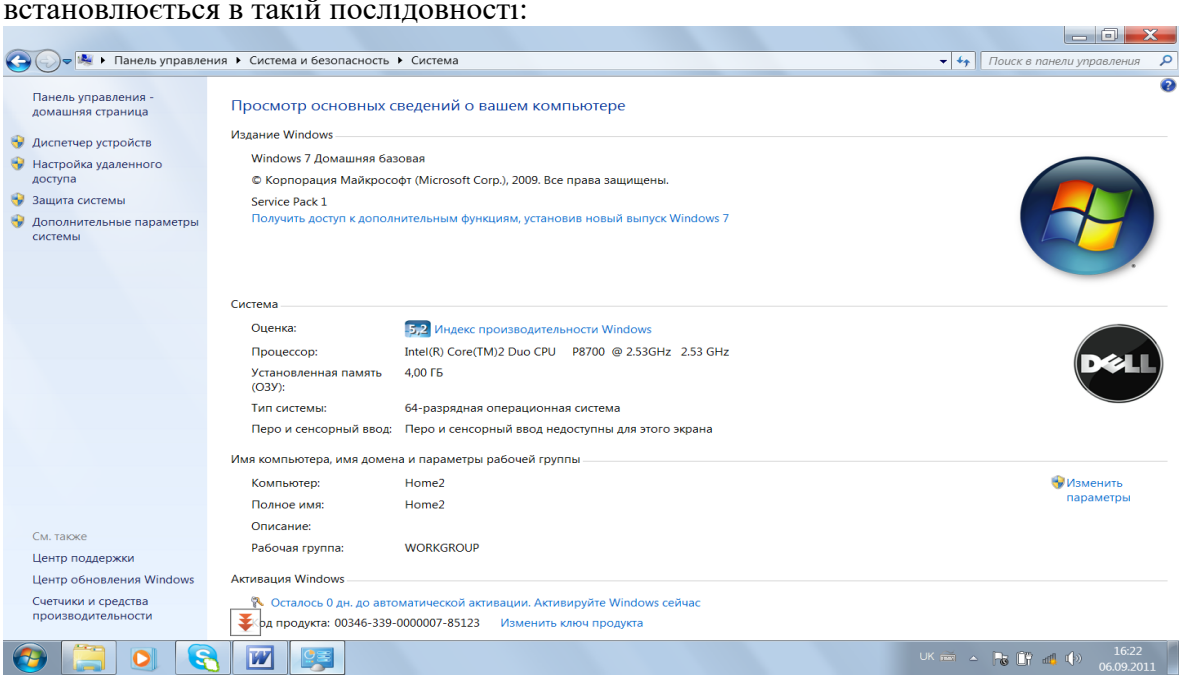


Рис. 25 Вікно захист системи

Введіть команду **Панель управления\ Система и безопасность\Система**.

В лівій панелі виберіть команду **Защита системы** (рис. 25). Вкажіть локальний диск на який буде встановлено захист (рис. 26) та введіть команду **Настроить** відберіть потрібні параметри захисту (рис 27) та натисніть кнопку **ОК**.

Примітка. В разі відсутності такого захисту на системному диску відновлення параметрів системи буде ускладнене.

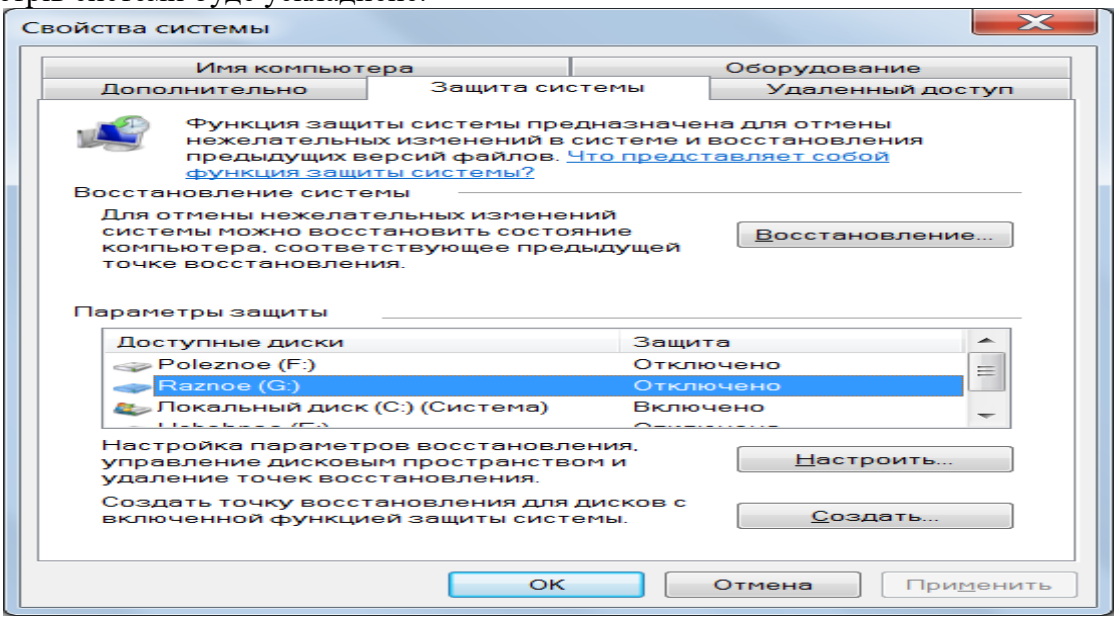


Рис. 26 Вікно відбору диску

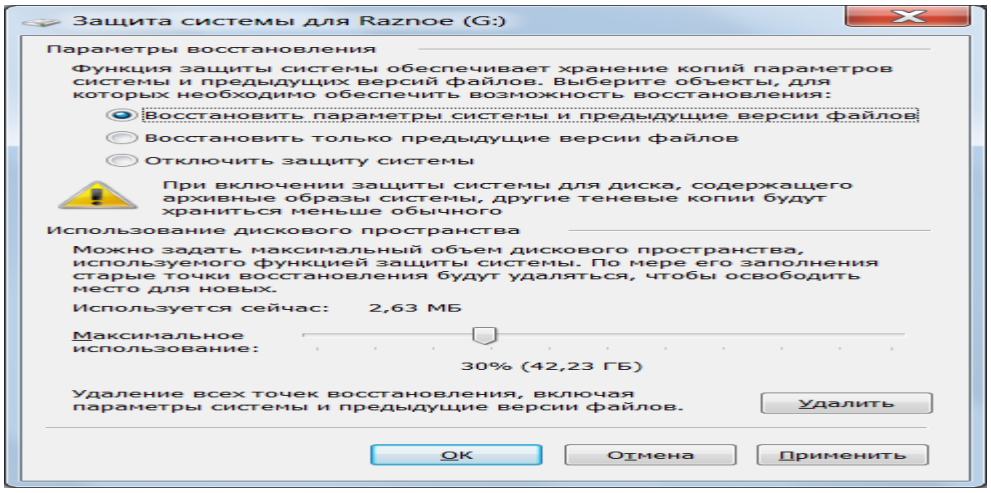


Рис. 27 Вікно відбору типу захисту

5 Хід роботи

1. Створіть групи користувачів гість та досвідчений користувач
2. Проведіть відкриття файлу, якщо відмовлено в доступі до нього
3. Проведіть архівацію образу системи та файлів і тек
4. Перегляньте вмісту резервної копії
5. Створіть крапку відновлення системи
6. Проведіть відновлення файлів
7. Проведіть видалення архіву
8. Створіть образ системи для диску
9. Створіть резервну копію реєстру
10. Створіть сертифікат
11. Створіть резервну копію EFS – сертифіката
12. Проведіть захист диску D

6. Контрольні питання

1. Які типи облікових записів користувачів допускає Windows 7?
2. Як створити групи користувачів?
3. Яке призначення фільтру Microsoft SmartScreen?
4. Як провести відкриття файлу, якщо відмовлено в доступі до нього
5. Які ключові властивості системи шифрування EFS?
6. Як провести захист файлів за допомогою шифрування дисків BitLocker?
7. Як провести архівацію образу системи та файлів і тек?
8. Як видалити старі резервні копії файлів?
9. Як проглянути вміст резервної копії?
10. Як відновити систему та файли?
11. Як створити крапку відновлення системи?
12. Як створити образ системи для диску?
13. Як створити резервну копію реєстру?
14. Як створити сертифікат?
15. Як створити резервну копію EFS – сертифіката?
16. Як провести захист диску?

РОЗДІЛ 2
Захист інформації в Microsoft Office

Лабораторна робота 6
Захист інформації у Microsoft Word 2003 і Excel 2003.

Мета роботи – засвоїти принципи і технологію роботи із захистом інформації у Microsoft Word і Excel.

ПЛАН

1. Теорія
1.1 Шифрування в Word і Excel
1.2 Захист інформації у Microsoft Word.
1.3 Захист документа за допомогою цифрового підпису.
1.4 Установлення паролю на дозвіл відкриття документа.
1.5 Захист інформації у Microsoft Excel.
2. Хід роботи
3. Контрольні питання

1. Теорія

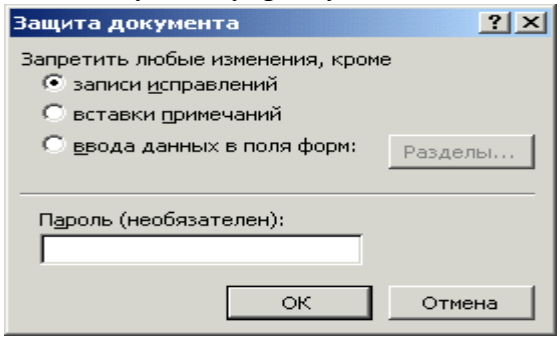
1.1 . Шифрування в Word і Excel

Фірма Майкрософт уключила у свої продукти деякий криптозахист. Це дуже законослухняна фірма, що чітко дотримує всі експертні обмеження США, так ще і перестраховується. Це не дозволяє сподіватися на стійкість такого захисту. До того ж, алгоритм шифрування не описаний, що, є показником ненадійності.

Крім того, маються дані, що Майкрософт залишає у використовуваних криптоалгоритмах «чорний хід». Якщо вам дуже потрібно розшифрувати файл, пароль до якого втрачений, можна звернутися у фірму. За офіційним запитом, при достатніх підставах вони проводять розшифрування файлів Word і Excel. Так, до речі, поводяться і деякі інші виробники ПО.

1.2 Захист інформації у Microsoft Word.

ля захисту змісту файлу в Microsoft Word необхідно з підменю **Сервис** податі команду **Установить защиту**. У діалоговому віконці, яку з'явиться вибрати відповідний тип захисту (рис. 1) та ввести пароль. Далі натиснути кнопку **ОК**. Підтвердити пароль.



Для зняття захисту з файлу подається команда Зняти захист із підменю **Сервис**.

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

Рис. 1. Вікно відбору типу захисту.

1.3 Захист документа за допомогою цифрового підпису.

В цьому випадку необхідно виконати наступні дії:

1. У меню **Сервис** виберіть команду **Параметры**, а потім відкрийте вкладку **Безопасность** (рис. 2)

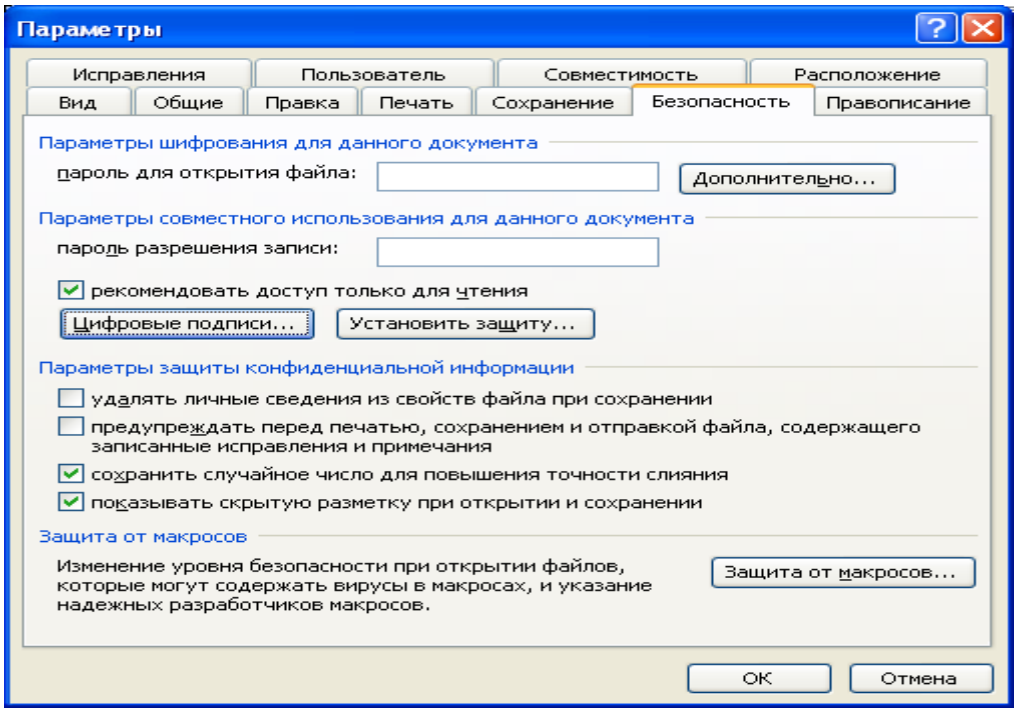


Рис. 2. Вікно Безпеки.

2. Натисніть кнопку **Цифровые подписи**.
3. Натисніть кнопку **Добавить**.
4. 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.

1.4 Установлення паролю на дозвіл відкриття документа.

1. Відкрийте файл.
2. У меню **Сервис** виберіть команду **Параметры**, а потім відкрийте вкладку **Безопасность.**
3. У полі **Пароль** для відкриття файлу введіть пароль (рис. 3), а потім натисніть кнопку **ОК**.
4. Уведіть пароль ще раз повторно, а потім натисніть кнопку **ОК**.

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 ви можете запам'ятати, щоб не записувати його.

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

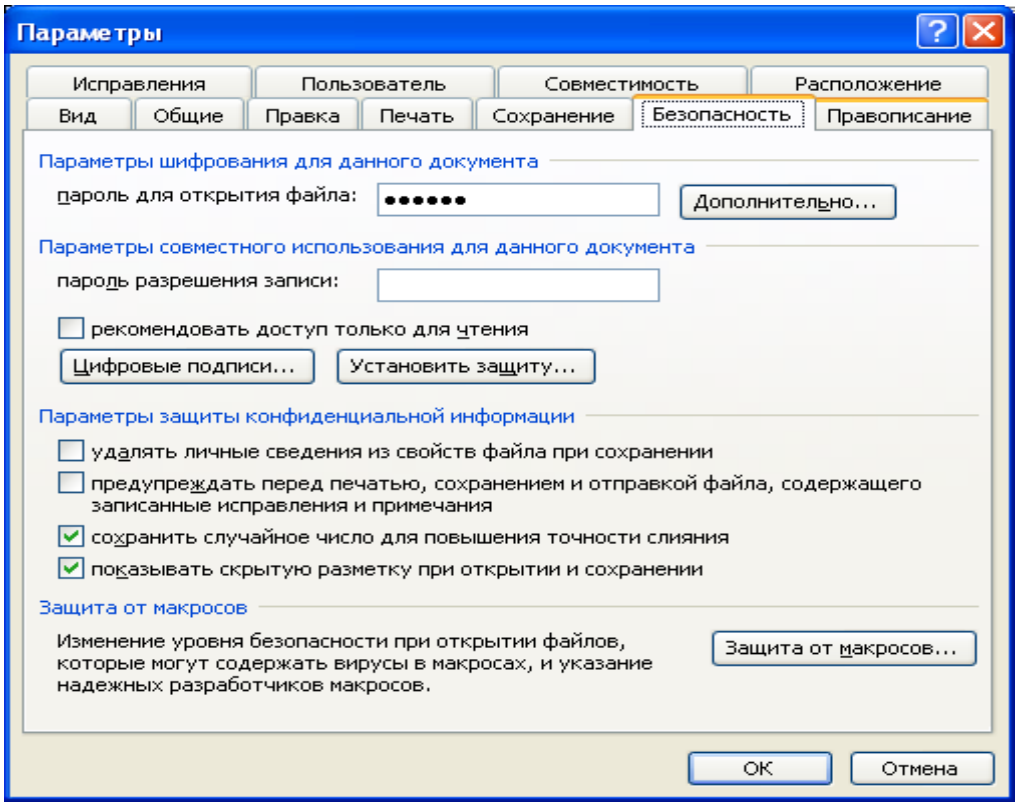


Рис. 3. Вікно введення паролю

1.5 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.

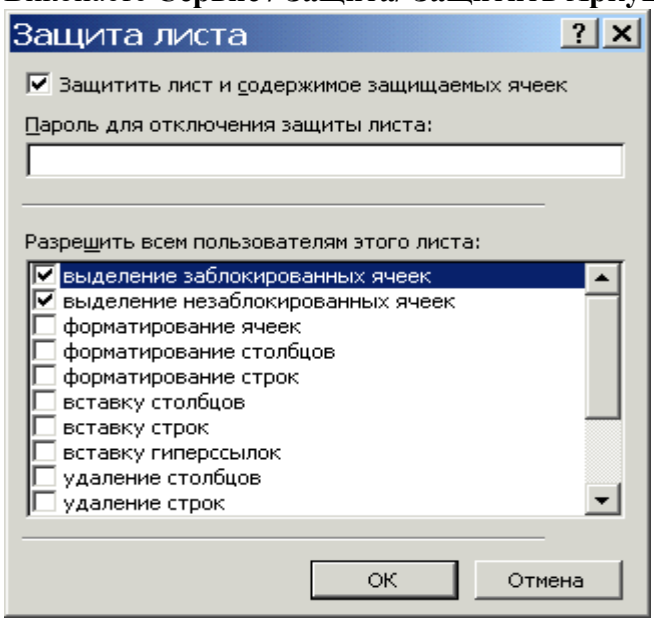
От приклад: Ви працюєте з таблицею нарахування заробітної плати і ненароком стерли комірку, де була формула обчислення премії. Чи не стерли, але занесли в неї щось інше. Це буває, особливо якщо надворі мерзенна погода, на сонці магнітні бури, в автобусі Вам наступили на ногу, а начальник стоїть над душею, і результати йому потрібні не пізніше ніж через п'ять хвилин. Це буває також, якщо вашою табличкою користуєтеся не Ви, а, скажімо, бухгалтер, який тільки і вміє, що проставляти значення окладів, але от промахнувся й уставив оклад туди, де потрібна премія. Тепер потрібно відновити все як було.

Яка там була формула до цього, Ви, звичайно, не пам'ятаєте (а вже бухгалтер зроду її не знав). Можна, звичайно, запам'ятати таблицю, відновити останню копію (чи подивитися в ній формулу і виправити), можна завантажити цю комірку з таблиці, що знаходиться на диску, і так далі, тощо. Але куди простіше подбати про те, щоб деякі комірки просто не можна було змінити.

Наприклад, у стовпці G 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 Аркуш.

Виконаєте **Сервис / Защита/ Защитить Аркуш** . З'явиться діалогове вікно (рис. 4).



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 комірки. Для зняття захисту з листа виконаєте **Сервис / Защита/Снять защиту листа**. Тепер потрібно визначити комірки, які не можна змінювати. Для цього необхідно виділити потрібні комірки та ввести команду **Формат ячеек/Защита**. З'явиться діалогове вікно (рис. 5).

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

Рис. 4. Вікно вибору параметрів захисту листа

Тепер комірка буде заблокована, якщо Ви захистите Аркуш, то цю комірку не можна буде змінювати.

Щоб розблокувати комірки, які можна змінювати, Ви повинні:

1. Зняти захист листа, якщо він є.
2. Виділити інтервал комірок, який потрібно розблокувати й виконати **Формат ячеек/ Защита** і забрати прапорець у вікні **Защищенная ячейка**. Аналогічно встановлюється захист на книгу (рис. 6).

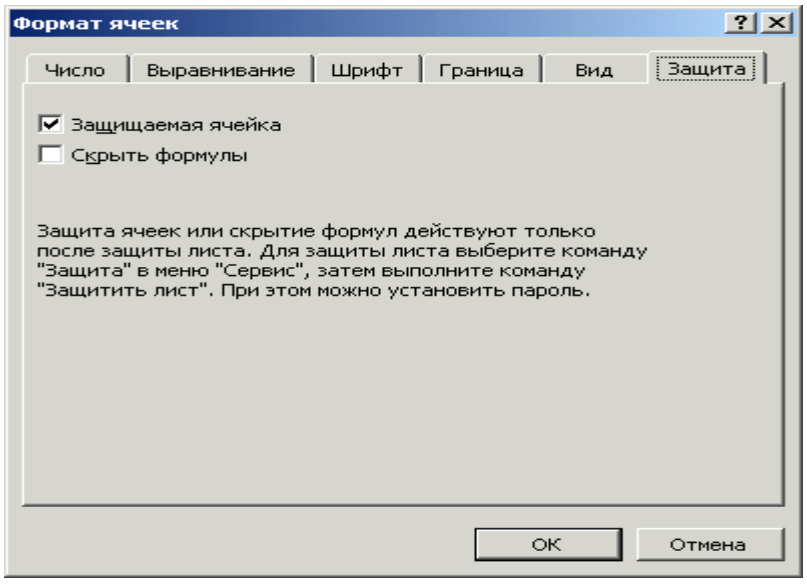


Рис. 5. Вікно формату комірок.

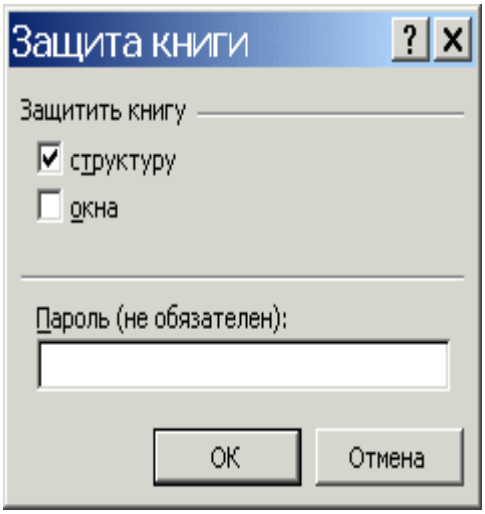


Рис. 6. Вікно захисту книги.

2. Хід роботи:

1. Провести захист інформації у Microsoft Word, вибравши тип захисту Записи справлень.
2. Відкрийте захищений файл та спробуйте внести відповідні зміни в текст, використавши клавіатуру, головне меню, контексно-залежне меню.
3. Зніміть захист із файлу та проведіть зміну тексту відповідно пункту 2.
4. Установіть інші типи захисту та виконайте пункти 2 і 3.
5. Установіть пароль на файл при відкритті його в програмі Microsoft Word.
6. Перевірте відкриття файлу при встановленому паролі на відкриття.
7. Створити в Microsoft Excel таблицю Розрахунку заробітної плати, яка наведена нижче.

A	B	C	D	E	F	G
		Розрахунок заробітної плати				
2	№ п/п	Прізвище І.Б.	Оклад	Кіль-кість відпра-цьова-них днів	Загаль-на кіль-кість днів	Сума до оплати
3	1	Іванов І.П.	500	22	22	500
4	2	Сидоров С.С.	400	18	22	327.27
5	3	Петров А.Р.	350	20	22	318.18
6	4	Полуботько М.М.	600	21	22	572.72
7	5	Мазепа П.С.	450	15	22	306.81

8. Установіть захист на Аркуш.
9. Спробуйте змінити зміст комірки. Використайте для цього клавіатуру, головне меню, контексно-залежне меню, клавішу Delete.
10. Спробуйте змінити зміст комірки F3. Чи зміниться число в комірці G3?
11. Спробуйте розблокувати комірку F4. Пункт меню "Формат" висвітлений сірім кольором?
12. Зніміть захист із листа та проведіть зміну змісту комірок.
13. Установіть захист на книгу.
14. Виконайте пункти 7-10.
15. Установіть захист на декілька комірок.
16. Виконайте в них пункти 7-10.
17. Установіть пароль на файл при відкритті його в програмі Microsoft Excel.
18. Перевірте відкриття файлу при встановленому паролі на відкриття.
19. Установіть захист файлу цифровим підписом.

3. Контрольні питання

1. Послідовність встановлення захисту на файл в у Microsoft Word.
2. Типи захисту тексту в у Microsoft Word.
3. Послідовність зняття захисту з тексту в Microsoft Word.
4. Послідовність встановлення захисту на файл при його відкритті.
5. Послідовність встановлення захисту на файл цифровим підписом.

6. Послідовність встановлення захисту на комірки в Microsoft Excel.
7. Послідовність встановлення захисту на листи в Microsoft Excel.
8. Послідовність встановлення захисту на книгу в Microsoft Excel.
9. Послідовність зняття захисту на книгу в Microsoft Excel.
10. Послідовність зняття захисту на листи в Microsoft Excel.
11. Послідовність зняття захисту на комірки в Microsoft Excel.
12. Як приховати формули в комірках у Microsoft Excel?

Лабораторна робота 7
Захист інформації у Microsoft Access 2003

Мета роботи – Засвоїти принципи і технологію захисту інформації у базах даних за допомогою паролів.

Ознайомитись з поняттям, принципом установлення різних видів паролів для баз даних.

План

1. Теорія
1.1 Паролі MS Access
1.2 Паролі баз даних
1.3 Паролі облікових записів користувачів.
1.4 Паролі Microsoft Visual Basic для додатків (VBA).
1.5 Установлення паролю баз даних.
1.6 Установлення пароля в проекті Microsoft Access (.adp)
1.7 Відображення й приховання об'єктів бази даних у вікні бази даних.
1.8 Використання параметрів запуску.
1.9 Видалення пароля в базі даних Microsoft Access (.mdb)
1.10 Захист паролем програми Microsoft Visual Basic для додатків (VBA)
2. Хід роботи
3. Контрольні питання

1. Теорія:

1.1 Паролі MS Access

Про надійність захисту інформації у базах даних можна судити за наступним діалогом:

Q: Я поставив пароль на базу. Можу я бути упевнений, що тепер нею ніхто не скористається?

A: Хто-знає? Паролі зберігаються в заголовку файлу. Заголовок, зашифрований за 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.

Q: При спробі відкрити базу Access я одержую пропозицію ввести логін і пароль. Що це за захист і наскільки він стійкий?

A: Це захист документа на рівні користувачів/груп. 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.

Загальні відомості про паролі.

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.

1.2 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 Дополнительно 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.

1.3 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 чи надати можливість користувачам додати власні паролі.

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

1.4 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 класу (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.

1.5 Установлення паролю 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 **Открыть**. Відкрийте базу даних у режимі **Монопольно** (рис. 1). У меню **Сервис** виберіть команду **Защита** і підкоманду **Задать пароль базы данных**. 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:

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

Примітка. У паролях враховується регістр символів.

Для підтвердження пароля введіть його ще раз у поле **Подтверждение**, а потім натисніть кнопку **OK** (рис. 2). 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 (міститься в тимчасовий буфер) у базі даних, із якою зв'язується таблиця. Це дозволить будь-якому користувачу бачити ваші дані.

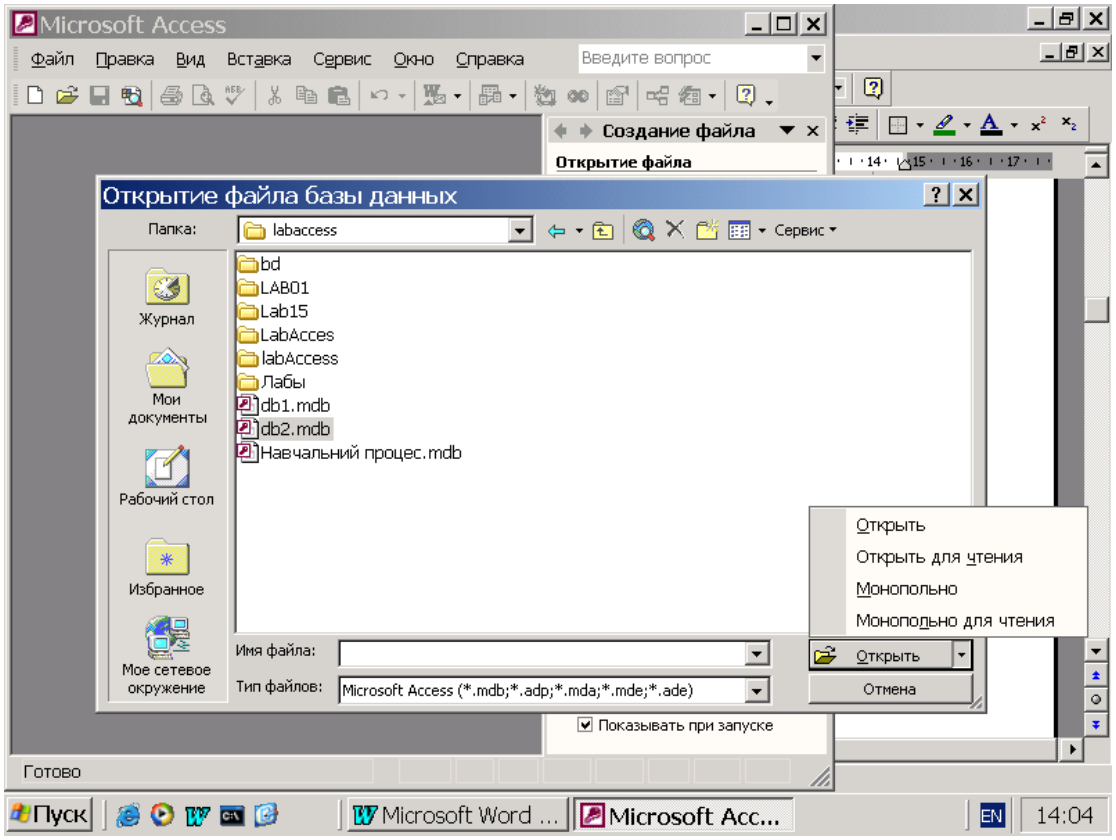


Рис. 1. Вібір монопольного режиму відкриття бази даних.

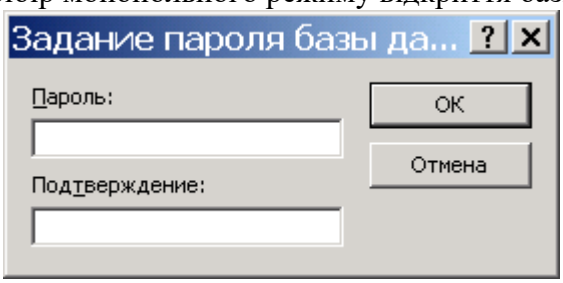


Рис. 2. Вікно введення паролю.

1.6 Установлення пароля в проекті Microsoft Access (.adp)

На відміну від бази даних Microsoft Access у проекті не можна захистити форми, чи звіти макроси за допомогою захисту на рівні користувачів, а також не можна установити пароль на файл проекту Microsoft Access (.adp). Для захисту об'єктів чи форми звіту можна сховати ці об'єкти у вікні бази чи даних настроїти параметри запуску. Для захисту доступу до макетів форм і звітів у проекті Microsoft Access можна задати параметри запуску чи зберегти проект Microsoft Access у виді 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 чи установити пароль.

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

У списку **Объекты базы данных** виберіть тип об'єкта бази даних, властивості якого потрібно змінити. Натисніть кнопку **Свойства** на панелі інструментів **База данных**. Установіть чи зніміть прапорець **Спрятанный** (рис. 3).

Примітка. У проекті Microsoft Access не можна змінювати властивості таблиць, чи 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.

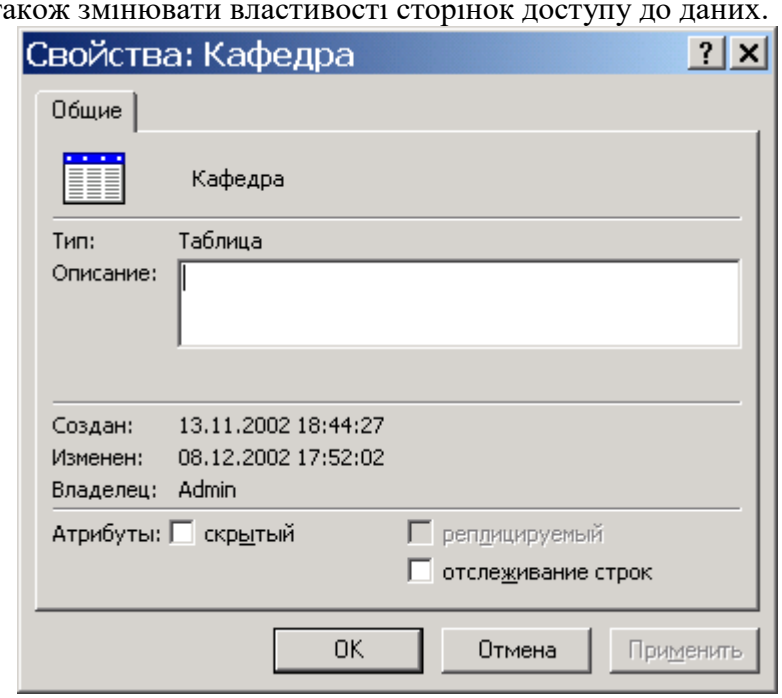


Рис. 3. Вікно присвоєння або зняття атрибуту прихований.

Відображення чи 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 **Сервис** виберіть команду **Параметры**. Виберіть вкладку **Вид**. Установіть чи зніміть прапорець сховані об'єкти в групі **Отображать**. Щоб показати розходження між схованими й іншими об'єктами, сховані об'єкти відображаються у виді сірих значків. Аналогічно відображаються або приховуються системні об'єкти.

1.8 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 чи 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.

Налагодження параметрів запуску.

У меню **Сервис** виберіть команду **Параметры** запуску. Виберіть потрібні параметри чи введіть потрібні значення (рис. 4). Для одержання додаткових даних про визначений елемент діалогового вікна натисніть кнопку контекстної довідки у верхньому куті вікна і виберіть відповідний елемент.

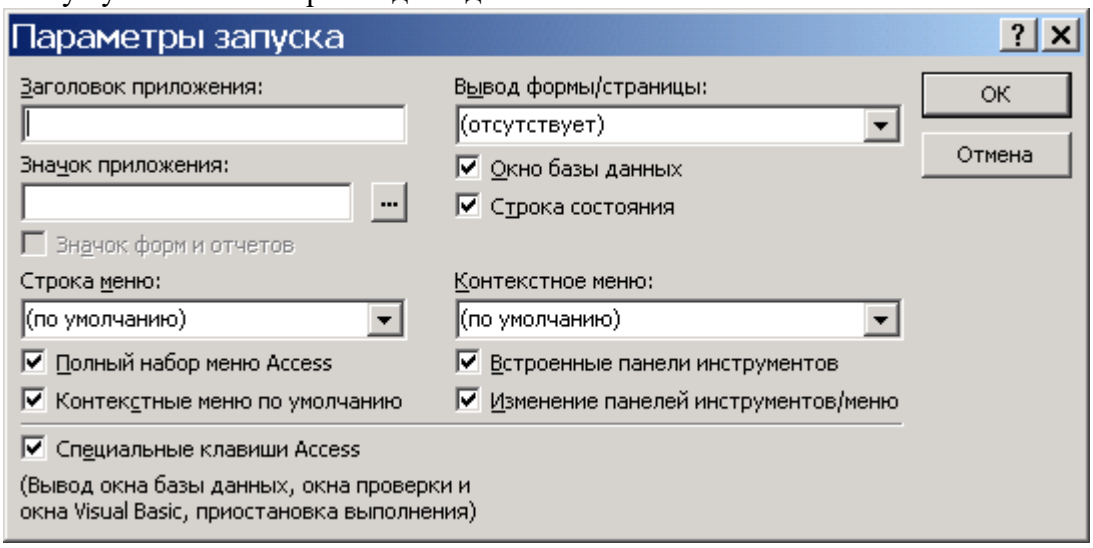


Рис. 4. Вікно відбору параметрів запуску.

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 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 чи мережній файловій системі (у припущенні, що маються відповідні дозволи), можна використовувати наступну операцію.

Відкрийте вікно Провідник Windows чи папку Мій комп'ютер. Знайдіть папку, у якій зберігається файл HTML сторінки доступу до даних. За замовчуванням файл зберігається в одному каталозі з базою даних Microsoft Access. Клацніть правою кнопкою **Файл страницы доступа к данным** (.htm) чи папку, що містить файл, виберіть команду **Свойства** в контекстному меню, а потім установіть прапорець **Только для чтения.**

1.9 Видалення пароля в базі даних Microsoft Access (.mdb)

У меню **Файл** виберіть команду **Открыть**. Відкрийте базу даних у режимі **Монопольно**. У діалоговому вікні **Нужно ввести пароль** уведіть пароль бази даних і натисніть кнопку **OK**. У меню **Сервис** виберіть команди **Защита** і **Удалить пароль базы данных**. Ця команда доступна, коли пароль бази даних уже встановлений. У діалоговому вікні **Удалить пароль базы данных** уведіть поточний пароль.

Створення чи 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 за тим обліковим записом, для якого потрібно створити чи змінити пароль. Для перевірки імені поточної робочої групи чи для зміни робочої групи використовуйте службову програму **Администратор рабочих групп**.

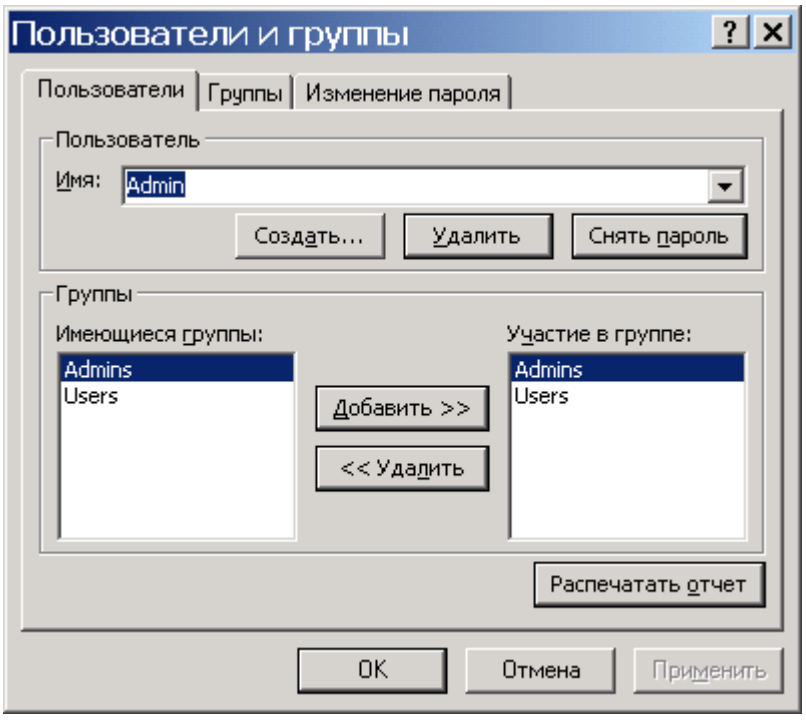


Рис. 5. Вікно користувачів та груп

Відкрийте базу даних. У меню **Сервис** виберіть команду **Защита**, а потім команду **Пользователи и группы** (рис. 5). На вкладці **Изменение пароля** залишіть поле **Текущий пароль** порожнім, якщо обліковий запис раніше не мав пароля. У противному випадку введіть у поле **Текущий пароль** старий пароль. Уведіть новий пароль у поле **Новый пароль**. Повторно введіть новий пароль у поле **Подтверждение** і натисніть кнопку **OK**.

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 чи змінити робочу групу можна за допомогою адміністратора робочих груп.

Відкрийте базу даних. У меню **Сервис** виберіть команду **Защита**, а потім команду **Пользователи и группы**. На вкладці **Пользователи** введіть ім'я облікового запису користувача в поле Имя. Натисніть кнопку **Снять пароль**.

1.10 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) чи базу даних Microsoft Access (.mdb), що містить програму VBA, яку потрібно захистити. У меню **Сервис** вікна бази даних виберіть команду **Макрос** і підкоманду **Редактор Visual Basic** (рис. 6).

Притмітка. Для запуску редактора Visual Basic можна також натиснути клавіші **ALT+F11**. У меню Tools редактора Microsoft Visual Basic виберіть команду **Имя базы данных или проекта Microsoft Access Project Properties**. На вкладці **Protection** установите 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.

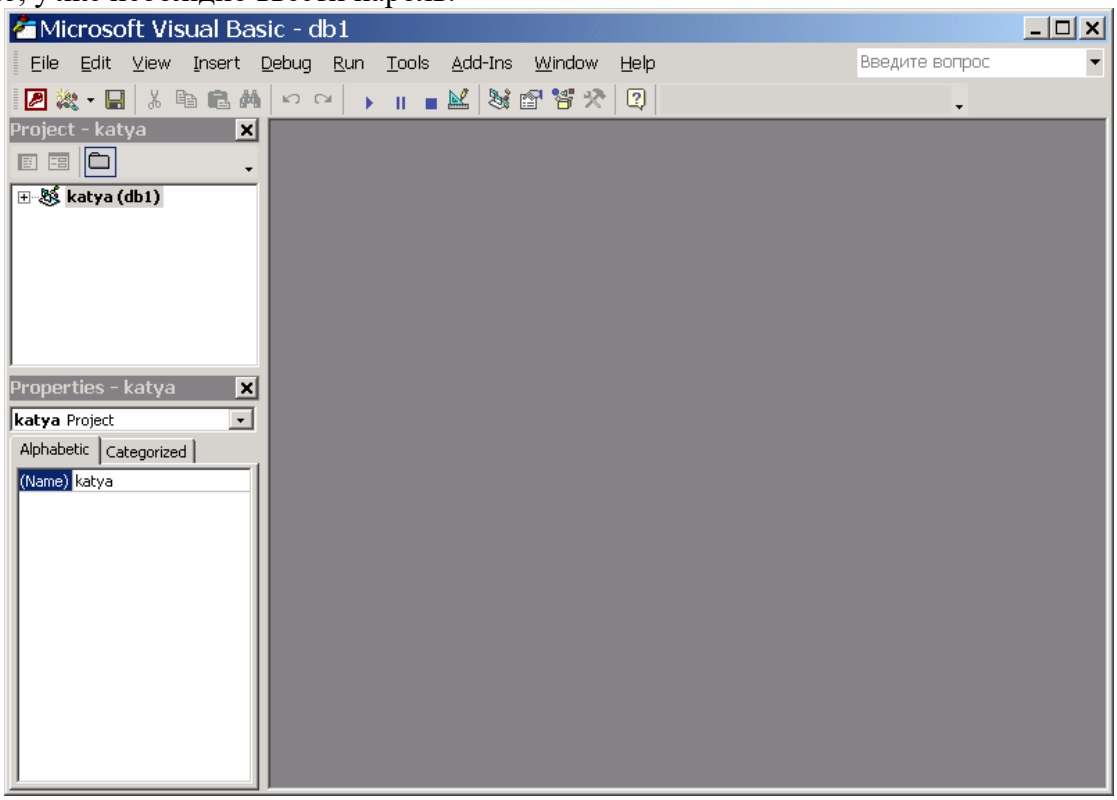


Рис. 6. Вікно редактора Visual Basic

2. Хід роботи.

1. Створити довільну базу даних та встановити на неї пароль бази даних.
2. Зняти з указаної бази даних пароль та встановити на неї пароль облікових записів користувачів.
3. Зняти з указаної бази даних пароль та встановити параметр “прихований” для однієї з таблиць бази даних.
4. Зняти з указаної бази даних параметр прихований, захистити сторінку доступу до даних, встановивши параметр “тільки для читання”.
5. Зняти з указаної бази даних параметр “тільки для читання” та встановити захист паролем програми Microsoft Visual Basic для додатків (VBA).

3. Контрольні питання.

1. Які типи паролів використовуються в програмі MS Access?
2. Вимоги до паролів у програмі MS Access.
3. Де зберігаються окремі типи паролів у програмі MS Access?
4. За яким стандартом шифрується пароль у заголовку файлу?
5. В якому файлі зберігається інформація про користувачів?
6. Порядок установлення, зняття паролю баз даних.
7. Порядок установлення, зняття паролю облікового запису користувача.
8. Порядок установлення, зняття паролю програми Microsoft Visual Basic для додатків.

9. Порядок захисту сторінки доступу.
10. Порядок приховування, відображення елементів баз даних.

Лабораторна робота 8
Захист від фішингових схем в Microsoft Office 2007

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в Microsoft Office від фішингових схем.

Ознайомитись з рівнями захисту комп'ютера, від фішингових схем, установленням та зняттям повідомлень про фішингові атаки.

План

1. Теорія
1.1 Приклади й характеристики фішингових схем
1.2 Стандартні ознаки фішингової схеми
1.3 Захист від фішингу й атак із застосуваннями омограм в Microsoft Office
1.4 Рекомендації із захисту від мережевих шахраїв
1.5 Повідомлення про мережеве шахрайство й крадіжку ідентифікатора.
1.6 Дії з системою безпеки Microsoft Office
1.7 Відключення оповіщень системи безпеки для веб-вузлів шляхом їхньої позначки як надійних вузлів в Internet Explorer
2. Хід роботи
3. Контрольні питання

1. Теорія

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. Мета цих облудних дій – змусити користувача представити порядку, 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 за кредитною картою. Наприклад, American Express використовує в якості цього кода чотиризначне її число на титульній стороні кредитної карти, а Visa, MasterCard і Discover трьохначне число на її 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 імені, 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.
-

1.1 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. Аркуш 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-вузл – зовні вони схожі на справжні. При відвідуванні цих веб-вузлів на комп'ютер може автоматично завантажитися потенційно небезпечне програмне забезпечення, наприклад комп'ютерний Комп'ютерна. 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 (не завжди), 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.

1.2 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 особисті дані. 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, або встановити шпигунське ПЗ. 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 правильну URL-Адресу в папку «Вибране» веб-оглядача. Не слід копіювати URL із повідомлень у вікно веб-оглядача через буфер обміну. Зловмисники можуть використовувати для підробки посилань наступні методи.
  - Маскування посилань. Навіть якщо запропоноване посилання містить повністю або частково назву існуючої компанії, вона може бути «маскованою». Це означає, що відображуване посилання здійснює перехід із 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 полі 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 все, 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 домену 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.

1.3 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. 1):

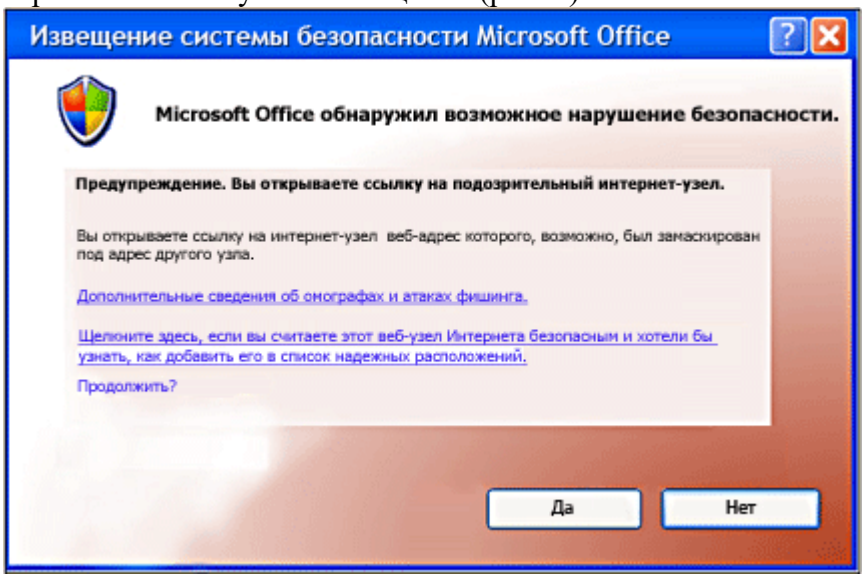


Рис. 1 Вікно повідомлення про підроблене посилання

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 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. 2).

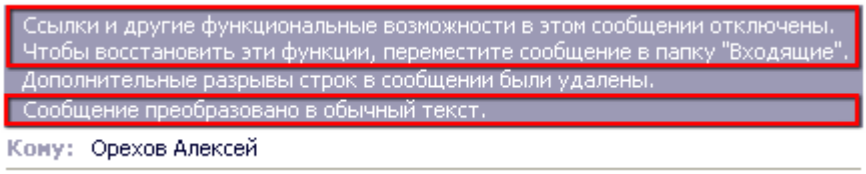


Рис. 2 Вікно інформаційної панелі

Якщо клацнути посилання, що було відключено в повідомленні фішингу, відобразиться діалогове вікно Безпека Outlook (рис. 3).

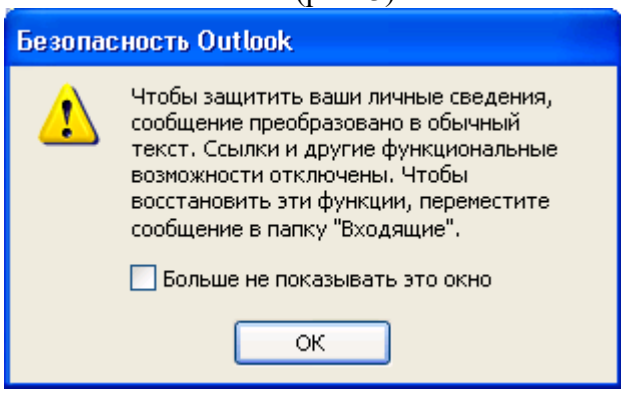


Рис. 3 Вікно безпека Outlook.

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

1.4 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 цифрової 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 номери кредитної карти, які великі компанії з випуску кредитних карт стали надавати своїм клієнтам для покупок у мережі.

1.5 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.

1. У додатку Outlook виберіть, але не відкривайте повідомлення, про яке потрібно повідомити.
2. У меню **Действия** виберіть команду **Переслать** як вкладення, або натисніть сполучення клавіш **CTRL+ALT+F.**

3. 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.

4. Натисніть кнопку Відправити.

1.6 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.

1. Натисніть **кнопку Microsoft Office**  , а потім кнопку **Параметры**, наприклад, в Word (рис. 4).

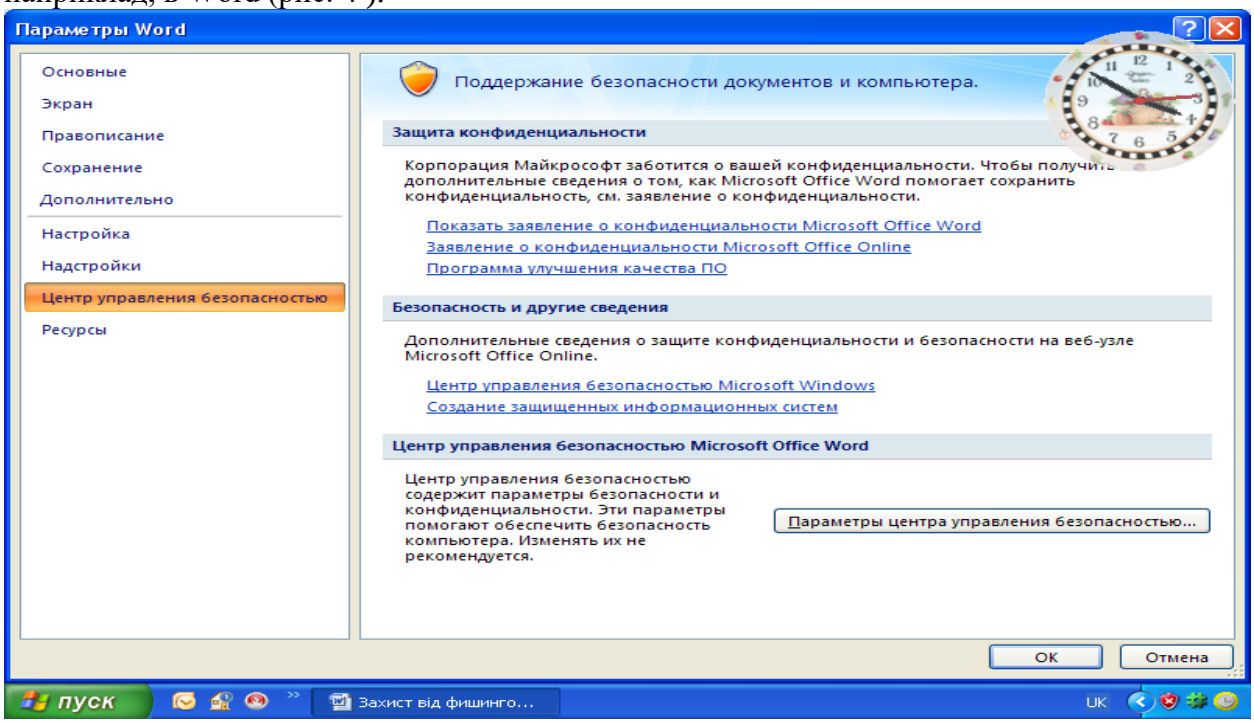


Рис. 4 Вікно параметрів Word

2. Виберіть категорію **Центр управления безопасностью**, натисніть кнопку **Параметры центра управления безопасностью**, і перейдіть у категорію **Параметры конфинденциальности (рис. 5).**

3. Зніміть прапорець **Проверка документов Microsoft Office, полученных от подозрительных веб-узлов** або утримуючих посилань на такі веб-вузли. Visio і InfoPath

1. У меню **Сервис** виберіть команду **Центр управления безопасностью,** і клацніть **Параметры конфинденциальности**.

2. Зніміть прапорець **Проверка документов Microsoft Office, полученных от подозрительных веб-узлов** або утримуючих посилань на такі веб-вузли.

1.7 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**.

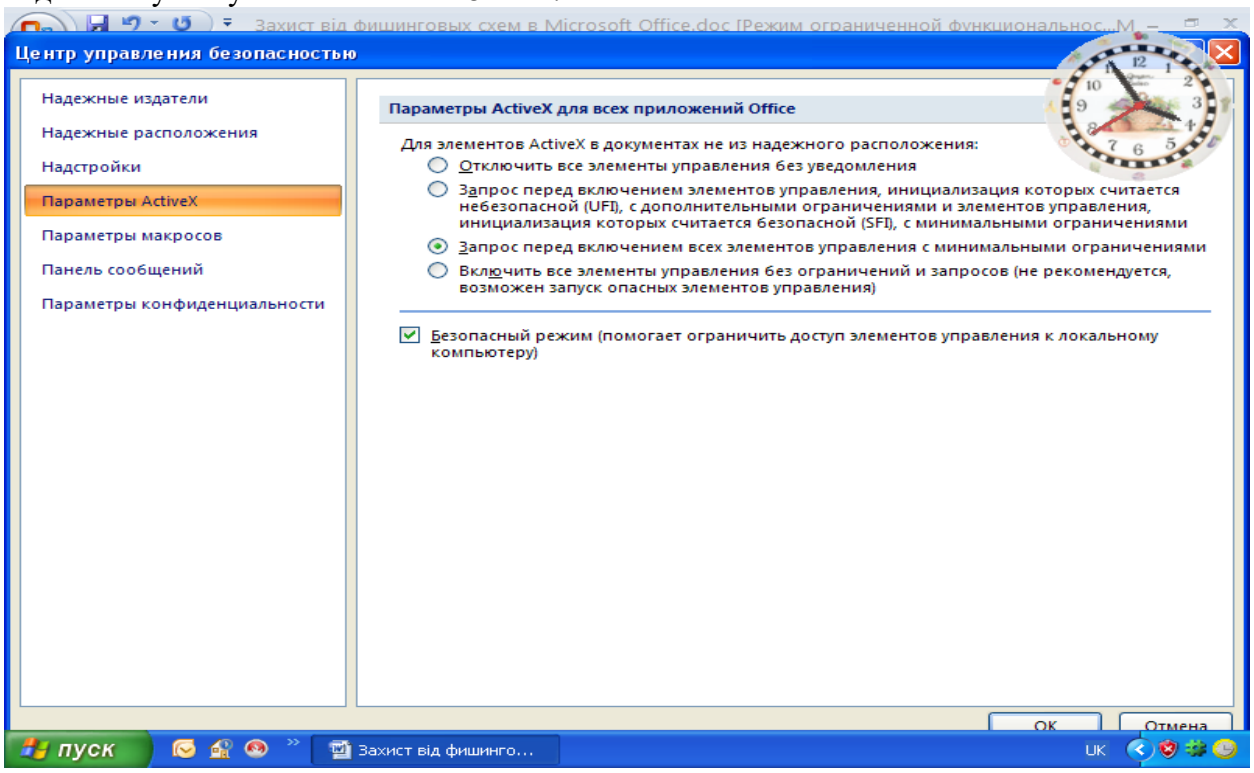


Рис. 5 Вікно відключення повідомлень на підозрілі адреси

Додавання веб-вузла в зону надійних вузлів

1. В оглядачі Internet Explorer версій 5, 6 або 7 виберіть у меню **Сервис** команду **Свойства пользователя**.
2. На вкладці **Безопасность** клацніть значок **Надежные узлы**, а потім натисніть кнопку **Узлы**.
3. У поле **Добавить узел** у зону введіть або виберіть адресу конкретного веб-вузла, а потім натисніть кнопку **Добавить**.
4. 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:).
5. Двічі натисніть кнопку **ОК**.

2. Хід роботи

1. Відключити виявлення підроблених доменних імен за замовчуванням у додатках Word, Excel, PowerPoint і Access.

2. Включити виявлення підроблених доменних імен за замовчуванням замовчуванням у додатках Word, Excel, PowerPoint і Access.
3. Відключити виявлення підроблених доменних імен за замовчуванням в Internet Explorer.
4. Включити виявлення підроблених доменних імен за замовчуванням в Internet Explorer.

3. Контрольні питання

1. Фішинг та його основні характеристики
2. Приклади й характеристики фішингових схем
3. Стандартні ознаки фішингової схеми
4. Підозрілі посилання в повідомленнях електронної пошти
5. Рекомендації із захисту від мережевих шахраїв
6. Повідомлення про мережеве шахрайство й крадіжку ідентифікатора.
7. Дії із системою безпеки Microsoft Office
8. Відключення оповіщень системи безпеки для веб-вузлів шляхом їхньої позначки як надійних вузлів в Internet Explorer

Лабораторна робота 9
Захист інформації в Microsoft WORD 2007

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в Microsoft WORD

Ознайомитись з рівнями захисту документа та його елементів порядком створення сертифікату та його приєднання до документа.

План

1. Теорія

1.1 Захист документа від небажаних змін і приміток

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

Дозвіл на внесення приміток і записаних виправлень

1. На вкладці **Рецензирование** в групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничить форматирование и редагирование (рис. 1)**.
2. Для вказівки стилів, які рецензент зможе застосовувати або змінювати, в області завдань **Защита документа** в групі **Ограничение на форматирование** встановіть прапорець **Ограничить набор разрешенных стилей (рис. 2)**, а потім клацніть **Настройка**.
3. У групі **Ограничение** на редагування встановіть прапорець **Разрешить только этот способ редактирования документа**.
4. У списку обмежень на редагування виберіть пункт **Запись исправлений**. (Сюди входять примітки, а також вставлений, вилучений і переміщений текст.)

Примітка. Для додаткових можливостей захисту використовуйте службу **Active Directory**, клацніть **Ограничить разрешение**, щоб скористатися керуванням правами на доступ до даних.

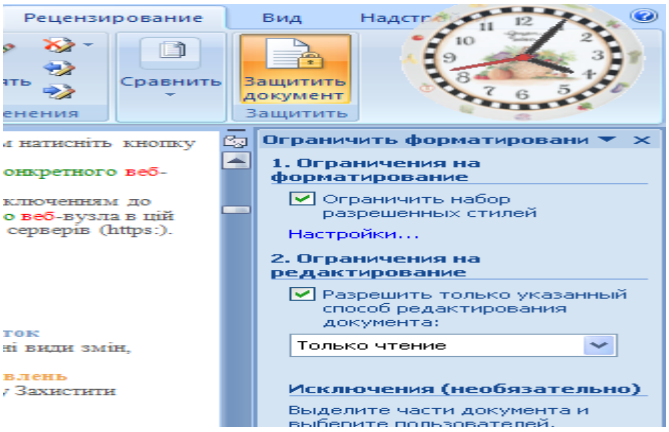


Рис. 1 Вікно налагодження обмежень

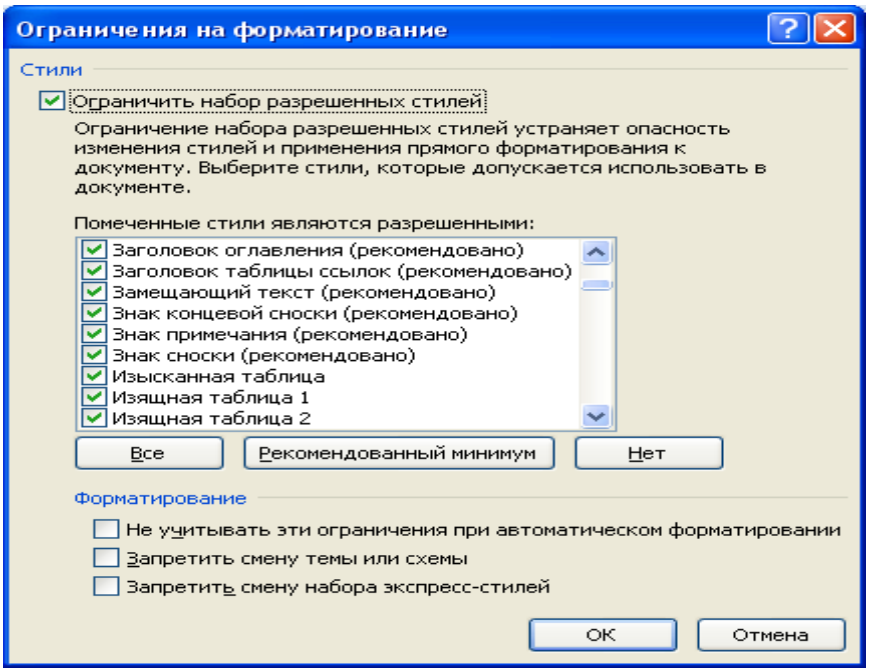


Рис. 2 Вікно відбору дозволених стилів

1. У групі **Включить** захист натисніть кнопку **Да**, включити захист.
2. Для установки пароля на документ і надання паролю користувачам можливості зняти захист уведіть пароль у поле **Новый пароль** (необов'язково), а потім підтвердіть його.

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

Дозвіл тільки на додавання приміток

1. На вкладці **Рецензирование** в групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничить редагирование.**
2. В області завдань **Защита** документа в групі **Ограничение на редагирование** встановіть прапорець **Разрешить только этот способ редактирования документа**.
3. У списку обмежень на редагування виберіть необхідний 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 із ім'ям користувача або групи користувачів для перегляду області, або всіх областей, доступних даному користувачеві, або групі користувачів для внесення змін, або зняття дозволу для певного користувача, або групи.

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

1. У групі **Включить защиту** натисніть кнопку **Да**, включити захист.
2. Для установки пароля на документ і надання паролю користувачам можливості зняти захист уведіть пароль у поле **Новый пароль** (необов'язково), а потім підтвердіть його (рис. 3)

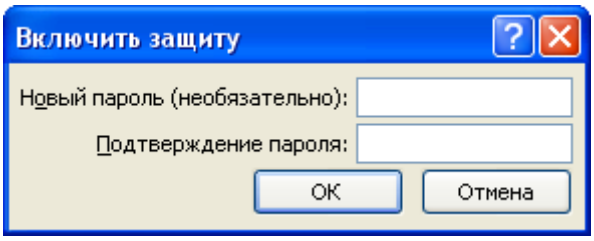


Рис. 3 Вікно введення паролю

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

Зняття захисту від додавання приміток і виправлень

1. На вкладці **Рецензирование** в групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничение на форматирование и редагирование**.
2. В області завдань **Защита** документа натисніть кнопку **Включить защиту**.

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

1.2 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 **Сервис** (рис. 4), а потім виберіть **Общие параметры** (рис. 5).

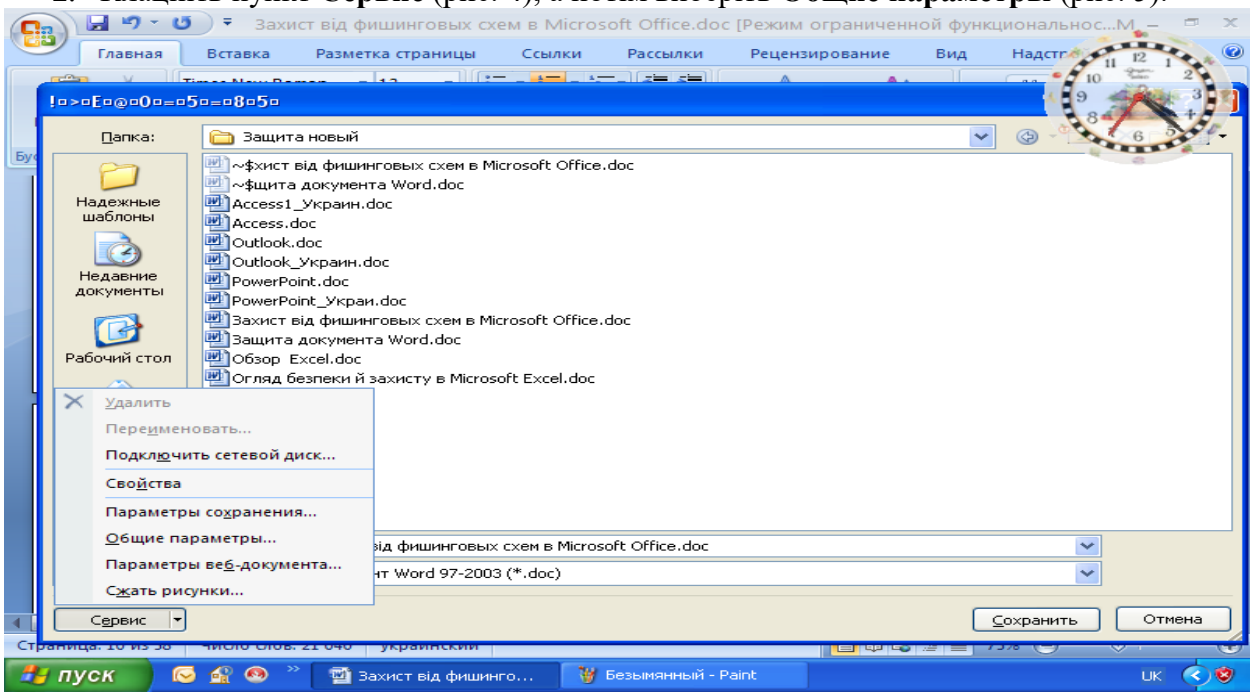


Рис. 4 Вікно збереження документа

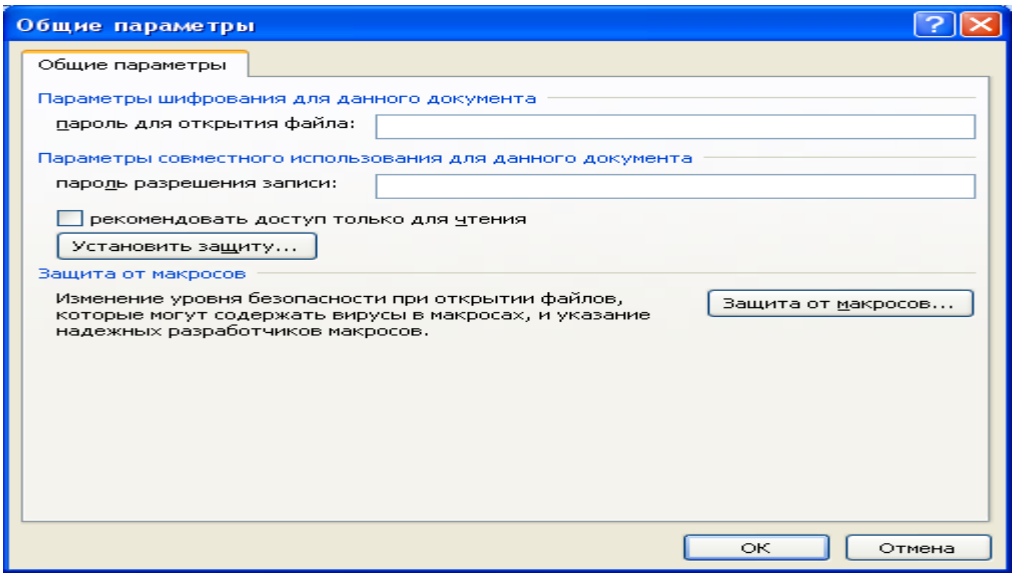


Рис. 5 Вікно введення паролів

3. Виконайте наступні дії:
   - Якщо потрібно, щоб рецензенти вводили пароль перед переглядом документа, уведіть пароль у поле **Пароль на открытие**.
   - Якщо потрібно, щоб рецензенти вводили пароль перед збереженням внесених у документ змін, уведіть пароль у поле **Пароль для изменений**.

Примітка.

- 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 **Рекомендовать только для чтения**. При відкритті файлу рецензентам буде запропоновано відкрити його в режимі **только для чтения**.
2. Натисніть кнопку **ОК**.
3. При запиті підтвердити пароль уведіть його ще раз, а потім натисніть кнопку **ОК**.
4. Натисніть кнопку **Сохраниить**.
5. Якщо піде запрошення, натисніть кнопку **Да**, щоб замінити існуючий документ.

1.3 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 **Сохранить как**

Клацніть пункт **Сервис**, а потім виберіть **Общие параметры** (рис. 6).

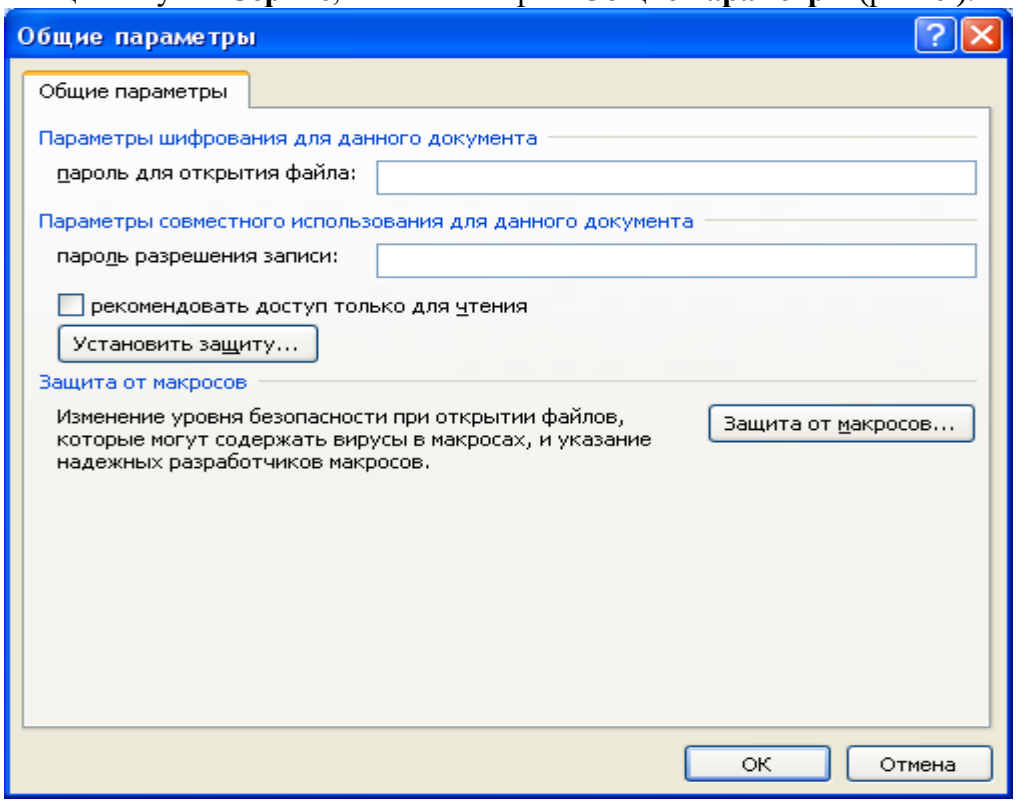


Рис. 6 Вікно введення паролів для книги.

Виконайте наступні дії:

1. Якщо потрібно, щоб рецензенти вводили пароль перед переглядом книги, уведіть пароль у поле **Пароль на открытие**.
2. Якщо потрібно, щоб рецензенти вводили пароль перед збереженням внесених у книгу змін, уведіть пароль у поле **Пароль для изменений**.

Примітка. 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. 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 **Рекомендовать только для чтения**. 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 **Сохранить**.
7. Якщо піде запрошення, натисніть кнопку **Да**, 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 **Сохранить как**.
3. Клацніть пункт **Сервис**, а потім виберіть **Общие параметры**.
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 **Сохранить**.
8. Якщо піде запрошення, натисніть кнопку **Да**, 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 Office , а потім виберіть команду **Сохранить как**.
3. Клацніть пункт **Сервис**, а потім виберіть **Общие параметры**.
4. Виберіть пароль, а потім натисніть клавішу **DEL**.
5. Натисніть кнопку **ОК**.
6. Натисніть кнопку **Сохранить**.
7. Якщо піде запрошення, натисніть кнопку **Да**, щоб замінити існуючий файл.

1.4 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 **Разработчик** в групі **Элементы управления** виберіть пункт **Свойства** рис. 7.

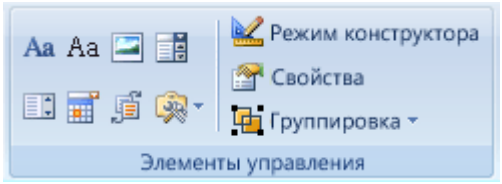


Рис. 7 Вікно відбору властивостей

4. У діалоговому вікні **Свойства** елемента керування вмістом у групі **Блокирование** виконайте наступні дії.
   - Установіть прапорець **Элемент управления содержанием нельзя удалить**, що дозволяє редагування елемента керування вмістом, але забороняє видалення елемента керування вмістом із форми.
   - Установіть прапорець **Содержание нельзя редагировать**, що дозволяє видалення елемента керування, але забороняє редагування вмісту в елементі керування.

Примітка. Цей варіант недоступний для всіх елементів керування.

Якщо вкладка **Разработчик** недоступна, натисніть **кнопку Microsoft Office** і клацніть **Основные** й потім установіть прапорець **Показывать на ленте вкладку разработчик** (рис. 8). Visio, Outlook або Publisher

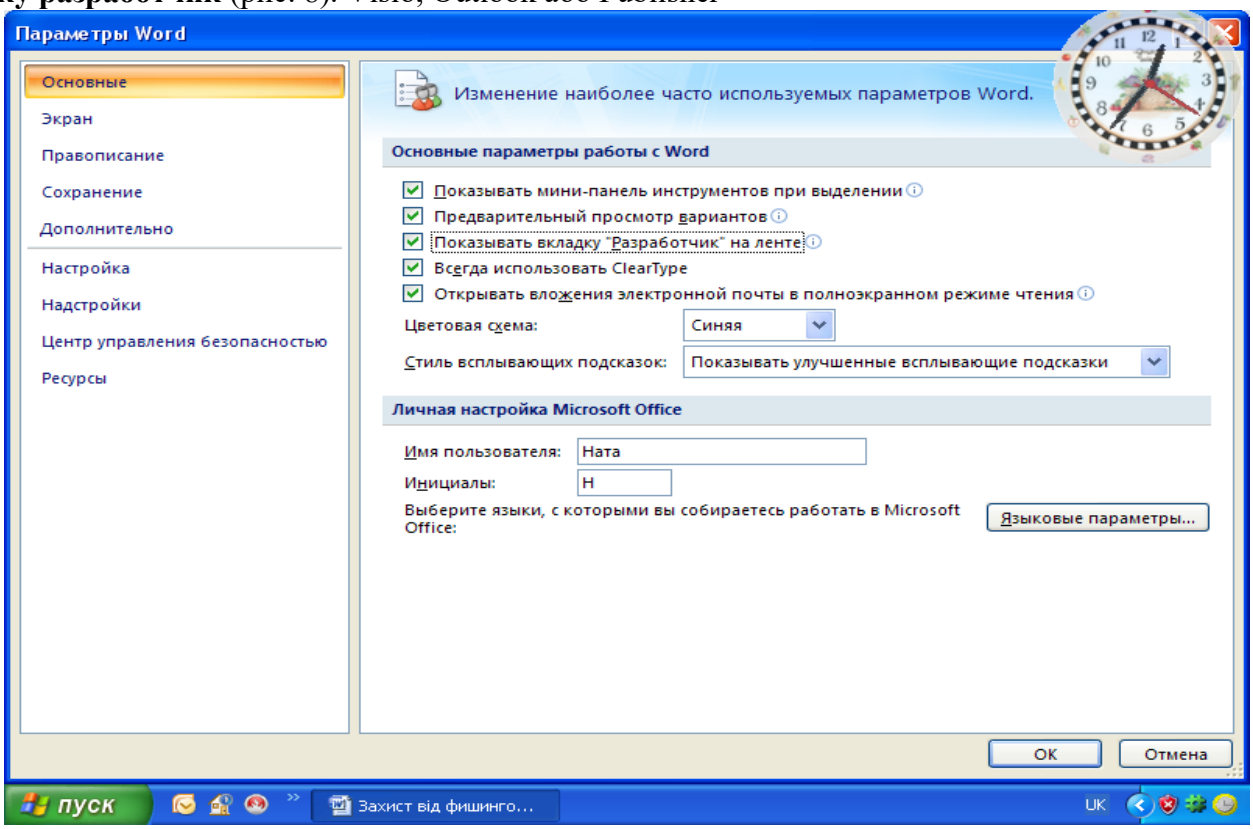


Рис. 8 Вікно встановлення вкладки Розроблювач

Додавання захисту всього вмісту форми

1. Відкрийте форму, яку необхідно захистити.
2. Нажавши кнопку **Режим конструктора** в групі **Элементы управления**, переконайтеся, що не використовується режим конструктора.
3. На вкладці **Разработка** в групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничить форматирование и редагирование**.
4. В області завдань **Защита документа** в групі **Ограничение на редагирование** встановіть прапорець **Разрешить только указанный способ редагирования документа**.
5. У списку обмежень редагування виберіть пункт **Введение данных поля форм**.
6. У групі **Включить защиту** натисніть кнопку **Да**, включити захист.
7. Для призначення пароля для документа, щоб тільки знаючі його користувачі могли видалити захист, уведіть пароль у вікні **Новый 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 **Элементы управления** на вкладці **Разработчик**.
2. На вкладці **Разработчик** у групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничить форматирование и редагирование**.

3. В області завдань **Защитить документ** у групі **Ограничение на редагирование** встановіть прапорець **Разрешить только указанный способ редагирования документа.**
4. У списку обмежень редагування виберіть пункт **Введение данных поля форм**.
5. У групі **Включить защиту** натисніть кнопку **Да**, включити захист.
6. Для призначення пароля для документа, щоб тільки користувачі, що знають його, могли видалити захист, уведіть пароль у вікні **Новый пароль** (необов'язково), а потім підтвердіть пароль.

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

Розблокування форми

1. На вкладці **Разработчик** у групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничение на форматирование и редагирование**.
2. В області завдань **Защитить документ** натисніть кнопку **Отключить защиту**

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

1.5 Дозвіл вибіркового виправлення захищеного документа

Після установки захисту документа шляхом вибору параметрів **Только чтение** або **Примечания в области заданий /Защитить документ** 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 **Рецензирование** групі **Защита** виберіть команду **Защитить документ,** і потім клацніть **Ограничить форматирование и редагирование**.
2. В області завдань **Ограничение на форматирование и редагирование** виберіть команду **Отключить документ**.
3. Якщо документ уже був захищений паролем, у діалоговому вікні **Снять защиту** 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 **Снять защиту** установіть прапорець **Группы**.
8. Щоб дозволити тільки персональне редагування обраних фрагментів, виберіть пункт **Другие пользователи**, 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 **Группа как элементы**; 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 **Включить защиту** натисніть кнопку **Да**, включити захист.
3. Виконайте одну з наступних дій.
4. Щоб призначити пароль документу, і щоб знаючі пароль користувачі могли зняти захист, уведіть пароль у поле Новый пароль (необов'язково), а потім підтвердіть його.

5. Щоб зашифрувати документ, для того щоб тільки авторизовані власники могли зняти захист, клацніть **Проверка действительности пользователя.**

- .

1.6 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, **Параметры** Word.
2. Відкрийте сторінку **Центр управления безопасность**, натисніть кнопку **Параметры центра управления безопасностью,** і потім натисніть кнопку **Параметры конфиденциальности** (рис. 9).

1.7 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 **Выполнить**.
3. Щоб запустити консоль керування MMC, у вікні Відкрити введіть **mmc.exe** (рис. 10).
4. Щоб відкрити діалогове вікно **Добавить, или удалить оснащение**, у меню **Консоль** (рис. 11) консолі керування клацніть **Добавить,** або видалити оснащення.
5. Щоб відкрити діалогове вікно **Добавить изолированное оснащение**, натисніть кнопку **Добавить**.
6. У списку Додати ізольоване оснащення виберіть пункт **Сертификаты**, а потім натисніть кнопку **Добавить**.
7. У діалоговому вікні **Оснащение диспетчера сертификатов** виберіть пункт **Моей учетной записи пользователя** й клацніть **Готово**.
8. У діалоговому вікні **Добавить изолированное оснащение** клацніть **Закрыть**, а потім натисніть кнопку **ОК** у діалоговому вікні **Добавить или удалить оснащение**.
9. Перейдіть на рівень кореневої папки дерева консолі й клацніть +, зображений поруч із пунктом **Сертификаты - пользователь**, щоб розгорнути вузол.

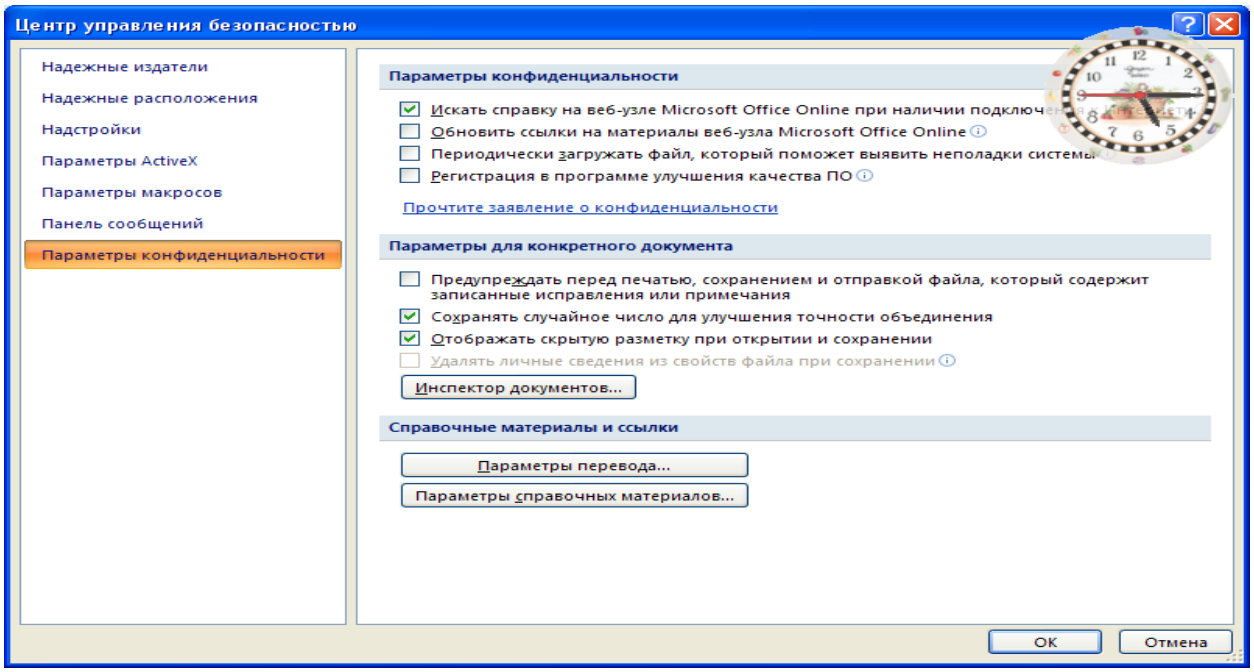


Рис. 9 Вікно параметрів конфіденційності

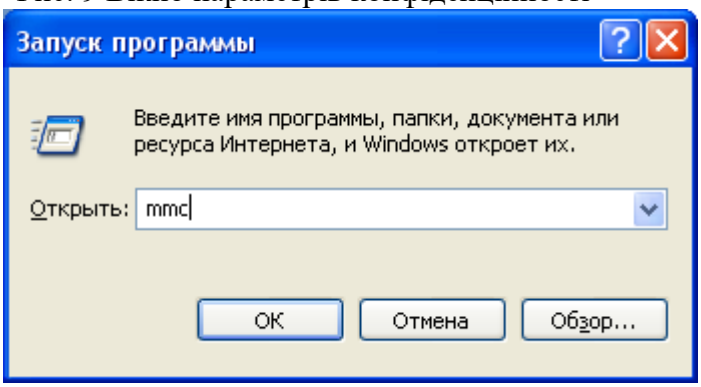


Рис. 10 Вікно запуску консолі

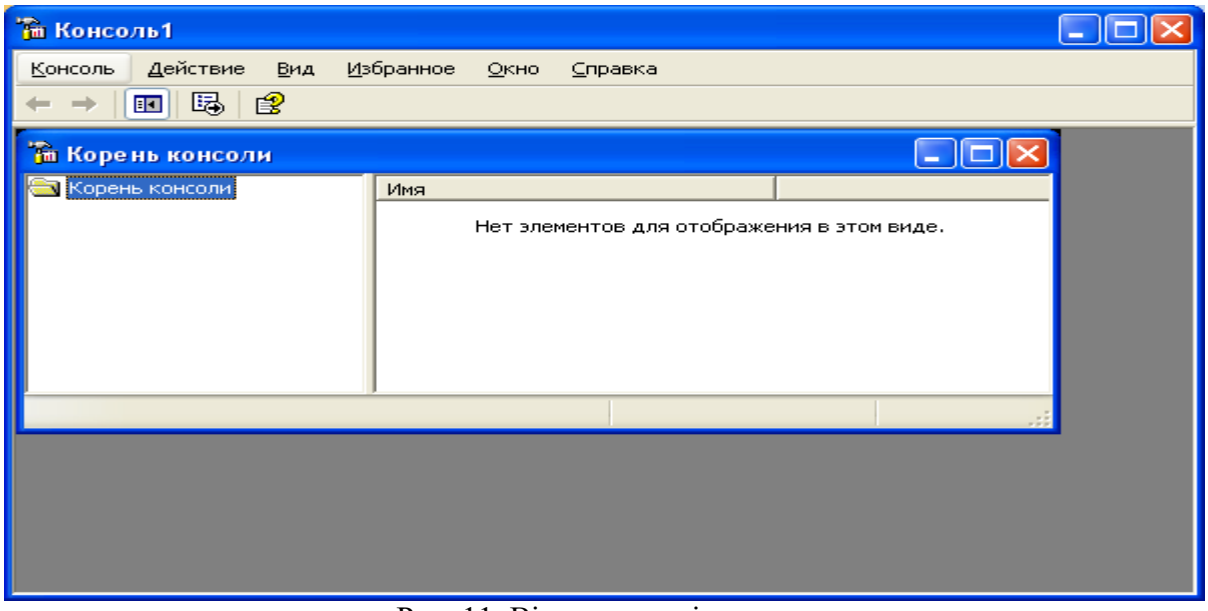


Рис. 11 Вікно консолі

10. У розгорнутому вузлі виділіть пункт **Личные**.
11. У меню **Действия** виберіть пункт **Все задачи**, потім - пункт **Импорт**.
12. Щоб вибрати місце розташування сертифіката, підготовленого на першому кроці, на другому екрані майстра натисніть кнопку **Осмотр**, а потім натисніть кнопку **Далее**.
13. Уведіть пароль у вікні **Пароль,** і зніміть обидва прапорці **Включить усиленную защиту закрытого ключа, і Позначить этот ключ как экспортированный**. Щоб перейти на наступну сторінку, натисніть кнопку **Далее**.
14. Установіть прапорець **Поместить все сертификаты в тайник,** і виберіть **тайник сертификатов как личный**. Щоб перейти на наступну сторінку, натисніть кнопку **Далее**.
15. Щоб вийти з майстра імпорту сертифікатів натисніть кнопку **Готово**.
16. Підтвердіть повідомлення, що імпорт був завершений.
17. З вузла в групі **Сертификаты** - поточний користувач клацніть вузол **Доверенный узлы сертификации** або вузол **Промежуточные узлы сертификации**.
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 **Вибор сертификата**.

2. Хід роботи

1. Відкрити документ та встановити захист документа від небажаних змін і приміток
2. Установити дозвіл на внесення приміток і записаних виправлень
3. Установити дозвіл тільки на додавання приміток
4. Зняти захист від додавання приміток і виправлень
5. Установити пароль для відкриття й зміну документа
6. Установити пароль для файлу
7. Змінити пароль для файлу
8. Додати захист в оперативну форму
9. Блокувати форму
10. Розблокувати форму
11. Створити дозвіл вибіркового виправлення захищеного документа
12. Провести Перегляд параметрів конфіденційності
13. Створити сертифікат

3. Контрольні питання

1. Дозвіл на внесення приміток і записаних виправлень
2. Дозвіл тільки на додавання приміток
3. Зняття захисту від додавання приміток і виправлень
4. Установка пароля для відкриття й зміну документа
5. Рекомендації до паролів, що використовуються
6. Установка пароля для файлу
7. Призначення паролю на відкриття та зміну файлу.
8. Додавання захисту в оперативну форму

9. Блокування форми
10. Розблокування форми
11. Дозвіл вибіркового виправлення захищеного документа
12. Перегляд параметрів конфіденційності
13. Створення сертифікату

Лабораторна робота № 10
Захист інформації в Microsoft Excel 2007

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в Microsoft Excel

Ознайомитись з рівнями захисту файлів та їх елементів порядком створення сертифікату для постановки підпису.

План

1. Теорія
   Використання паролів для захисту книги
   .2 Захист окремих елементів книги й листа
   .3 Основні відомості про безпеку макросів
   .4 Одержання цифрового сертифіката для постановки підпису
2. Хід роботи
3. Контрольні питання

Теорія

В Microsoft Excel передбачено кілька рівнів захисту для керування доступом до даних 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.

1.1 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.

1.2 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 Аркуш, 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

Виберіть Аркуш, який потрібно захистити.

Щоб розблокувати всі комірки або діапазони, які повинні бути доступні іншим користувачам для зміни, виконайте наступні дії:

Виберіть послідовно всі комірки або діапазони, які потрібно розблокувати.

На вкладці **Главная** в групі **Ячейки** клацніть **Формат**, а потім виберіть команду **Формат ячеек** (рис. 1).

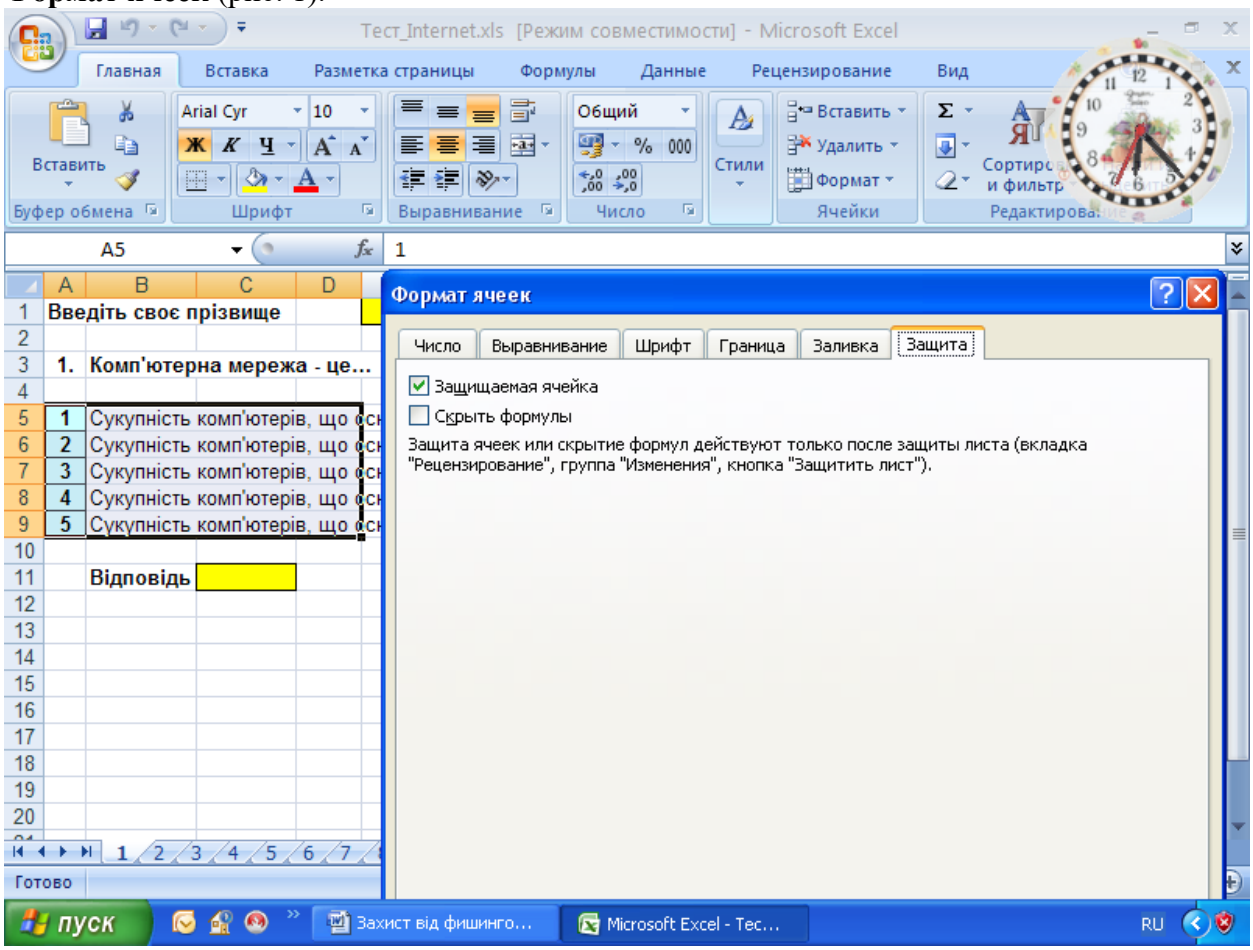


Рис. 1 Вікно захисту комірок

На вкладці **Защита** зніміть прапорець **Не обязательная связь** і натисніть кнопку **ОК**.

Щоб сховати всі формули, які не повинні відображатися, виконайте наступні дії:

Виберіть на листі комірки, що містять формули, які необхідно сховати.

На вкладці **Главная** в групі **Ячейки** клацніть **Формат**, а потім виберіть команду **Формат ячеек**.

На вкладці **Защита** установіть прапорець **Спрятанный** і потім натисніть кнопку **ОК**.

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. 2).

На стрічці з'явиться вкладка **Работа** з малюнками або **Засобы рисования**, що містить вкладку **Формат**.

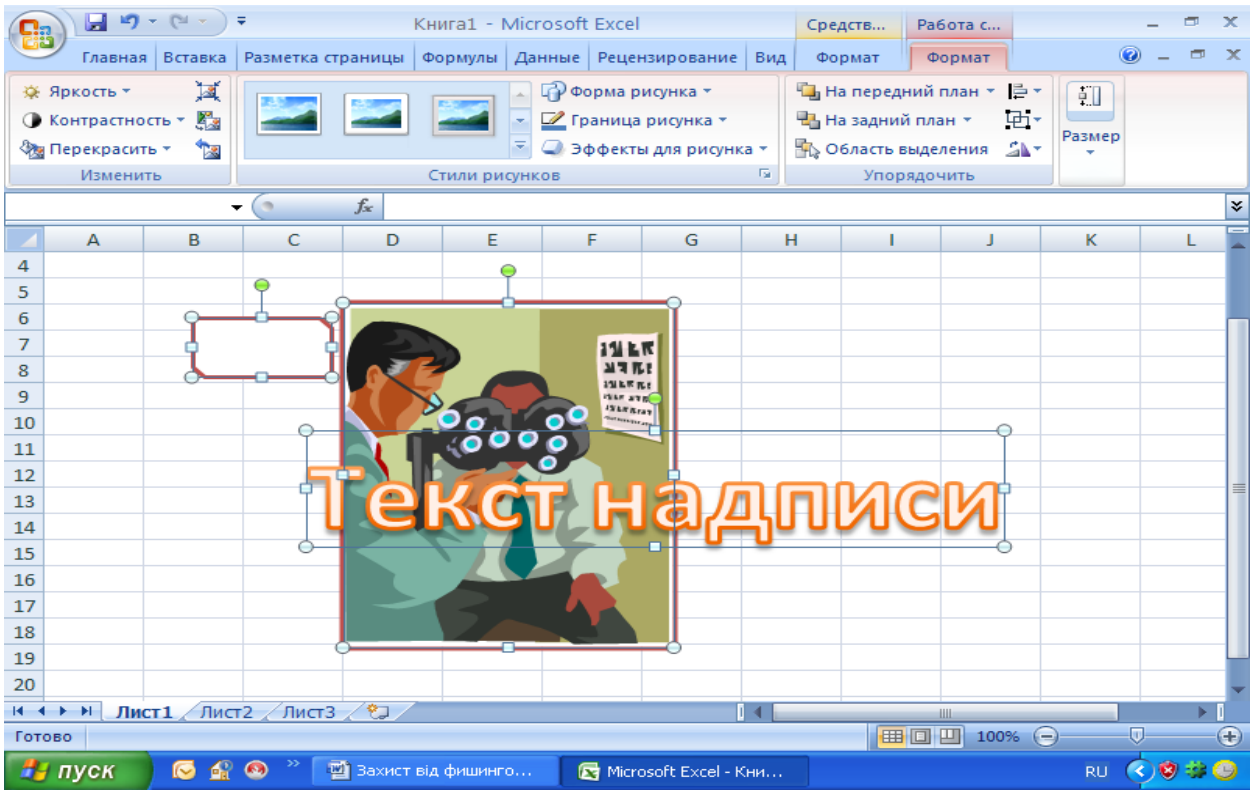


Рис. 2 Графічні проекти

Примітка. Можна також використовувати команду **Перейти** для швидкого вибору всіх графічних проектів на листі (рис. 3). На вкладці **Главная** в групі **Редагирование** натисніть кнопку **Найти и выделить**, а потім виберіть команду **Перейти**. Натисніть кнопку **Виделить**, а потім виберіть пункт **Объєкты.**

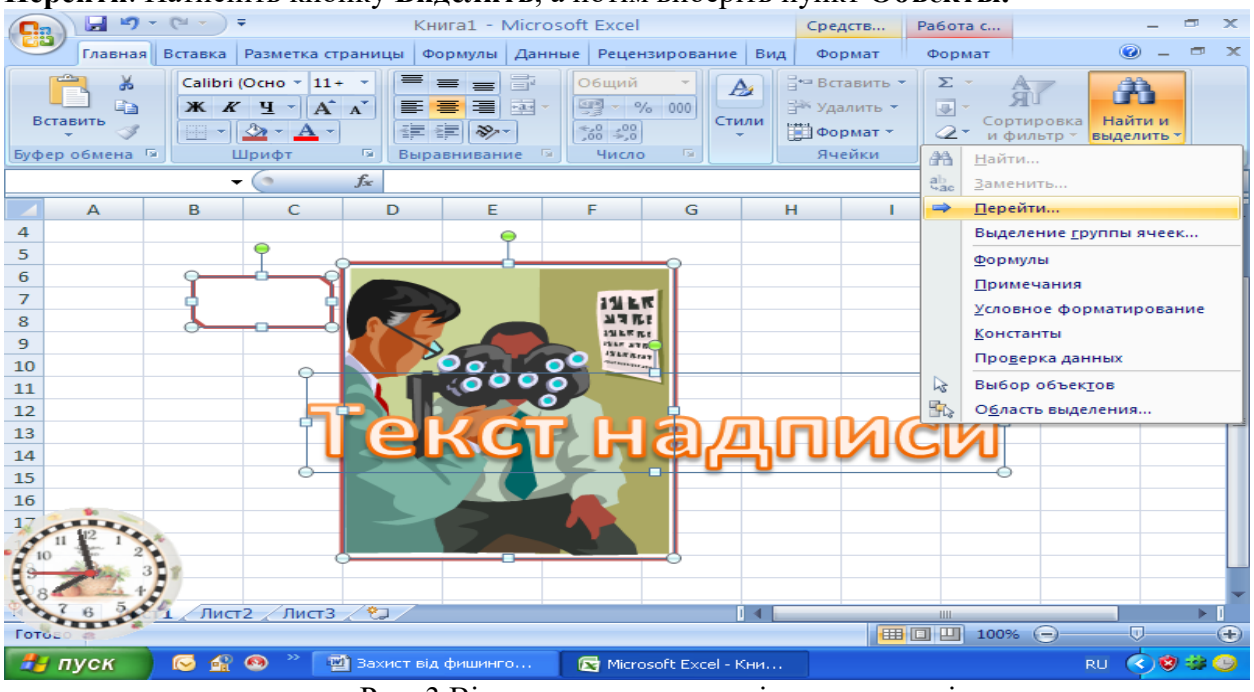


Рис. 3 Вікно переходу до виділення проектів

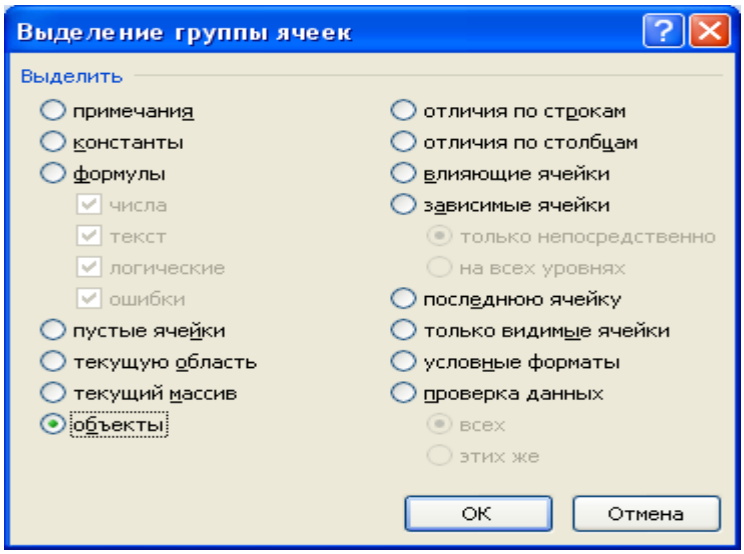


Рис. 4 Вікно відбору проектів

1. На вкладці **Формат** у групі **Размер** натисніть кнопку виклику діалогового вікна **размер и свойства** поруч із кнопкою **Размер** (рис. 5).
2. На вкладці **Свойства** зніміть прапорець **Защита ячейки**, а також прапорець **Заблокировать 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.

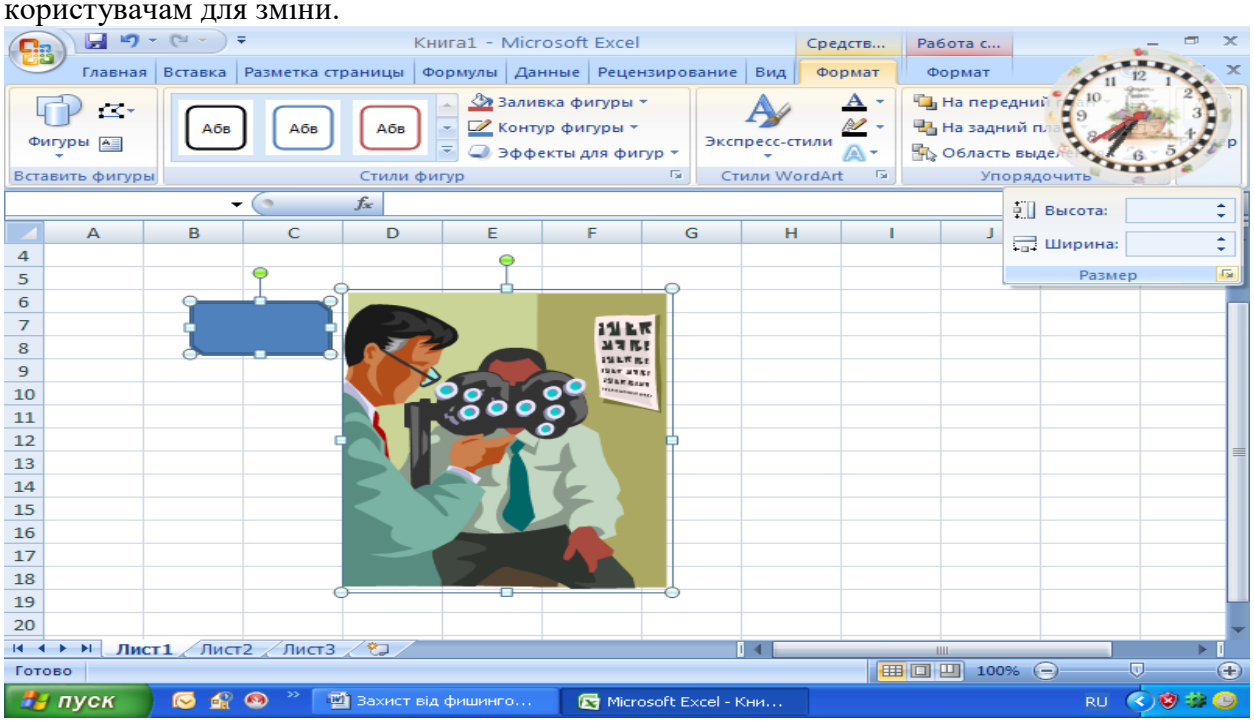


Рис. 5 Вікно відкриття діалогового вікна Розмір та Властивості

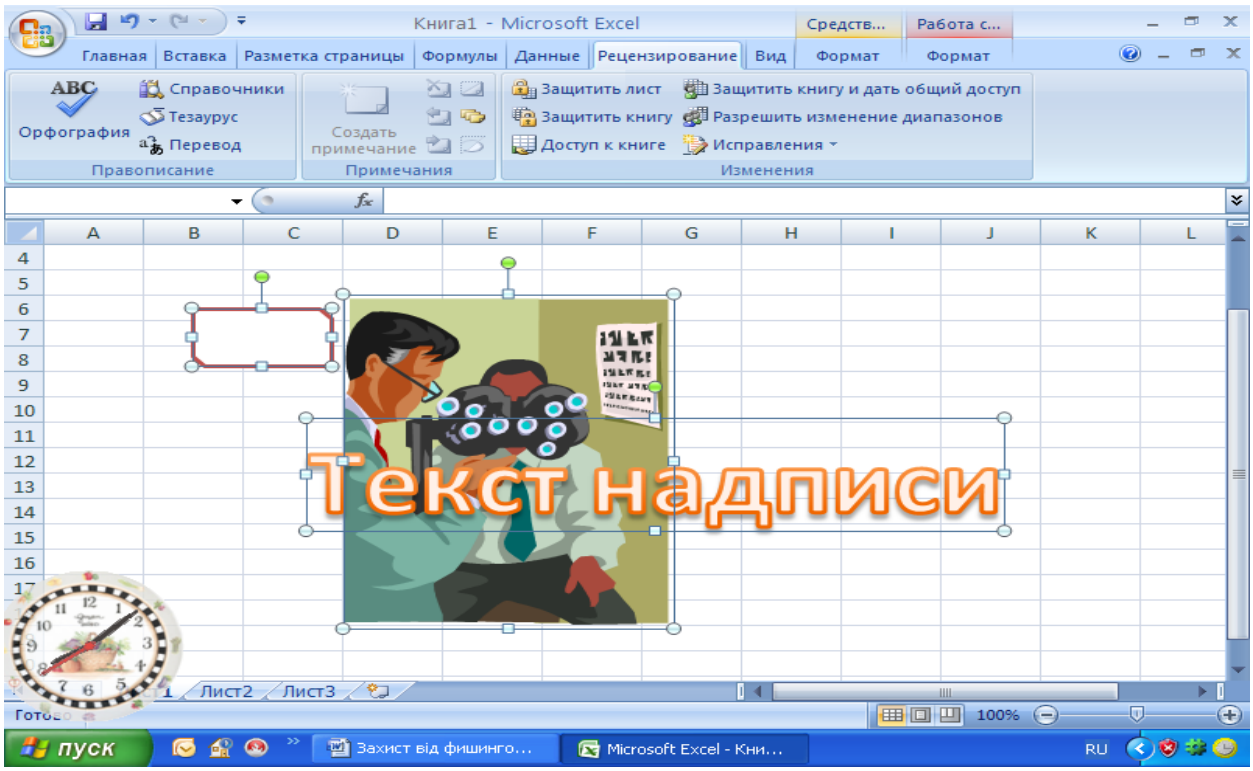


Рис. 6 Вікно відбору команди Захист листа

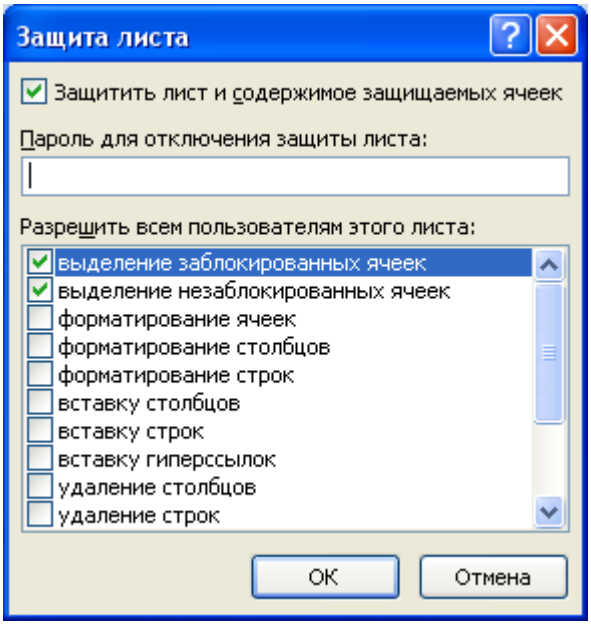


Рис. 7 Вікно дозволу визначених параметрів користувачам

3. На вкладці **Рецензирование** групі **Изменения** виберіть команду **Защитить лист** (рис. 6).
4. У списку **Разрешить всем пользователям** цього листа відзначте прапорцями елементи, зміна яких повинна бути доступною користувачам (рис. 7).
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.

Таблиця 1

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 Налагодження 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 Налагодження цього параметра.
використання звітів зведеної таблиці	Форматувати, змінювати макет, обновляти або змінювати яким-небудь іншим способом Інтерактивний, 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 видалення цих сценаріїв. Користувачі можуть змінювати значення в

	змінюваних комірках, якщо комірки не захищені, і додавати нові сценарії.

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 **Рецензирование** групі **Изменения** виберіть команду **Защитить книгу**.
2. У розділі **Защитить 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 **Окна** (рис. 8).

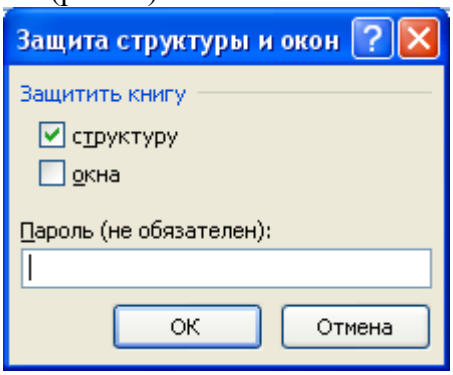


Рис. 8 Вікно захисту книги.

Таблиця 2

Структура	Перегляд аркушів, які були сховані. Переміщення, видалення, приховання або перейменування аркушів. Вставку нових аркушів або листів діаграм (Аркуш діаграми. Аркуш 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 Аркуш, а не на окремий Аркуш діаграми. Впроваджені діаграми зручні для перегляду або друку звіту зведеної діаграми разом з вихідними даними і іншими довідками, які містяться на листі.) впроваджений Аркуш. Переміщення або копіювання аркушів в іншу книгу. У звітах зведеної таблиці -

можна

	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.

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 журналу, які будуть загублені при закритті загального доступу до книги, виконайте наступні дії:
   1. На вкладці **Рецензирование** групі **Изменения** виберіть команду **Исправления**, а потім виберіть у списку пункт **Выделять исправления**.
   2. Зніміть прапорець **Отслеживать изменения** (рис. 9).

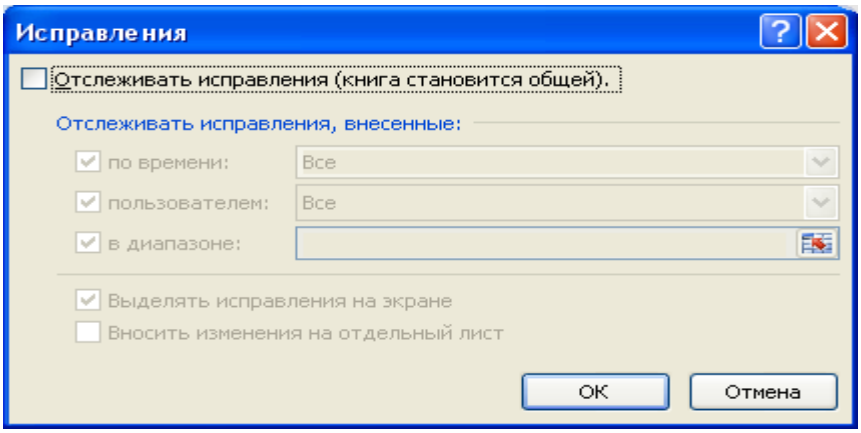


Рис. 9 Вікно відбору параметрів

3. Установіть прапорець **Вносить изменения на отдельный лист**, а потім натисніть кнопку **ОК**.
   Виконайте одну з наступних дій:

1. Щоб надрукувати Аркуш журналу, натисніть кнопку **Печать** .
2. Щоб скопіювати журнал в іншу книгу, виділіть комірки, які потрібно скопіювати, натисніть кнопку **Копировать** на вкладці **Главная** в групі **Буфер обмена**, перемкніться у вікно іншої книги, виберіть місце для розміщення скопійованих даних, а потім натисніть кнопку **Вставить** на вкладці **Главная** в групі **Буфер обмена**.

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 **Рецензирование** в групі **Изменения** натисніть кнопку **Доступ к книге**.
4. На вкладці **Исправления** переконайтеся, що ви – єдиний користувач у списку **Файл открыт следующим пользователям** (рис.10)

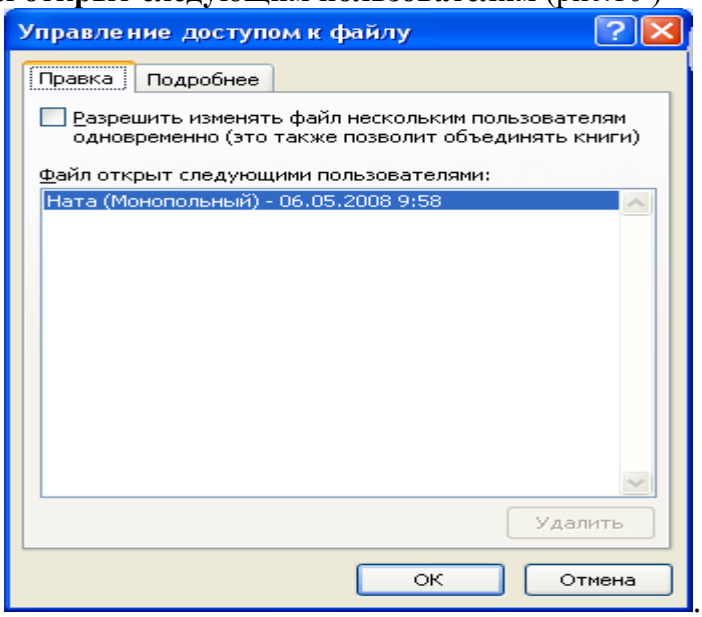


Рис. 10 Вікно Доступ до книги

5. Зніміть прапорець **Разрешить изменять файлы нескольким пользователям одновременно** (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 **Рецензирование** групі **Изменения** виберіть команду **Защита 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 **Рецензирование** у групі **Изменения** виберіть команду **Доступ к книге**.
5. На вкладці **Исправления** зніміть прапорець **Разрешить изменять файлы нескольким пользователям одновременно** (це також дозволить поєднувати книги).
6. Якщо з'явиться повідомлення про вплив на інших користувачів, натисніть кнопку **Да**.

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

1. На вкладці **Рецензирование** у групі **Изменения** виберіть команду **Доступ к книге**.
2. Установіть прапорець **Общий доступ с исправлениями**.
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.

1.3 Основні відомості про безпеку макросів

В Microsoft Office Excel можна вибирати Налагодження 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.

Налагодження безпеки макросів і її дія

Змінити налагодження безпеки макросів можна в центрі управління безпекою (кнопка Microsoft Office  , кнопка - Параметри Excel, рис. 11, категорія - **Центр управления безопасностью**, кнопка – **Параметры центра управления безопасностью,** категорія - **Параметры макросов** рис.12; або вкладка – **Разработчик,** група – **Код**, кнопка – **Безопасность макросов**). 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.

Нижче приводяться загальні відомості про те, як працює захист від вірусів у макросах при різних налагодженнях. При будь-яких налагодженнях, якщо в системі

встановлена антивірусна програма, що працює з Випуск 2007 системи Microsoft Office, і якщо книга містить макроси, перед відкриттям книга перевіряється цією програмою на наявність відомих вірусів.

Змінити Налагодження безпеки макросів можна в центрі керування безпекою (кнопка Microsoft Office  , кнопка Параметри Excel, категорія Центр керування безпекою, кнопка **Параметры центра управления безопасностью** (рис. 13), категорія **Параметры макросов**; або вкладка **Разработчик**, група **Код**, кнопка **Безопасность макросов**). Однак потрібно врахувати, що при роботі в локальній мережі системний адміністратор міг змінити Налагодження за замовчуванням і унеможливити їхню зміну користувачем.

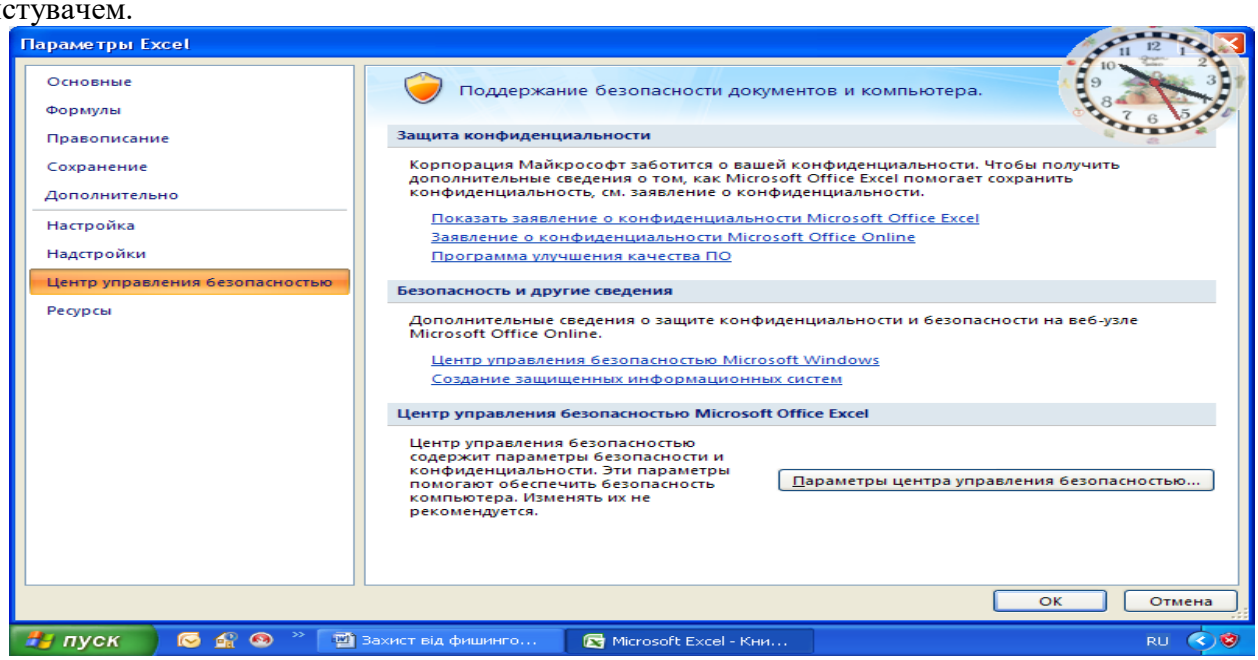


Рис. 11 Вікно параметрів Excel

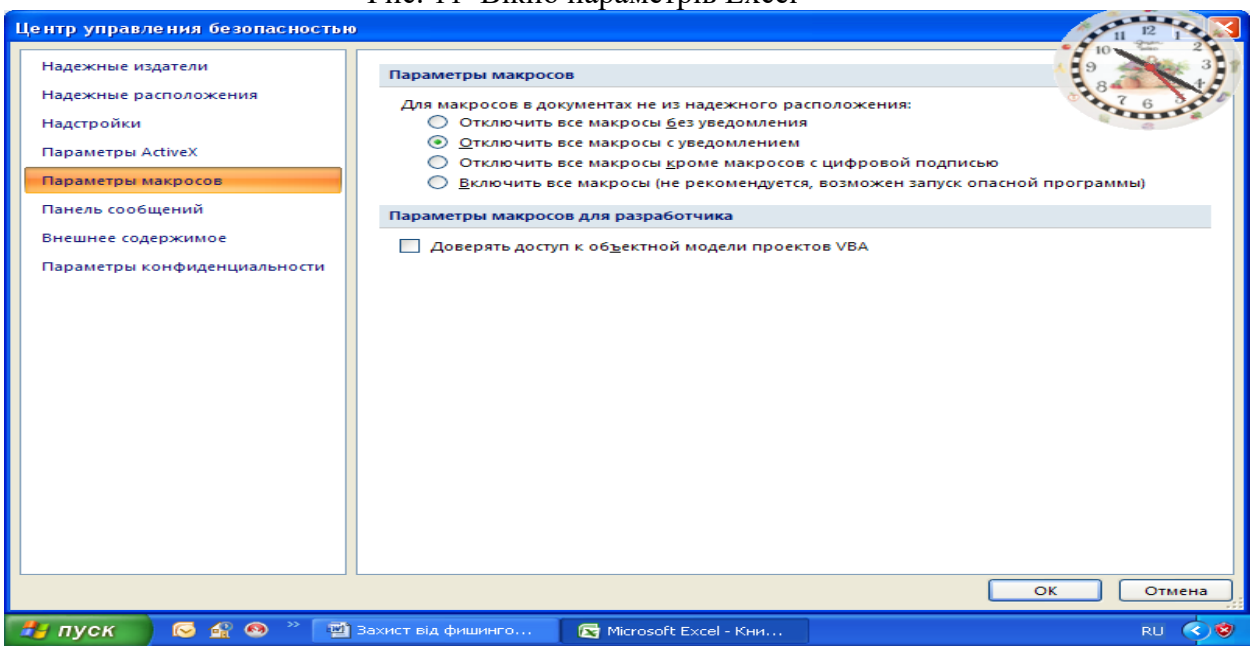


Рис. 12 Вікно Параметри макросів

Таблиця 3

Параметр безпеки макросів

Параметр безпеки макросів	Мета
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 небезпечної програми)	Дане Налагодження тимчасово дозволяє виконання всіх макросів. Цей варіант не рекомендується для постійного користування, оскільки він робить комп'ютер уразливим для потенційно небезпечних програм.
Довіряти доступ до проектної 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.)

Проекту 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.

1.4 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

Виконайте одну з наступних дій:

В Microsoft Windows Vista натисніть кнопку **Пуск**, послідовно виберіть **Все программы, Microsoft Office, Засоби Microsoft Office і Цифровой сертификат для проектов VBA**. У поле **Імя сертификата** введіть описове ім'я для сертифіката.

В Microsoft Windows XP натисніть кнопку **Пуск**, послідовно виберіть **Все программы, Microsoft Office, Засоби Microsoft Office і Цифровой сертификат для проектов VBA**.

У поле **Імя сертификата** введіть описове ім'я для сертифіката.

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

Щоб переглянути сховище особистих сертифікатів, виконайте наступні дії.

Відкрийте оглядач Internet Explorer.

У меню **Сервис** виберіть **Свойства** оглядача, а потім - вкладку **Содержание**.

Натисніть кнопку **Сертификати** й перейдіть на вкладку **Личные**.

Цифровий підпис проекту макросу

Відкрийте файл, що містить проект макросу, який потрібно підписати.

Виконайте наступні дії в додатках Word, Excel або PowerPoint

Випуск 2007 Microsoft Office:

На вкладці **Разработчик** (рис. 13)у групі **Код** натисніть кнопку **Visual Basic** (рис. 14).

У меню **Сервис** (Tools) виберіть пункт **Макрос** і потім клацніть **Редактор Visual Basic.**

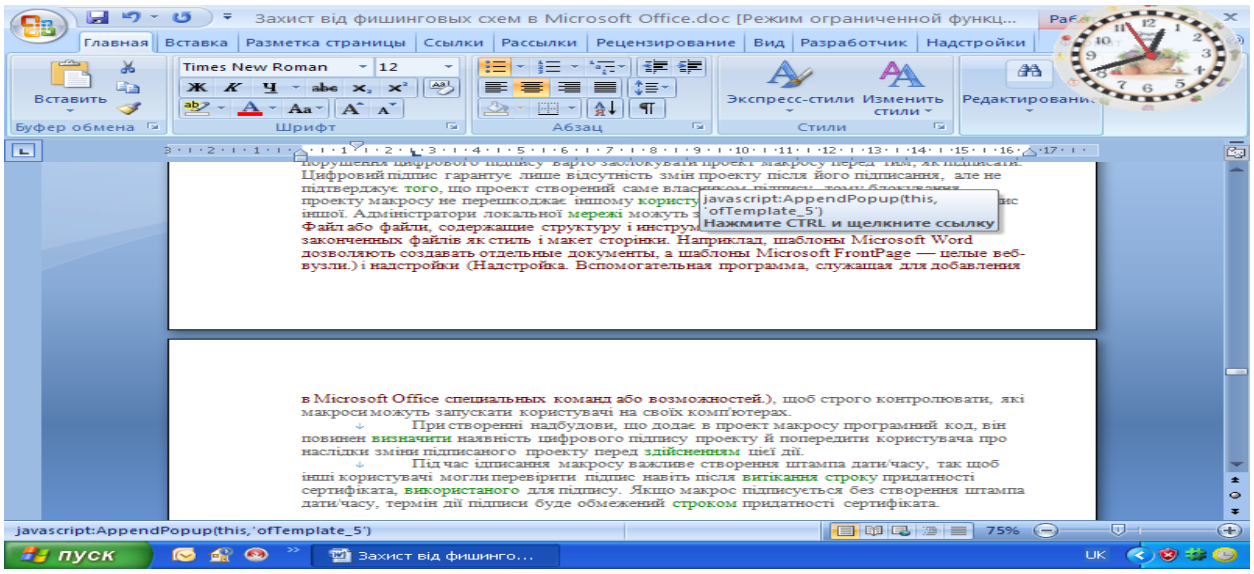


Рис. 13 Вікно Розроблювача

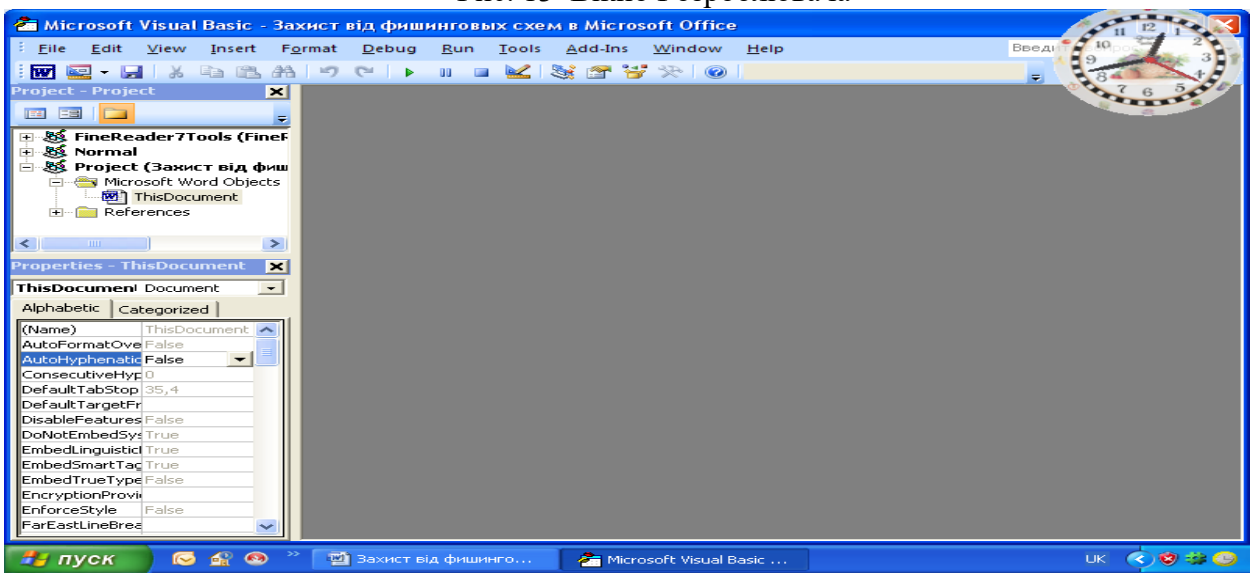


Рис. 14 Вікно Visual Basic

У вікні проекту **Visual Basic** виберіть проект, що потрібно підписати.

У меню **Сервис** виберіть **Цифровая подпись**.

Виконайте одну з наступних дій.

Якщо цифровий сертифікат не був заздалегідь обраний або необхідно скористатися іншим сертифікатом, натисніть кнопку **Выбрать**, 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 дійсного цифрового сертифіката, що використовувався раніше для підпису даного проекту, змінений проект макросу при збереженні буде автоматично підписаний заново.

Для запобігання випадкової зміни користувачами проекту макросу й порушення цифрового підпису варто заблокувати проект макросу перед тим, як підписати.

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.

2. Хід роботи

1. Установити пароль на книгу
2. Установити блокування окремих комірок
3. Розблокувати комірки захищеного листа
4. Установити захист структури й вікон книги
5. Створити книгу загального користування
6. Захистити елементи загальної книги
7. Зняти захист із загальної книги
8. Створити макрос та встановити параметри безпеки
9. Створити цифровий сертифікат

3. Контрольні питання

1. Рівні захисту в Microsoft Excel
2. Установлення пароля на книгу
3. Захист окремих елементів книги й листа
4. Блокування та розблокування обраних областей захищеного листа
5. Захист структури й вікон книги
6. Захист елементів книги
7. Захист елементів загальної книги
8. Основні відомості про безпеку макросів
9. Параметри безпеки макросів
10. Одержання цифрового сертифіката для постановки підпису

Лабораторна робота 11
Захист інформації в Microsoft Access 2007

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в Microsoft Access

Ознайомитись з рівнями захисту баз даних та її елементів порядком створення сертифікату для постановки підпису, зміною параметрів реєстру.

План

1. Теорія
1.1 Можливості системи безпеки в Office Access 2007
1.2 Office Access 2007 і захист на рівні користувача
1.3.Структура системи безпеки Office Access 2007
1.4 Запуск центра керування безпекою
1.5 Створення підписаного пакета
1.6 Включення відключеного вмісту при відкритті бази даних
1.7 Додавання ключа реєстру для відображення модальних діалогових вікон
1.8 Використання пароля для шифрування бази даних Office Access 2007
1.9 Про роботу системи безпеки з базами даних з попередніх версій Access, відкритих в Office Access 2007
1.10 Створення сертифіката із власним підписом
1.11 Зміна параметра реєстру
2. Хід роботи
3. Контрольні питання

Теорія

1.1 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 Налагодження 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 з'являється єдиний засіб, називаний «Панель повідомлень» (рис. 1).

Рис. 1 Вікно повідомлень

- 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.

1.2 Ofice 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.

1.3 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 проектів – 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. 2). 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 відключені 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.

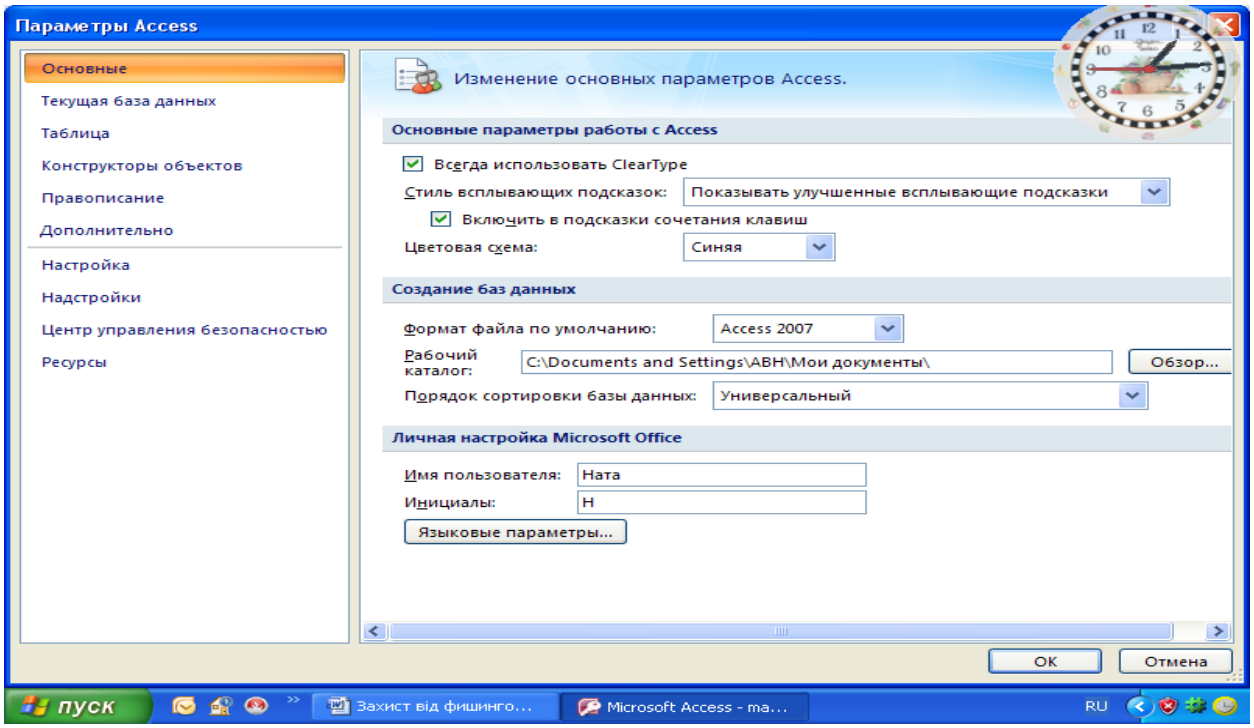


Рис. 2 Вікно відбору параметрів відкрита бази даних

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.

1.4 Запуск центра керування безпекою

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

Примітка. Відкривати базу даних не потрібно.

Відкриється діалогове вікно Параметри Access.

2. Виберіть пункт **Центр управления безопасностью,** і у групі **Центр управления безопасностью Microsoft Office Access** натисніть кнопку **Параметры центра управления безопасностью** (рис. 3).

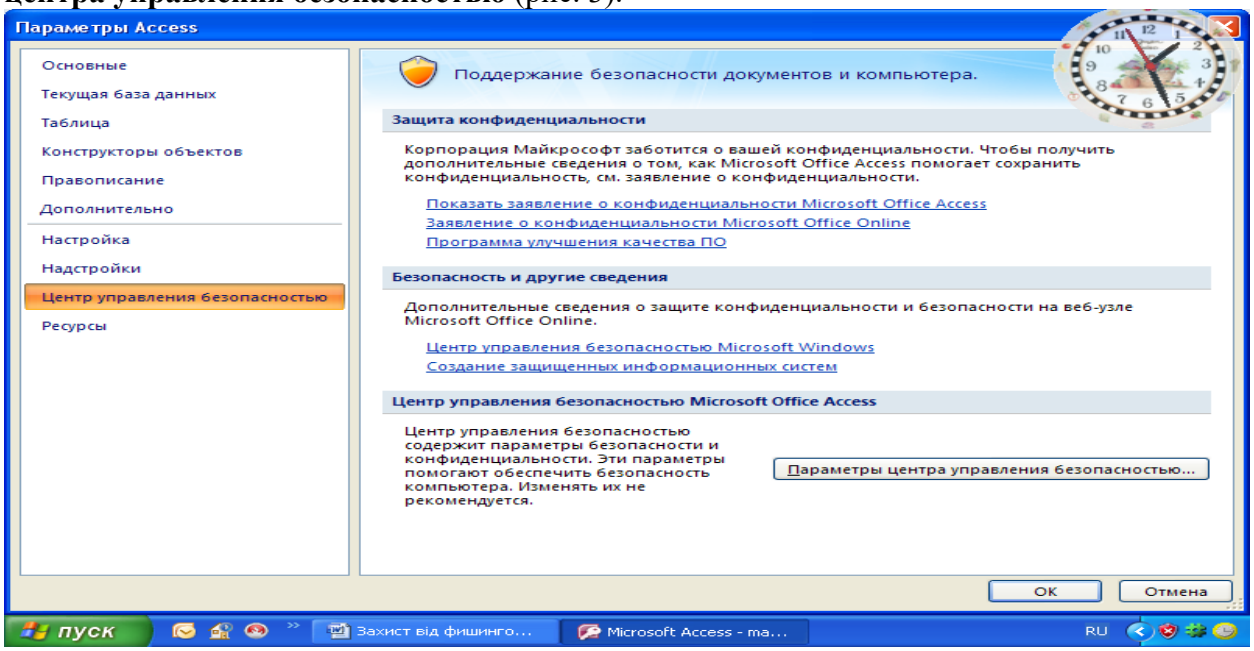


Рис. 3 Вікно управління безпекою

3. Виберіть **Надежные расположения** (рис. 4), а потім виконайте одну з наступних дій.

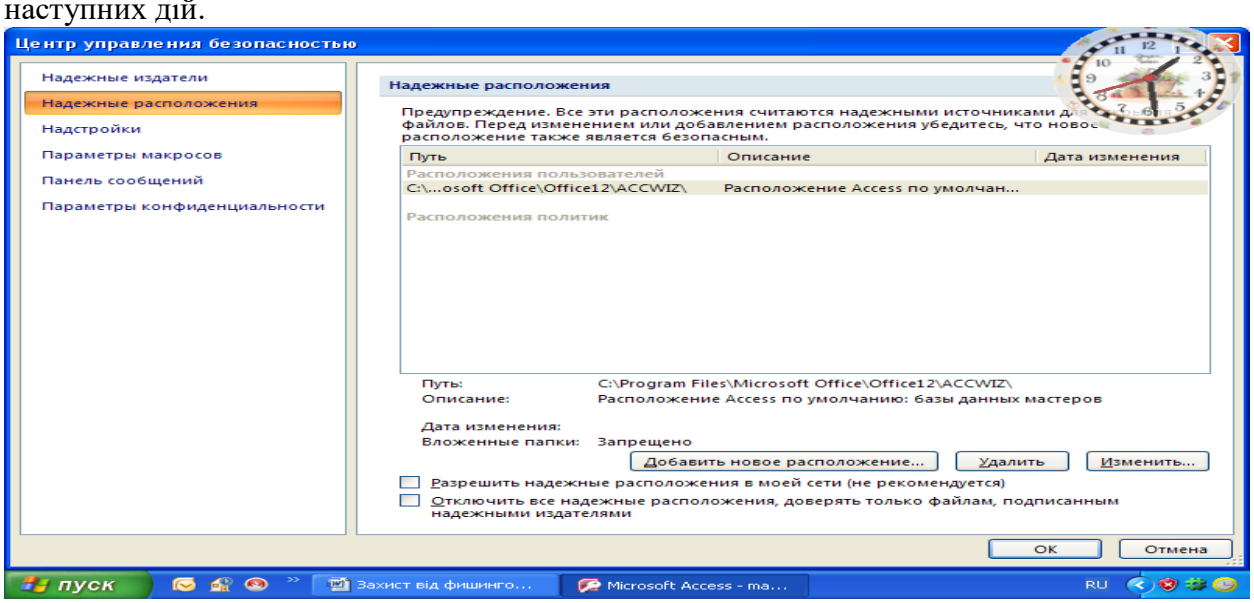


Рис. 4 Вікно вибору надійного розташування

- Укажіть шлях до одного або декількох надійних розташувань.
- Створіть нове надійне розташування. Для цього натисніть кнопку **Добавить** нове розташування, а потім укажіть значення параметрів у діалоговому вікні **надежное расположение Microsoft Office** (рис. 5).

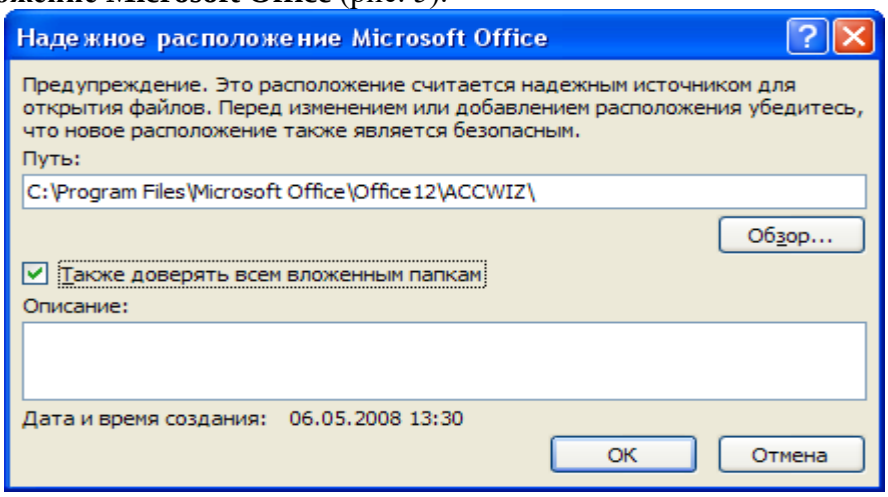


Рис. 5 Вікно вибору надійного розташування баз

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.

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.

1.5 Створення підписаного пакета

1. Відкрийте базу даних, для якої потрібно створити пакет і підписати його.
2. Натисніть кнопку Microsoft Office  , виберіть команду **Опубликовать**, а потім команду **Архивировать и подписать** (рис. 6).

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 **Сохранить у** виберіть розташування для підписаного пакета бази даних.
5. У поле **Імя файла** введіть ім'я для підписаного пакета, а потім натисніть кнопку **Создать**.

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 **Открыть**.

Відкриється діалогове вікно Відкрити.

2. У списку **Тип файлов** виберіть варіант **Подписанные пакеты Microsoft Office Access** (*.accdc).
3. Скористайтеся списком **Папка**, щоб знайти папку, що містить ACCDC-Файл, виділіть цей файл і натисніть кнопку **Открыть**.

4. Виконайте одну з наступних дій:

- Якщо обрано параметр довіри до цифрового сертифіката, застосованому до розгорнутого пакета, з'явиться діалогове вікно **Вытянуть базу данных в...** Перейдіть до наступного етапу.
- Якщо параметр довіри до цифрового сертифіката ще не обраний, з'явиться попередження (рис. 7).

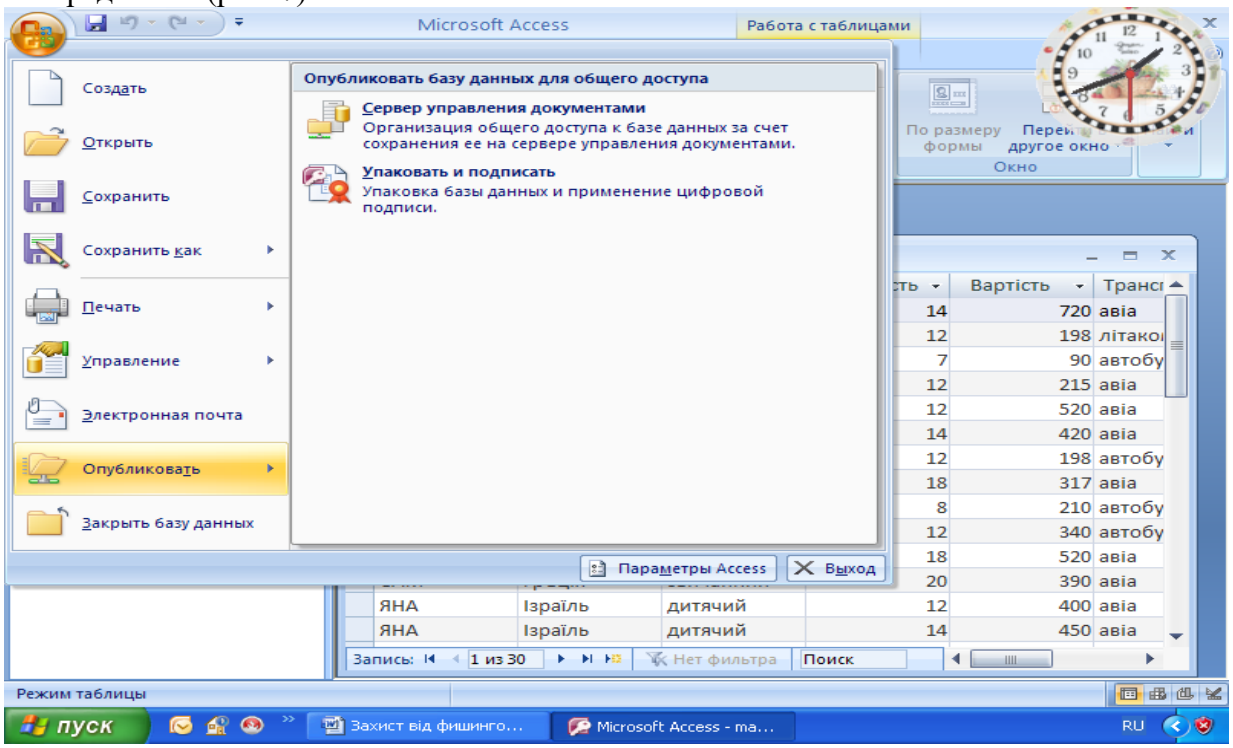


Рис. 6 Вікно Публікації

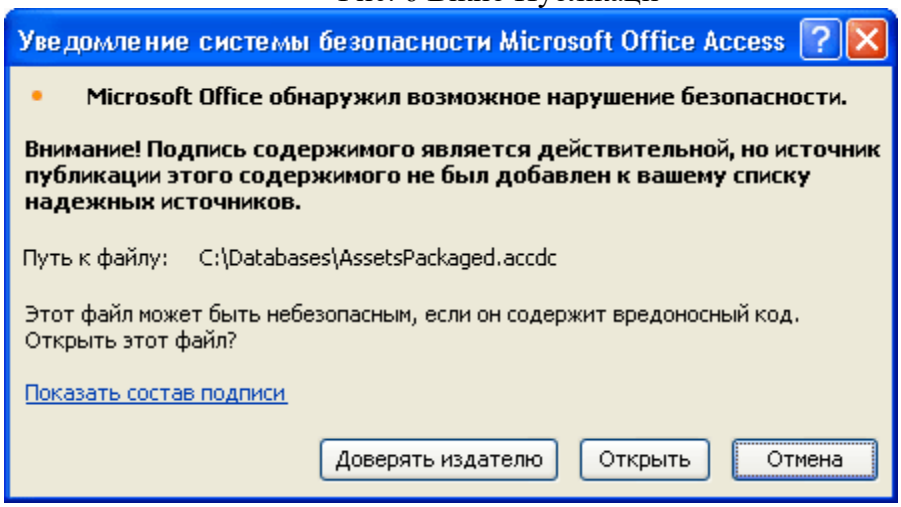


Рис. 7 Вікно попередження

Якщо ви довіряєте базі даних, натисніть кнопку **Открыть**. Якщо ви довіряєте всі сертифікатам цього постачальника, натисніть кнопку **Доверять всему от издателя**. Відкриється діалогове вікно Витягти базу даних в.

5. У списку **Сохранить** в можна вибрати розташування для бази даних, а в поле **Імя файла** - увести для неї інше ім'я.

6. Натисніть кнопку **ОК**.

1.6 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. 8).

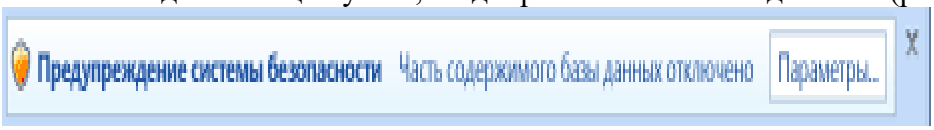


Рис. 8 Вікно панелі повідомлень

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 дані стану довіри

1. На панелі повідомлень натисніть кнопку **Параметры**.

Відкриється діалогове вікно Параметри безпеки Microsoft Office.

2. Виберіть варіант **Включить это содержание**, а потім натисніть кнопку **ОК**.

Якщо панель повідомлень не відображається

- На вкладці **Работа с базами данных** у групі **Отображение** виберіть параметр **Панель оповещений**.

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 **Закрить базу данных**.

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 **Параметры**.

Відкриється діалогове вікно Параметри безпеки Microsoft Office.

2. Виберіть варіант **Установить защиту от незнакомого содержания** (рекомендується) і натисніть кнопку **ОК**.

Access відключить усі потенційно небезпечні компоненти.

Приховання панелі повідомлень

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

Відображення панелі повідомлень

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

1.7 Додавання ключа реєстру для відображення модальних діалогових вікон

Примітка. 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 **Выполнить**.
2. У поле **Открыть** введіть **regedit**, а потім натисніть клавішу **Ввести**.

Запуститься редактор реєстру.

3. Розгорніть папку HKEY_CURRENT_USER (рис. 9)і вкажіть наступний розділ реєстру:

Software\Microsoft\Office\12.0\Access\Security

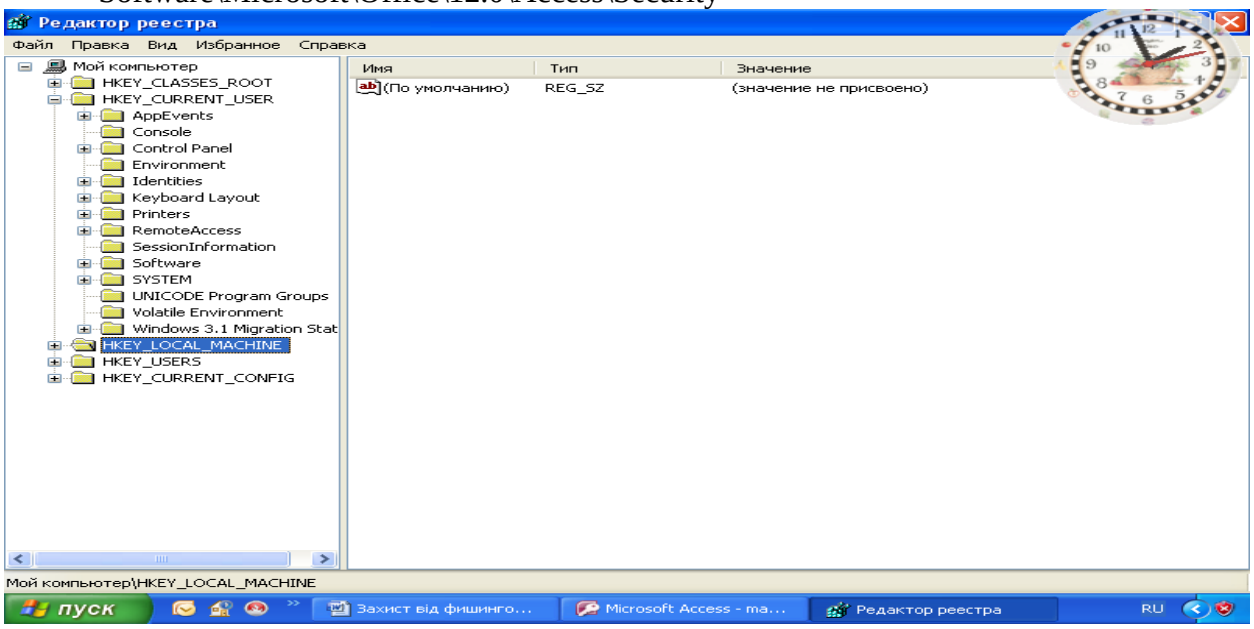


Рис. 9 Вікно реєстру

4. У правій області редактора реєстру клацніть правою кнопкою миші порожнє місце, виберіть команду **Создать**, 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 **Значение** 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.

1.8 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 **Открыть**.
2. У діалоговому вікні відкрити знайдіть файл, якому потрібно відкрити, і виділіть його.
3. Виберіть команду **Монопольно** (рис. 10).
4. На вкладці **Работа з базамы** даних клацніть **Зашифровать с помощью пароля.**

Відкриється діалогове вікно **Создание пароля базы данных** (рис. 11).

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

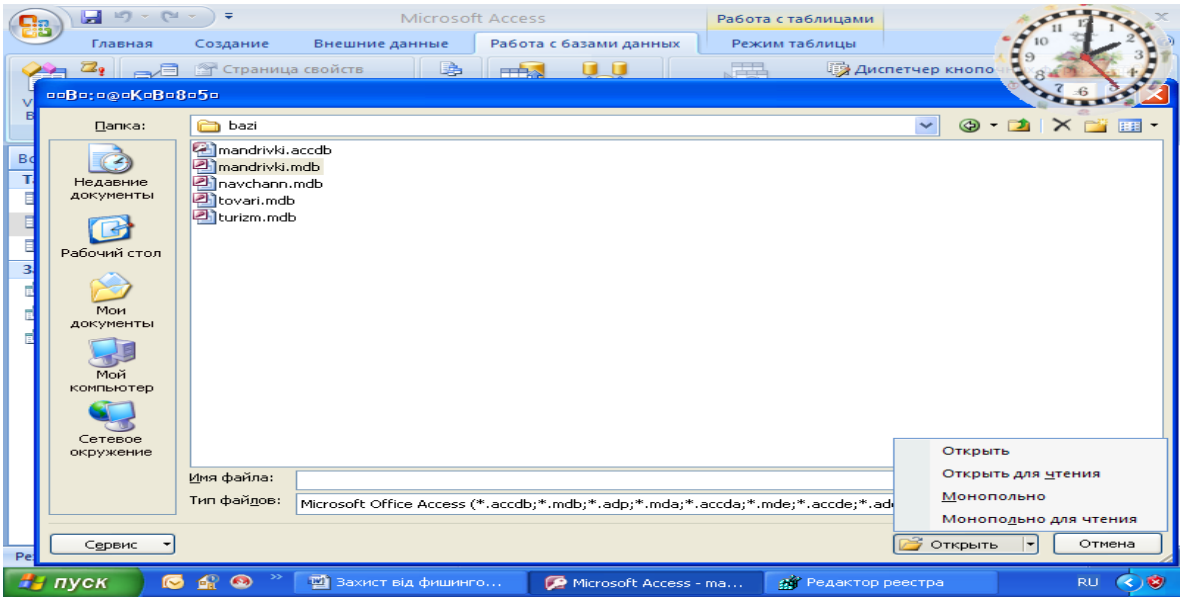


Рис. 10 Відкриття бази даних у монопольному режимі

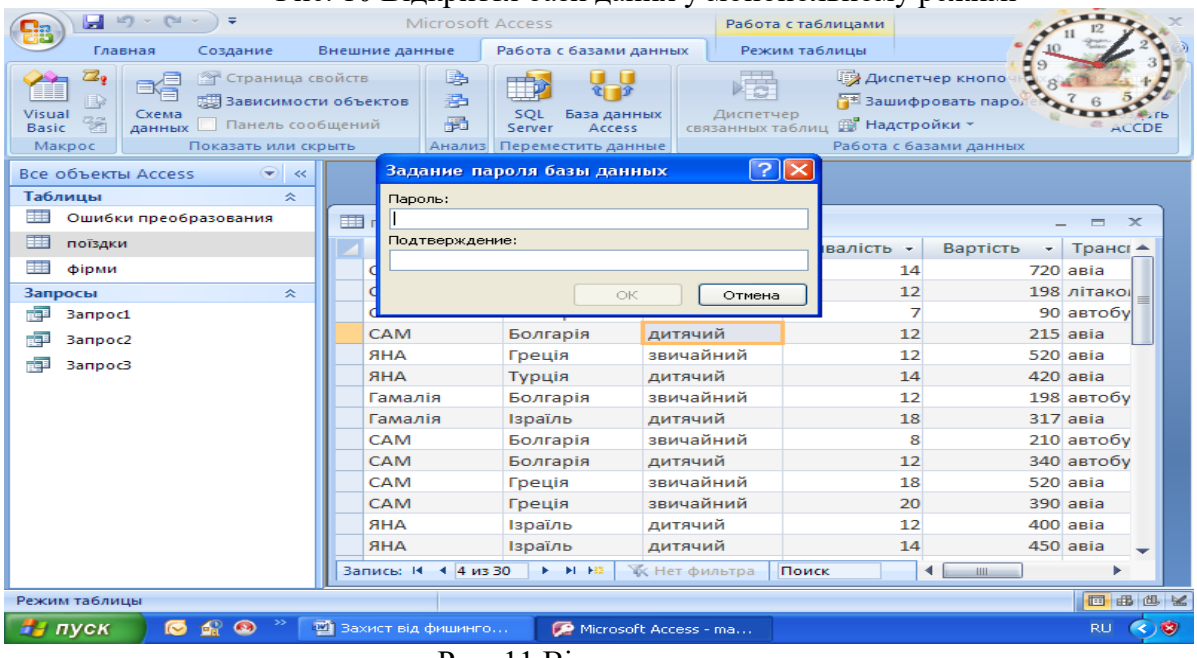


Рис. 11 Вікно введення пароля

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 **Необходимо ввести пароль**.

2. Уведіть пароль у поле **Введите пароль базы данных** і натисніть кнопку **ОК**.

Видалення пароля

1. На вкладці **Работа з базамы данных** клацніть **Дешифрировать базу данных**.

Відкриється діалогове вікно **Удалить пароль базы данных**.

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

1.9 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 інший 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.

1.10 Створення сертифіката із власним підписом

1. Натисніть кнопку **Пуск**, виділіть пункт **Все программы**, потім - пункти **Microsoft Office** і **Засоби Microsoft Office,** і виберіть команду **Цифровое свидетельство для проектов 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. 12)

2. У поле **Імя вашего сертификата** введіть ім'я для нового сертифіката.
3. Два рази натисніть кнопку **ОК** (рис. 13).

.

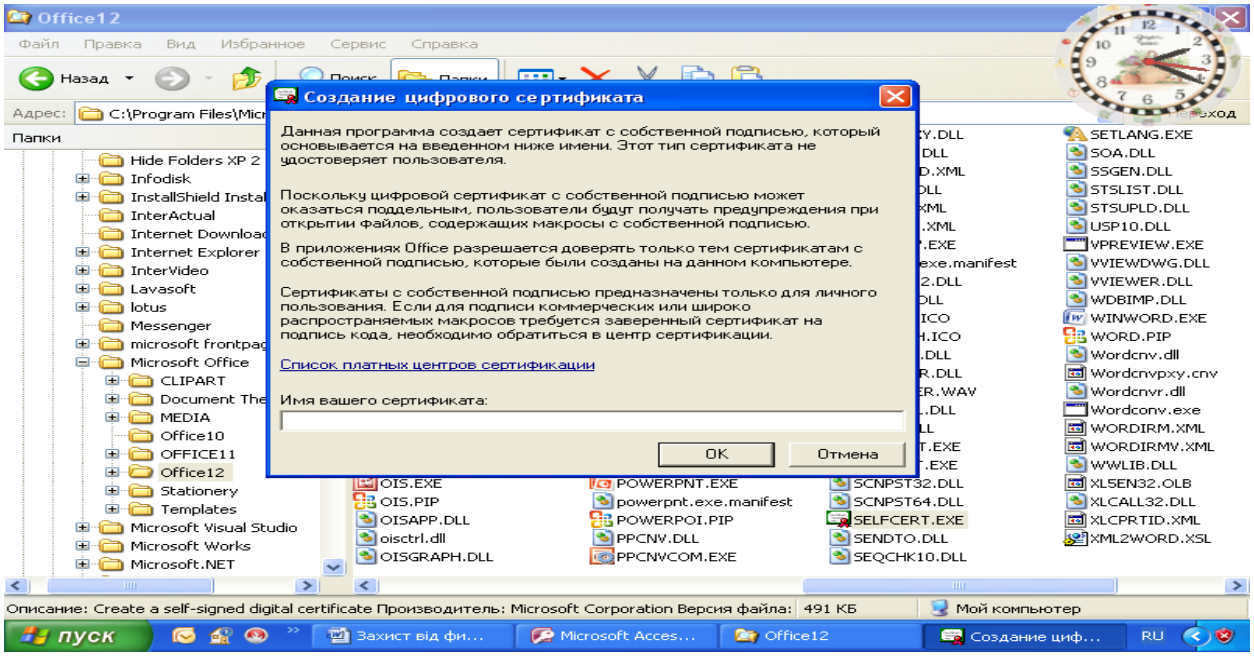
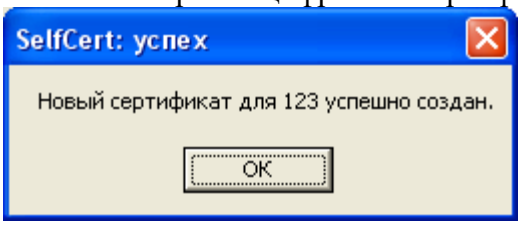


Рис. 12 Вікно створення цифрового сертифіката



.

Рис. 13 Вікно повідомлення

Підпис кодом бази даних

1. Відкрийте базу даних, до якої потрібно додати підпис.
2. На вкладці **Средства базы данных** у групі **Макрос** виберіть команду **Visual Basic**, щоб запустити редактор Visual Basic (рис. 14)

Натисніть клавіші **ALT+F11**.

3. У вікні проекту виберіть базу даних, макрос або модуль, до яких потрібно додати підпис.
4. У меню **Сервис** виберіть команду **Цифровые подписи**.

Відкриється діалогове вікно Цифрові підписи (рис. 15).

5. Натисніть кнопку **Выбор**, щоб вибрати сертифікат.

Відкриється діалогове вікно **Выбор сертификата** (рис. 17)

6. Виберіть необхідний сертифікат.

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

7. Щоб закрити діалогове вікно **Сертификат**, 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.

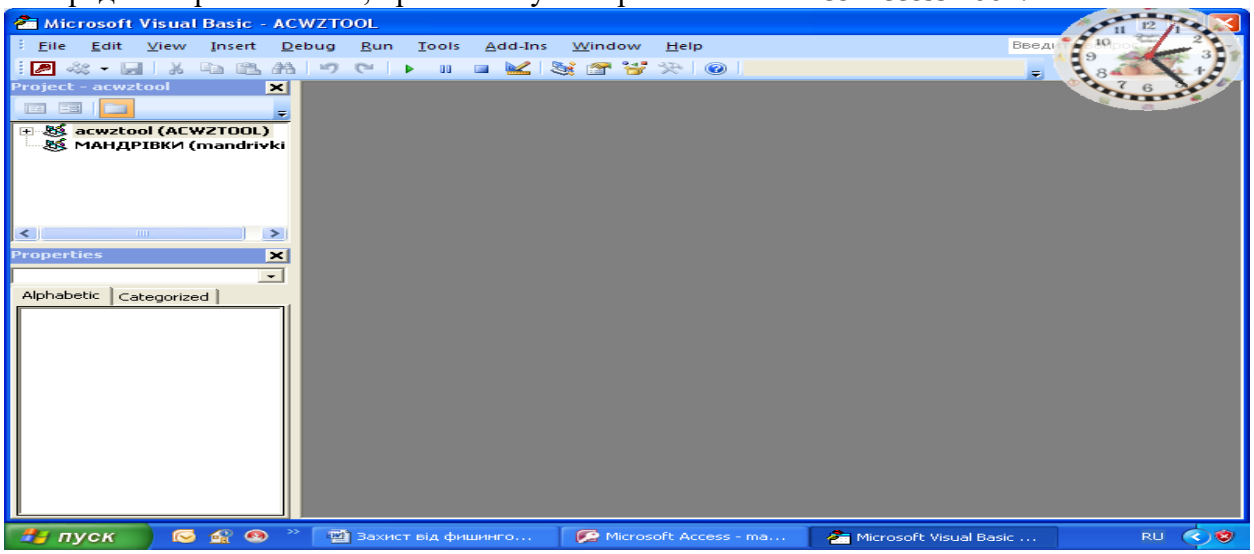


Рис. 14 Вікно редактора Visual Basic

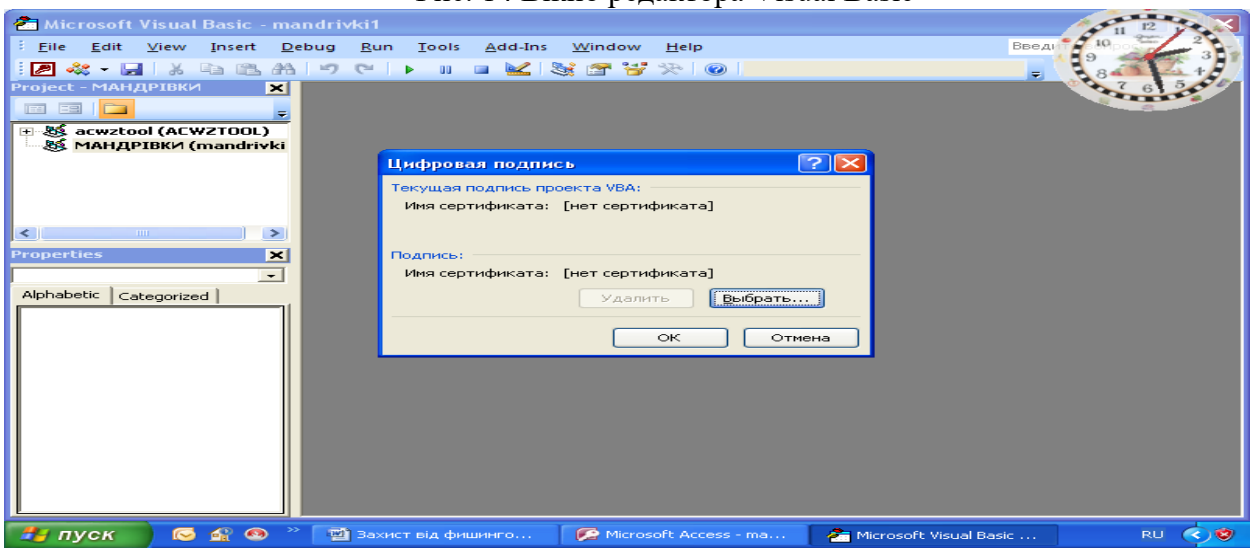


Рис. 15 Цифрові підписи

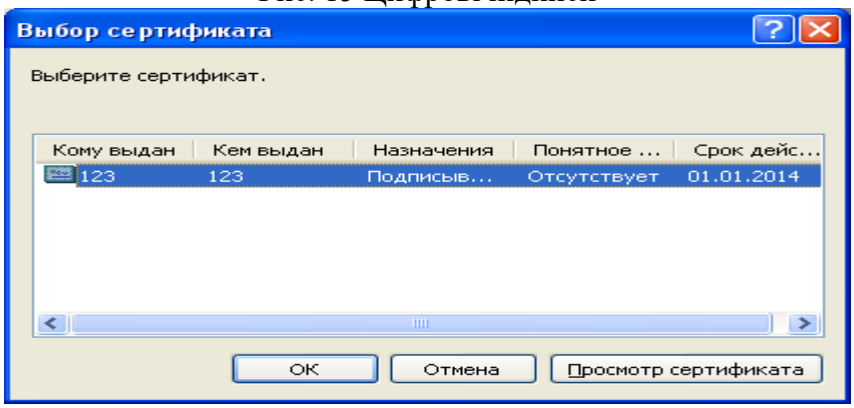


Рис. 16 Вибір сертифіката

Установка засобу SelfCert.exe

1. **Запустите установочный диск** Office Professional 2007 або інший засіб установки.

2. У вікні установки клацніть **Добавить или удалить компоненты**, 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 управления**.

2. Двічі клацніть компонент **Установка и удаление программ** і натисніть кнопку **Изменить**. **Выделите Випуск 2007 системи Microsoft Office**

Почнеться процес установки.

3. Установіть перемикач у положення **Добавить или удалить компоненты** й натисніть кнопку **Далее**.

4. Виконайте наступні дії.

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

4. Клацніть **Цифровое свидетельство для проектов VBA**.

5. Клацніть **Запускать з моего компьютера.**

6. Натисніть кнопку **Далее**, щоб установити компонент.

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

1.11 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 **Выполнить**.

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

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.

2. Хід роботи

1. Укажіть шлях до одного або декількох надійних розташувань бази даних
2. Розмістіть бази даних у надійному розташуванні
3. Проведіть упакування, підпис і поширення бази даних Office Access 2007
4. Створіть підписаний пакет
5. Проведіть Витяг і використання підписаного пакета
6. Надайте базі дані стан довіри
7. Використайте пароль для шифрування бази даних
8. Проведіть Розшифрування й відкриття бази даних
9. Створіть сертифікат із власним підписом

3. Контрольні питання

1. Можливості системи безпеки в Office Access 2007
2. Використання вікна повідомлень поза довіреним розташуванням
3. Office Access 2007 і захист на рівні користувача
4. Структура системи безпеки Office Access 2007
5. Режим відключення виконуваного вмісту.
6. Використання бази даних Office Access 2007 у надійному розташуванні
7. Запуск центра керування безпекою
8. Розміщення бази даних у надійному розташуванні
9. Упакування, підпис і поширення бази даних Office Access 2007
10. Створення підписаного пакета
11. Витяг і використання підписаного пакета
12. Надання базі дані стану довіри
13. Додавання ключа реєстру для відображення модальних діалогових вікон
14. Використання пароля для шифрування бази даних Office Access 2007
15. Розшифрування й відкриття бази даних
16. Створення сертифіката із власним підписом
17. Підпис кодом бази даних
18. Зміна параметра реєстру

Лабораторна робота 12
Захист інформації в Microsoft Office2010

Мета роботи – Засвоїти принципи й елементи технології захисту інформації в Microsoft Office2010

Ознайомитись з рівнями захисту документів, які створені за допомогою додатків Microsoft Office2010, обмеженням змін в документах, дозволів для користувачів, використання шифрування та цифрових підписів, захист від фішингу, попереджень системи безпеки.

ПЛАН

1. Теорія
1.1 Захист документа паролем та шифруванням
1.2 Захист остаточної версії файлу від змін
1.3 Обмеження на внесення змін у файли Word і Excel
1.4 Обмеження змін в Word 2010
1.5 Обмеження змін в Excel 2010
1.6 Обмеження на форматування
1.7 Обмеження дозволів для користувачів
1.8 Додавання цифрового підпису користувача
1.9 Створення рядка підпису в документі Word або Excel
1.10 Видалення цифрових підписів з документа Word або Excel
1.11 Додавання невидимих цифрових підписів у документ Word, Excel або PowerPoint
1.12 Видалення невидимих цифрових підписів з документа Word, Excel або PowerPoint
1.13 Недійсні цифрові підписи
1.14 Посилання на підозрілий web – сайт
1.15 Включення й відключення попереджень системи безпеки на панелі повідомлень
1.16 Захист від фішингу і інших підозрілих схем в Internet
2. Хід роботи
3. Контрольні питання

1. Теорія

На багатьох підприємствах для захисту уразливої інформації, наприклад, медичних і фінансових документів співробітників, платіжних відомостей і персональних даних використовується тільки обмеження доступу до мереж або комп'ютерів, де усе це зберігається. Технологія управління правами на доступ до даних (IRM), яка застосовується в Microsoft Office 2010, допомагає організаціям і співробітникам інформаційних центрів забезпечити електронний контроль уразливої інформації методом вибору дозволів на доступ, використання документів і повідомлень.

Office 2010 надає наступні групи прав, які користувачі можуть вибирати при створенні, захищеного службою управління правами на доступ до даних.

1. Захист документа паролем та шифруванням.
2. Захист остаточної версії файлу від змін.
3. Обмеження на внесення змін у файли Word і Excel.
4. Обмеження на форматування.
5. Обмеження дозволів для користувачів.
6. Додавання цифрового підпису користувача.
7. Посилання на підозрілий web — сайт.

1.1 Захист документа паролем та шифруванням

Щоб запобігти несанкціонованому доступу до документа, його можна захистити паролем в Microsoft Word, Excel, Acces, InfoPath, PowerPoint.

Використовуйте надійні паролі, що представляють собою комбінація 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 мати не менш ніж 8 знаків. Рекомендується використовувати фразу — пароль, що складається з 14 або більш знаків.

1. Відкрийте вкладку **Файл**.
2. Введіть команду **Сведения**.
3. Клацніть **Защита документа**, (рис. 1) а потім – **Зашифровать паролем**.
4. У поле **Шифрование документа** введіть пароль (рис. 2) і натисніть кнопку **ОК**.
5. Ще раз уведіть пароль у **поле Подтверждение пароля** й натисніть кнопку **ОК**.
6. Примітки.
    - щоб зашифрувати документ і захист могли зняти тільки авторизовані користувачі треба встановити прапорець **Проверка подлинности пользователя**; шифрування документа не допускає сумісного редагування;
    - паролі необхідно вводити з урахуванням регістру;
    - у випадку втрати пароля додатку Office 2010 не вдасться відновити дані.
7. В Microsoft Excel крім захисту паролем книги, який проводиться аналогічно, існує можливість захисту аркуша та його структури. Команда вводиться з підменю **Защитить книгу** (рис. 3 –5).

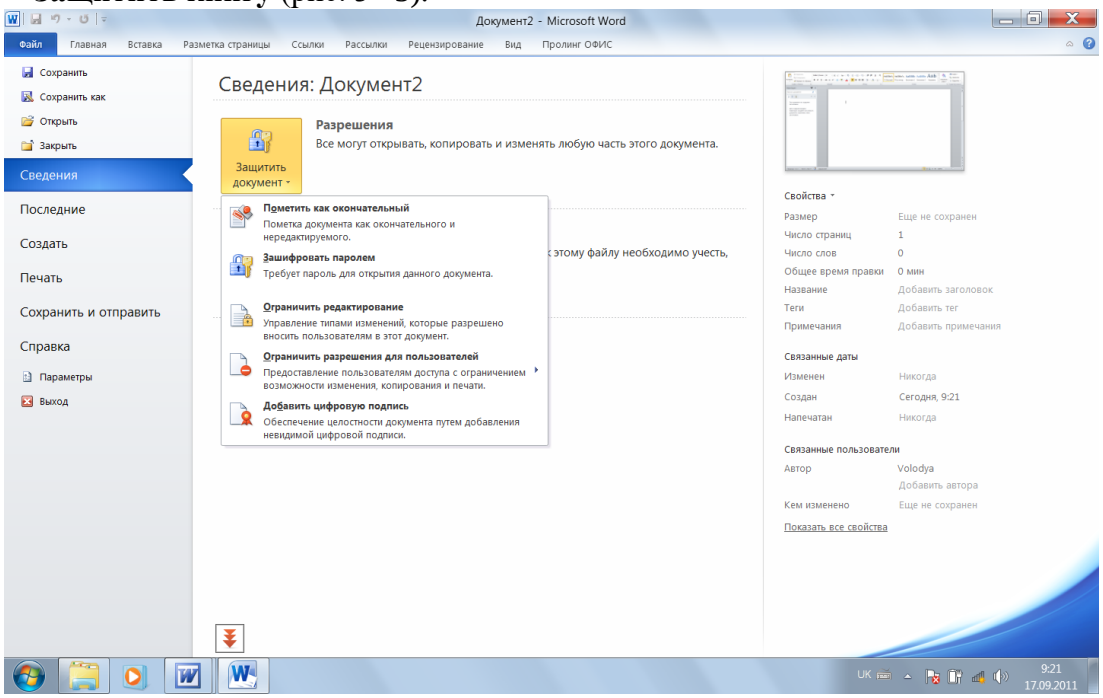


Рис. 1 Вікно вибору типу захисту документа

1.2 Захист остаточної версії файлу від змін

Перш ніж дозволити доступ до електронної копії документа Microsoft Office іншим користувачам, можна скористатися командою **Пометить как окончательный** (рис. 1,6), щоб зробити цей файл доступним тільки для читання й запобігти його зміні. Якщо файл позначений як остаточний, у ньому недоступні або відключені команди

введення й редагування й перевірка правопису, а сам файл доступний тільки для читання. Крім того, властивість документа **Состояние** має значення **Окончательный**.

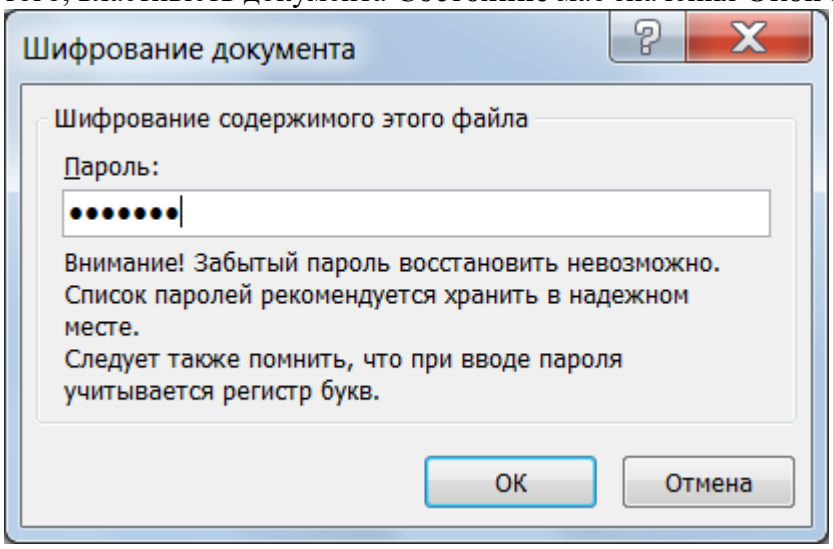


Рис. 2 Вікно введення пароля

Примітки:

- команда **Пометить как окончательный** не є засобом забезпечення безпеки. Будь — який користувач, що одержав електронну копію файлу, позначеного як остаточний, може відредагувати цей файл, скасувавши команду **Пометить как окончательный**;
- якщо файл, позначений у додатку Microsoft Office 2010 як остаточний, відкритий в більш ранній версії Microsoft Office, він буде доступний не тільки для читання, але й для інших операцій.

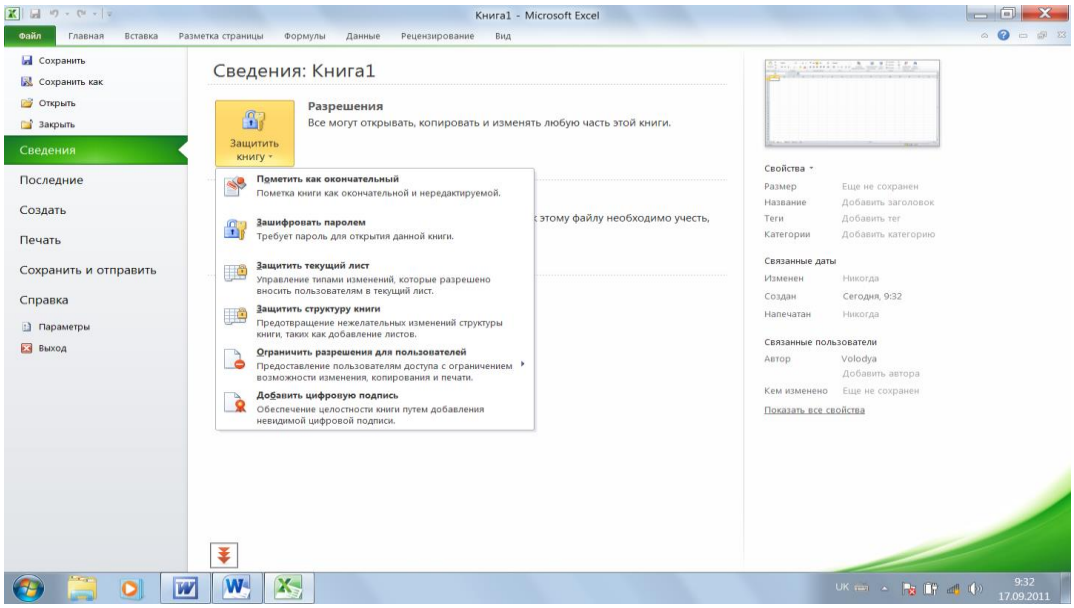
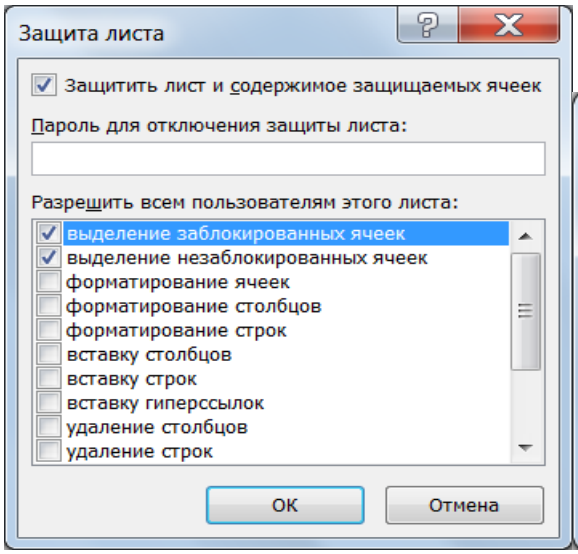


Рис. 3. Вікно відбору команд захисту в Microsoft Excel

Захист позначення документу як остаточний можна легко зняти відкривши відповідний файл та ввівши команду **Пометить как окончательный.**



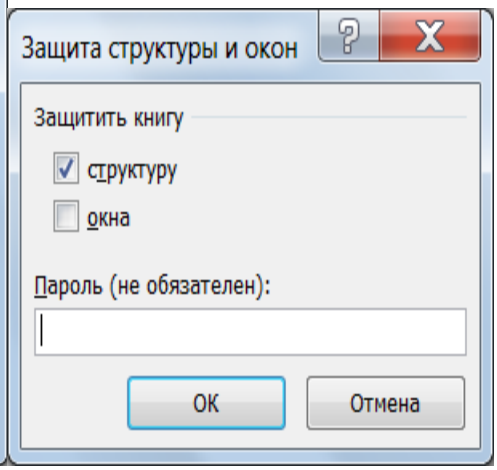


Рис. 4 Захист паролем аркуша Рис. 5 Захист паролем структури аркуша

Після скасування команди **Пометить как окончательный** стає можливим редагування файлу. Спливаюча підказка повідомляє, що будь – який користувач може відкривати, копіювати й змінювати будь –яку частину файлу.

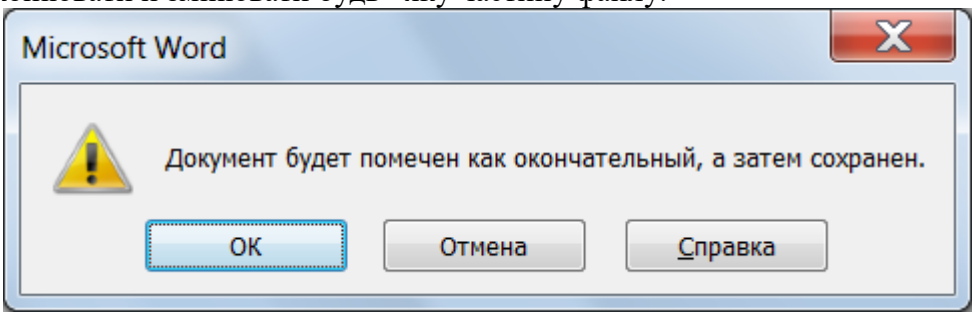


Рис. 6 Позначення документу як остаточний

1.3 Обмеження на внесення змін у файли Word і Excel

Щоб запобігти внесенню редакторами вмісту випадкових змін у документ Microsoft Word 2010 або таблицю Excel 2010, можна обмежити можливості форматування й зміни файлу.

1.4 Обмеження змін в Word 2010

На стрічці **Рецензирование** в групі **Защита** виберіть команду **Ограничить редактирование** (рис. 7). Відберіть необхідні параметри захисту

1.5 Обмеження змін в Excel 2010

На вкладці **Рецензирование** в групі **Изменения** налагодіть зазначені нижче параметри захисту. **Защита книги** (рис. 8), **Разрешить изменение диапазонов** (рис. 9) з введенням команди **Создать** (рис. 10), **Доступ к книге** (рис. 11).

1.6 Обмеження на форматування

За умовчанням всі стилі форматування доступні користувачам. Для обмеження вказаних параметрів необхідно:

1. На стрічці **Главная** в групі **Стили** введіть команду **Изменить Стили** (рис. 12). В правій панелі відберіть параметри обмежень.

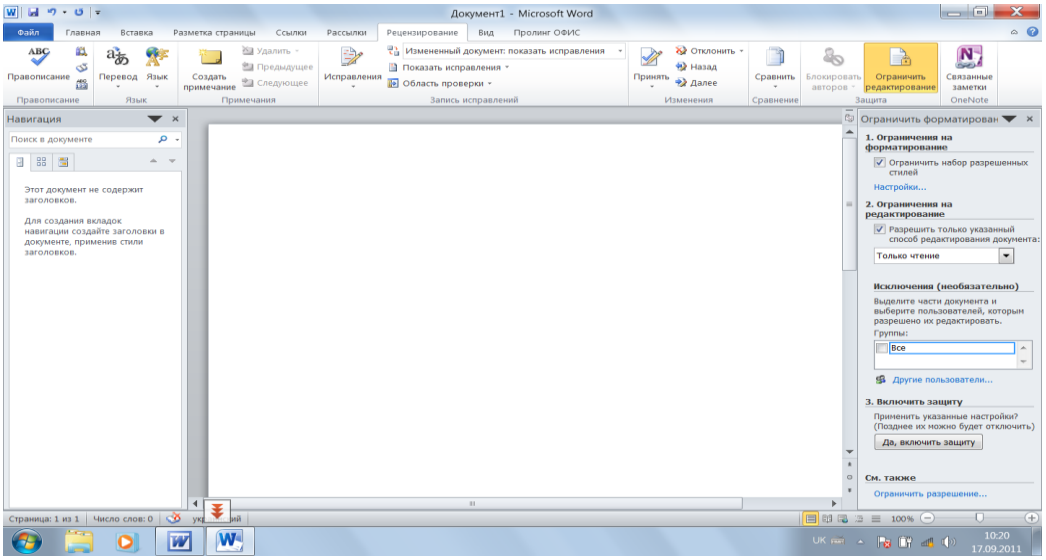


Рис. 7 Вікно відбору параметрів обмеження редагування документу

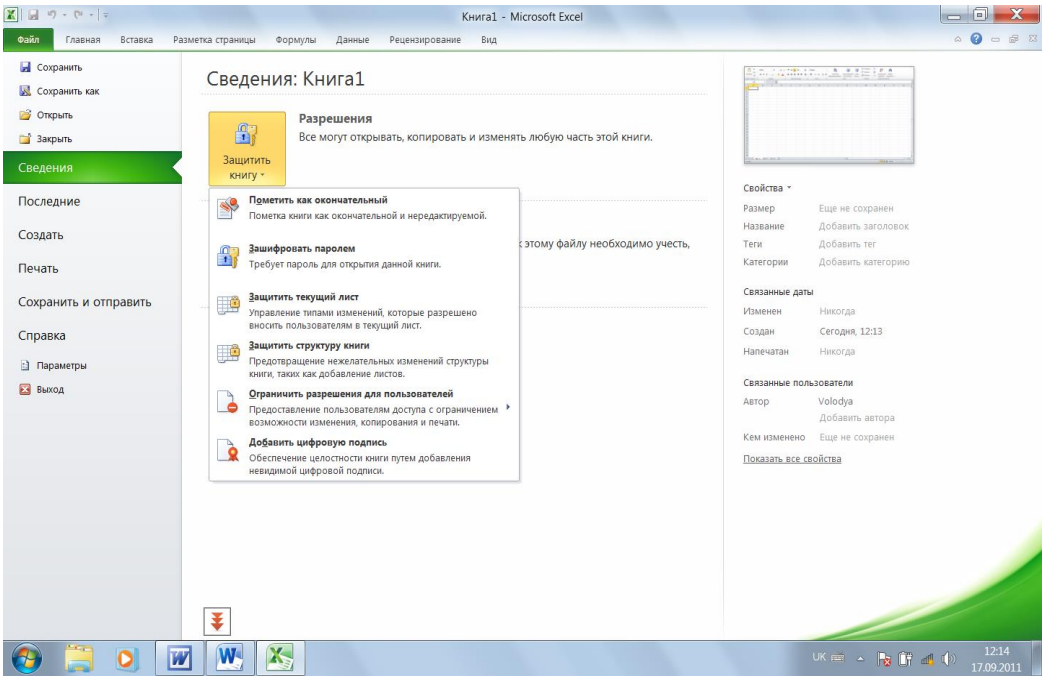


Рис. 8 Вікно захисту книги

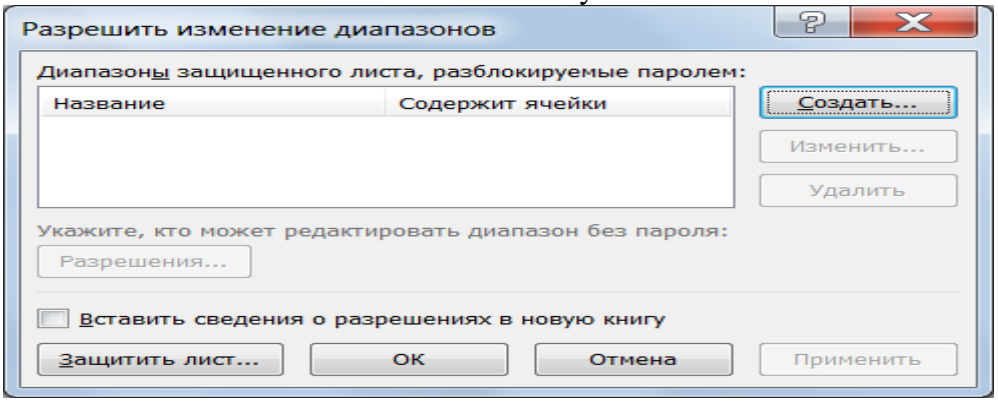


Рис. 9 Вікно створення захисту діапазонів комірок

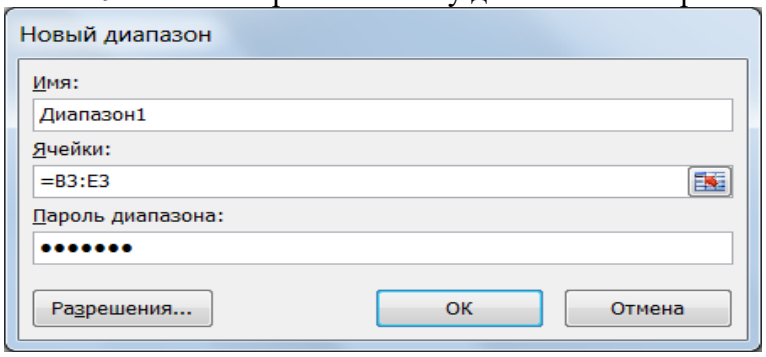


Рис. 10 Вікно відбору діапазонів комірок та введення паролю

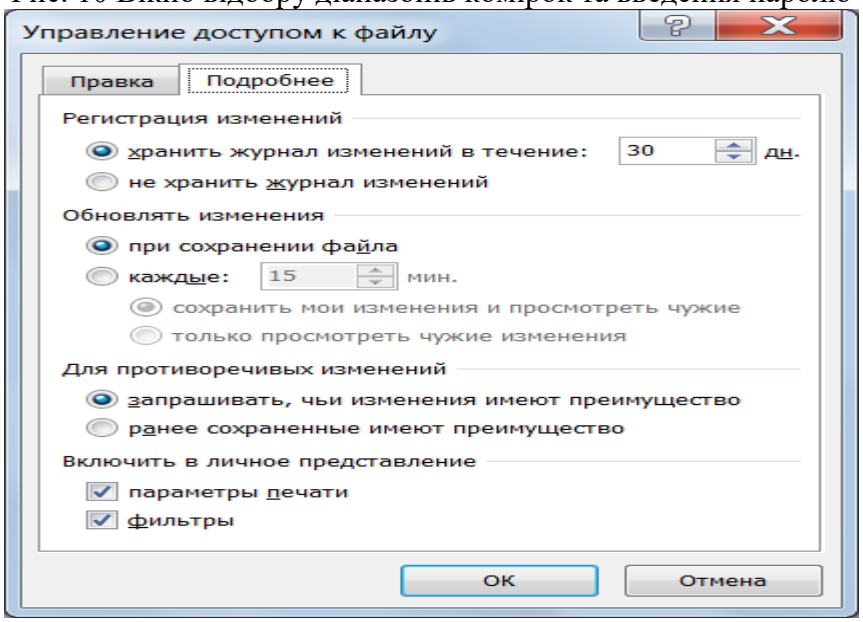


Рис. 11 Відбір параметрів доступу до книги

1.7 Обмеження дозволів для користувачів

Можна встановити (рис. 13) необмежений доступ користувачів до відкритого документа, обмежений доступ та управління обліковими даними – для чого треба зробити підписку на відповідну службу фірми Microsoft (рис.14), обмежити доступ до записної книжки в Microsoft OneNote (рис. 15).

1.8 Додавання цифрового підпису користувача

Рядок підпису нагадує звичайне місце для підпису в друкованому документі, але працює інакше. Додаючи рядок підпису у файл Office, автор може вказати відомості про особу, що підписує, і надати інструкції. Коли електронна копія файлу відправляється користувачеві, який підписує, він бачить рядок підпису й повідомлення про те, що необхідний його підпис. Він може:

- увести підпис;
- вибрати зображення цифрового підпису;
- увести підпис за допомогою функції рукописного введення на планшетному ПК.

Одночасно з видимим підписом у документ додається й цифровий підпис для підтвердження особистості, яка підписала.

Примітка. Документ, підписаний цифровий підписом, стає доступний тільки для читання

На наведеному нижче малюнку (рис. 16). показана панель повідомлень із повідомленням про те, що підписаний документ доступний тільки для читання.

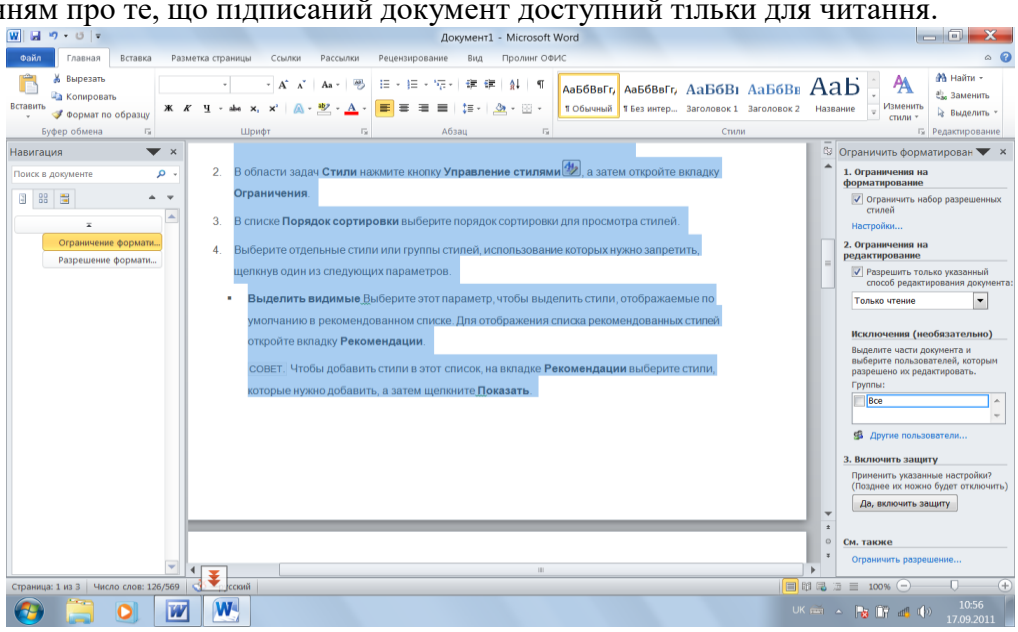


Рис. 12 Вікно зміни параметрів стилів

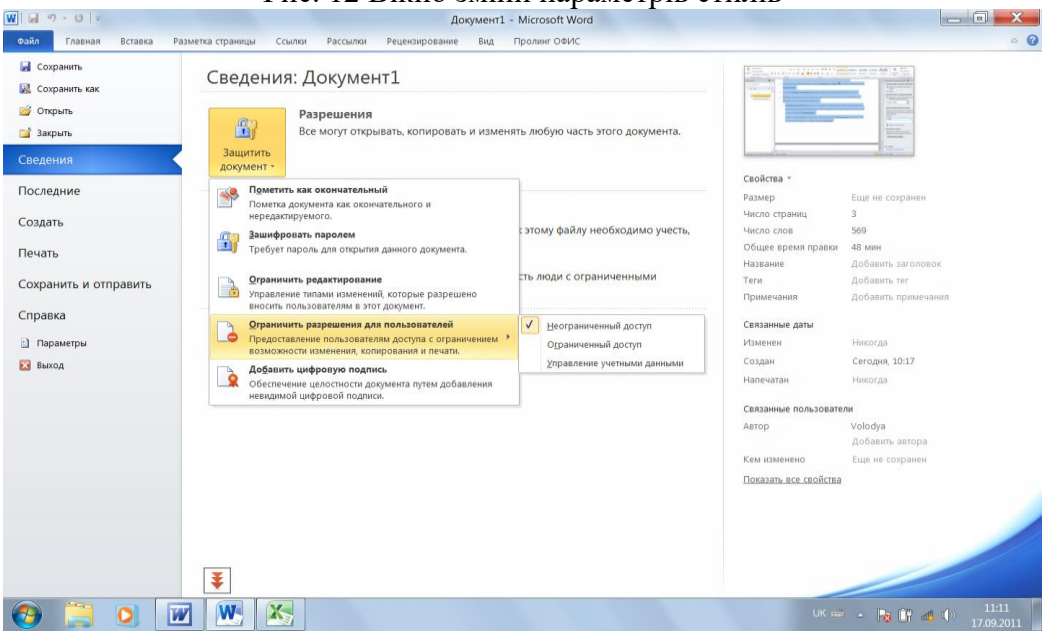


Рис. 13 Вікно відбору прав доступу

Рядки підпису у файлах Office 2010 дозволяють організаціям знизити ризик при обміні даними в електронному вигляді, а також оптимізувати обробку контрактів і інших угод. Цифрові підписи надають відомості про те, що саме було підписано, і можуть бути перевірені в майбутньому.

Одночасно з видимим підписом у документ додається й цифровий підпис для посвідчення особи, яка підписала.

1.9 Створення рядка підпису в документі Word або Excel

1. Помістить покажчик миші в те місце в документі або на аркуші, де необхідно створити рядок підпису.
2. На стрічці **Вставка** в групі **Текст** розкрийте список **Строка подписи** виберіть пункт **Строка подписи Microsoft Office** (рис. 17).

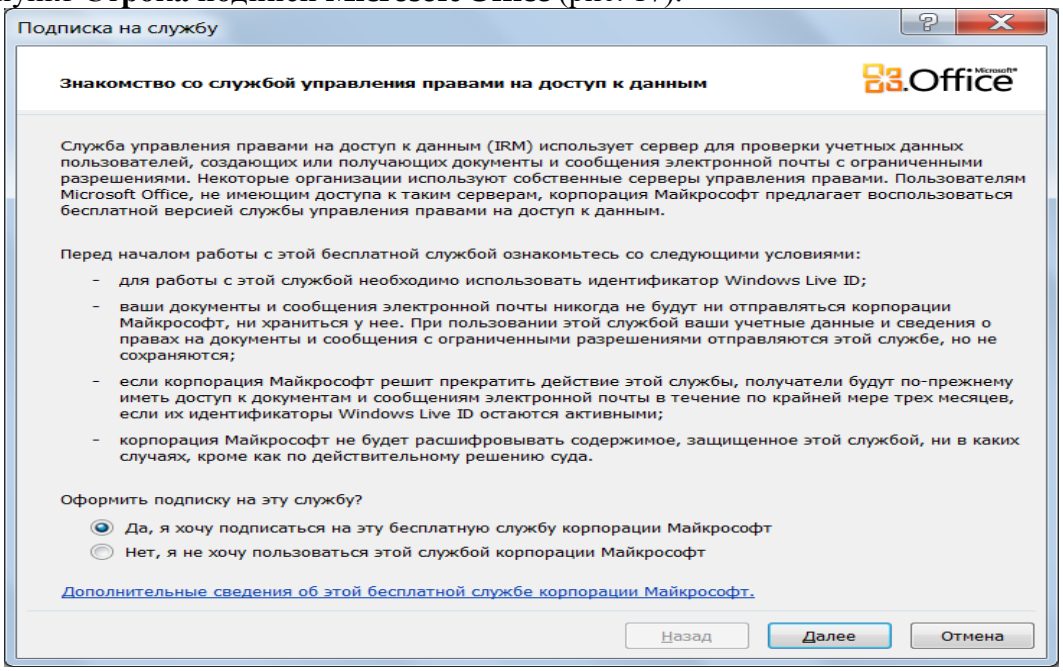


Рис. 14 Вікно майстра підписування на потрібну службу

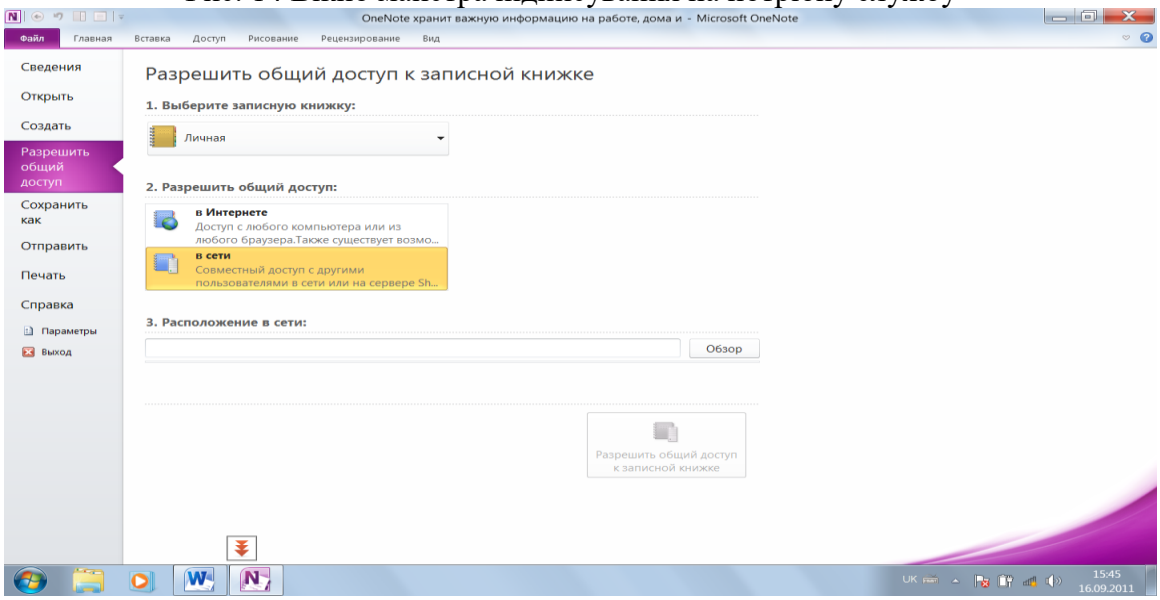


Рис. 15 Вікно відбору захисту записної книжки

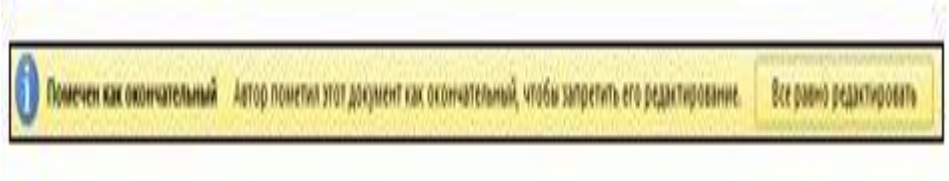


Рис. 16 Вікно повідомлення

- У діалоговім вікні **Настройка подписи** (рис. 18) введіть відомості, які будуть відображені під рядком підпису;

- ім'я того хто підписує. Повне ім'я особи, що підписує;
- посада. Посада особи, що підписує;
- адреса електронної пошти особи, що підписує (при необхідності);
- інструкції для особи, що підписує;
- дозволити, особі що підписує додавати примітки у вікні підпису (вказати мету додавання підпису);
- показувати дату підпису в рядку підпису. **Отображать дату подписи вместе с подписью.**

3. Натисніть кнопку **ОК**.

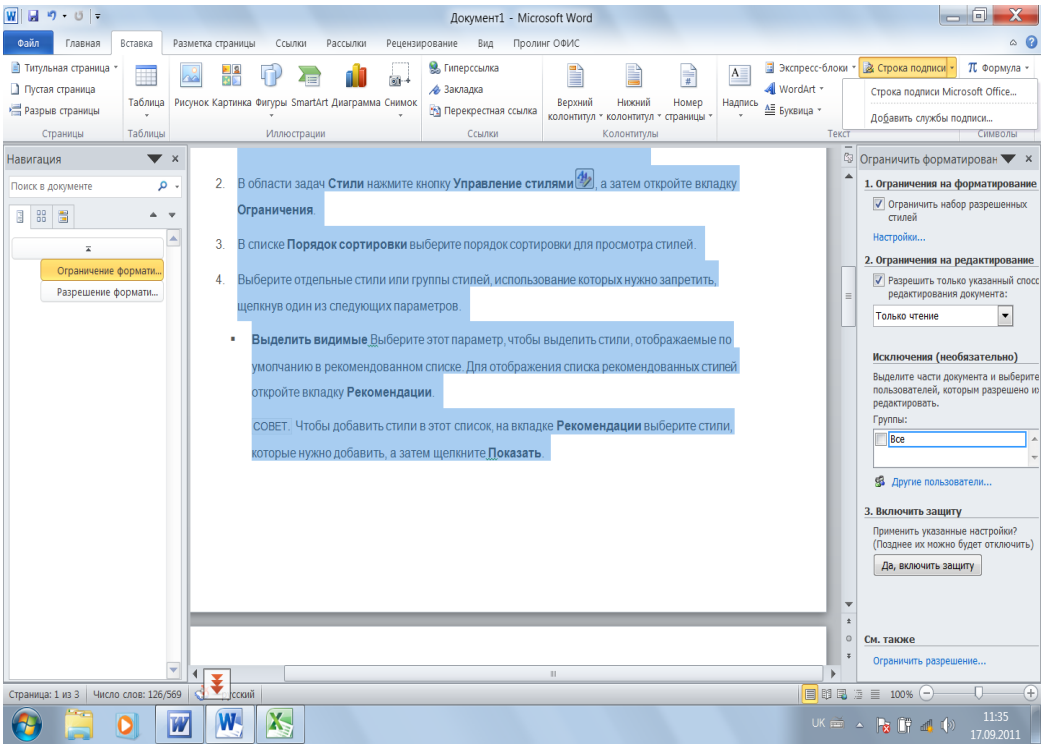


Рис. 17 Вікно відбору підпису

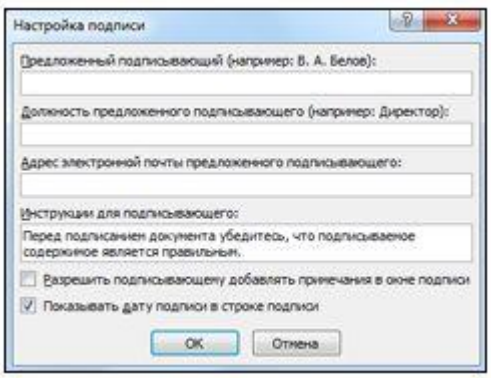


Рис. 18 Вікно налагодження параметрів підпису

На наведеному нижче малюнку показане діалогове вікно налагодження підпису.

Примітка. Якщо документ усе ще не підписаний, з'явиться панель повідомлень **Подписи** (рис. 19). Щоб завершити процес підписання, натисніть кнопку **Просмотр подписей.**

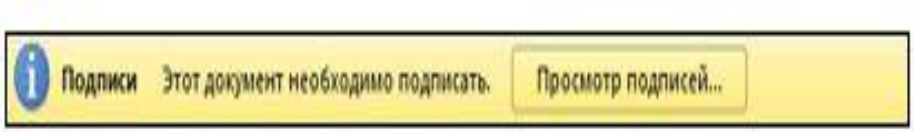


Рис. 19 Вікно панелі підписів

1.10 Видалення цифрових підписів з документа Word або Excel

1. Відкрийте документ або аркуш із видимим підписом, який необхідно вилучити.
2. Клацніть рядок підпису правою кнопкою миші.
3. Виберіть у меню команду **Удалить подпись**.
4. Натисніть кнопку **ОК**.

Примітка. Щоб вилучити підпис, також можна клацнути мишкою поруч із підписом в області підпису й вибрати в меню команду **Удалить подпись**.

1.11 Додавання невидимих цифрових підписів у документ Word, Excel або PowerPoint

Засвідчення дійсності умісту документа, проводиться шляхом додавання нього невидимого цифрового підпису. У нижній частині підписаних документів буде перебувати кнопка **Подпись**. Крім того, для таких документів відомості про підпис відображаються в розділі **Свойства**.

1. Відкрийте вкладку **Файл**. З'явиться вкладка **Backstage**.
2. Клацніть елемент **Свойства**.
3. У розділі **Разрешение** клацніть елемент **Защитить документ, Защитить книгу** або **Защитить презентацию.**
4. Виберіть у меню команду **Добавить цифровую подпись**.
5. Прочитайте повідомлення Microsoft Word, Excel або PowerPoint і натисніть кнопку **ОК**.
6. У діалоговім вікні **Подпись** у поле **Цель подписания документа** вкажіть мету підписання документа.
7. Клацніть елемент **Подпись**.

Після того як у файл буде доданий цифровий підпис, з'явиться кнопка **Подписи**, а сам файл стане доступний тільки для читання.

1.12 Видалення невидимих цифрових підписів з документа Word, Excel або PowerPoint

1. Відкрийте документ, книгу або презентацію з невидимим підписом, який необхідно вилучити.
2. Відкрийте вкладку **Файл**. З'явиться вкладка **Backstage**.
3. Клацніть елемент **Свойства**.
4. Клацніть елемент **Просмотр подписей**.
5. Відбудеться повернення до документа, книги або презентації, і з'явиться панель **Подпись**.
6. Клацніть мишкою поруч із підписом.
7. Виберіть у меню команду **Удалить подпись**.
8. Натисніть кнопку **ОК**.

1.13 Недійсні цифрові підписи

В Word 2010, Powerpoint 2010 і Excel 2010 недійсні цифрові підписи відзначаються червоним текстом в області підпису й червоним знаком X у діалоговім вікні склад підпису (рис. 20). Причини, за якими цифровий підпис може стати недійсною, зазначені нижче.

- цифровий підпис був ушкоджений, оскільки в підписаний ним вміст вносилися зміни;
- сертифікат не був виданий довіреним центром сертифікації. У цьому випадку підпис можна знову зробити дійсним, виразивши довіру видавцеві;
- сертифікат, що використовувався при створенні підпису, був відкликаний, а оцінка часу недоступна.

На наведеному нижче малюнку показана область Підпису з недійсним підписом.

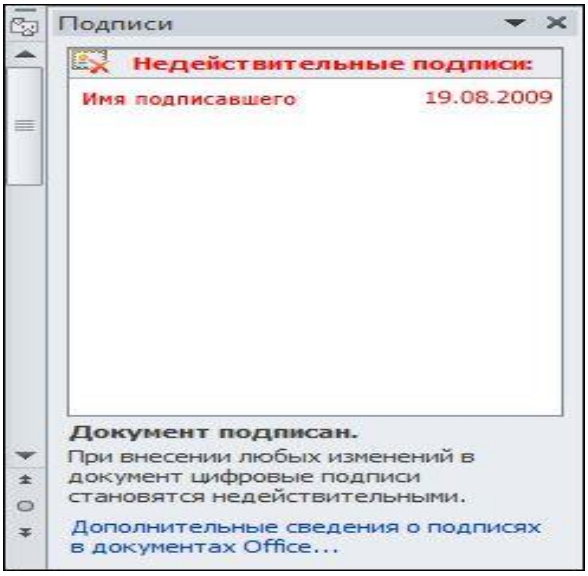


Рис. 20 Відображення недійсного підпису

Виклик діалогового вікна Цифрові підписи

1. Відкрийте файл, що містить цифровий підпис, який потрібно переглянути.
2. Відкрийте вкладку **Файл**. З'явиться вкладка **Backstage**.
3. Відкрийте вкладку **Свойства** й клацніть елемент **Просмотр подписей.** З'явиться область **Подписи**.
4. Клацніть мишкою внизу напроти імені підпису в списку. Виберіть команду **Состав подписи**.
5. Відкриється діалогове вікно **Состав подписи**.

1.14 Посилання на підозрілий web – сайт

В Office 2010 функція виявлення підозрілих посилань на web – сайти за замовчуванням включена. Її можна відключити, щоб не відображалися попередження системи безпеки, однак робити це не рекомендується.

1. У додатку Office відкрийте вкладку **Файл**. З'явиться вставка **Backstage**.
2. У меню **Справка** виберіть пункт **Параметры**. З'явиться діалогове вікно **Параметры**.
3. Клацніть елемент **Центр управления безопасностью**, а потім – **Параметри центра управления безопасностью.**
4. Натисніть кнопку **Параметры конфиденциальности**.

5. В області **Параметры конфиденциальности** встановіть або зніміть прапорець **Проверка документов Microsoft Office**, узятих з підозрілих web – сайтів або утримуючих посилання на такі web – сайти.

6. Натисніть кнопку **ОК** (рис 21).

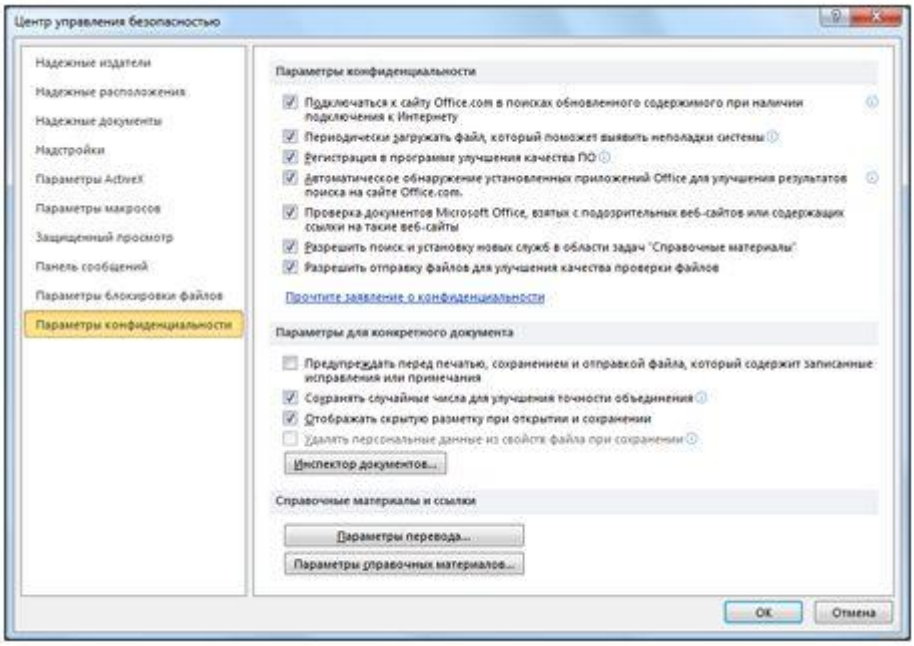


Рис. 21 Параметри центра управління безпекою

1.15 Включення й відключення попереджень системи безпеки на панелі повідомлень

1. У додатку Office відкрийте вкладку **Файл**. З'явиться вкладка **Backstage**.

2. У меню **Справка** виберіть пункт **Параметры**, щоб відкрити діалогове вікно **Параметры**.

3. Клацніть елемент **Центр управления безопасностью**, а потім – **Параметри центра управления безопасностью.**

4. Клацніть елемент **Панель сведений**, щоб відкрити діалогове вікно **Параметры панели сведений** для всіх додатків Office.

В панелі можна вибрати параметри:

- показувати панель повідомлень у всіх додатках, якщо вміст документа заблокований. Цей параметр використовується за замовчуванням. Панель повідомлень з'являється щораз при відключенні потенційно небезпечного вмісту;
- ніколи не показувати відомості про заблокований уміст. Цей параметр відключає панель повідомлень, через що не виводяться повідомлення ні про які проблеми з безпекою (незалежно від значень параметрів безпеки в центрі керування безпекою).

Примітка. Рекомендується не змінювати параметри безпеки в центрі керування безпекою. Це може привести до втрати або крадіжки даних, а також зниженню рівня захисту комп'ютера або мережі.

1.16 Захист від фішингу і інших підозрілих схем в Internet

У центрі керування безпекою можна налагодити параметри безпеки й конфіденційності для додатків Microsoft Office 2010. Завдяки однаковому інтерфейсу

стрічки у всіх додатках Office для переходу в центр керування безпекою використовується та сама послідовність дій.

1. У додатку Office відкрийте вкладку **Файл**. З'явиться вкладка **Backstage**.
2. У меню **Справка** виберіть пункт **Параметры**, щоб відкрити діалогове вікно **Параметры**.
3. Клацніть елемент **Центр управления безопасностью**, а потім – **Параметры центра управления безопасностью**.
4. Нижче зазначені доступні параметри (деякі з них можуть відрізнятися).

- надійні видавці. Складіть список видавців програмних проектів, яким можна довіряти;
- надійні розташування. Укажіть теки на комп'ютері, у які будуть поміщатися надійні файли з довірених джерел. Документи в надійних теках не зазнають перевірки файлів;
- надійні документи. Налагодьте параметри взаємодії додатків Office з активним умістом;
- надбудови. Укажіть, чи повинні надбудови вимагати наявності цифрових підписів, або відключіть надбудови;
- параметри Activex. Використовуйте ці параметри для керування повідомленнями системи безпеки для елементів Activex у додатках Office;
- параметри макросів. Включіть або відключіть макроси в програмах Office;
- панель повідомлень. Відобразіть або сховайте панель повідомлень;
- параметри блокування файлів. Укажіть, чи будуть відкриватися більш ранні версії файлів додатків Office;
- параметри конфіденційності. Ці параметри визначають рівень конфіденційності при роботі із програмами Office;
- клацніть потрібну область і налагодьте відповідні параметри.

2. Хід роботи

1. Проведіть шифрування довільного документа
2. Проведіть захист аркуша та його структури в Microsoft Excel
3. Помітьте довільного документ, як кінцевий
4. Проведіть обмеження змін в довільному документі Microsoft Word 2010
5. Проведіть обмеження змін в довільному документі Microsoft Excel 2010
6. Проведіть обмеження дозволів для користувачів до довільної записної книжки в Microsoft OneNote
7. Створіть рядок підпису (звичайний та невидимий) в довільному документі Microsoft Word
8. Створіть рядок підпису (звичайний та невидимий) в довільному документі Microsoft Excel
9. Перегляньте цифрові підписи
10. Проведіть видалення підпису в довільному документі Microsoft Word та Excel
11. Проведіть включення й відключення попереджень системи безпеки на панелі повідомлень

3. Контрольні питання

1. Які можливості надає Microsoft Office 2010 для захисту документів?
2. Які паролі є надійними?
3. Як провести захист аркуша та його структури в Microsoft Excel?

4. Як помітити довільного документ, як кінцевий?
5. Як провести обмеження змін в документі Microsoft Word?
6. Як провести обмеження змін в документі Microsoft Excel?
7. Як провести дозволів для користувачів до довільної записної книжки в Microsoft OneNote?
8. Як створити рядок підпису в документі Microsoft Word?
9. Як створити рядок підпису в документі Microsoft Excel?
10. Як видалити підпис в довільному документі Microsoft Word та Excel?
11. Як створити рядок невидимого підпису в документі Microsoft Word?
12. Як створити рядок невидимого підпису в документі Microsoft Excel
13. Як переглянути цифрові підписи?
14. Як відключити посилання на підозрілий web – сайт?
15. Як провести включення й відключення попереджень системи безпеки на панелі повідомлень?

Як провести Захист від фішингу і інших підозрілих схем в Internet?

Лабораторна робота 13
Пошук паролів у документах Microsoft Office за допомогою спеціальних програм.

Мета роботи ═засвоїти принципи і технологію роботи з програмами дешифраторами паролів Advanced Office 97 Password Recovery.

Ознайомитись з поняттям, принципом роботи та призначенням головного меню програм дешифраторів паролів.

ПЛАН

1. Теорія
2. Хід роботи:
3. Контрольні питання:

1. Теорія:

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

1. Advanced Office 97 Password Recovery - Дозволяє знаходити всі паролі Word 97/2003, Excel 97/2003, Access 97/2003. (крім паролів користувачів/груп).
2. Advanced Office 95 Password Recovery.

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

3. Advanced VBA Password Recovery.

Дозволяє знаходити всі паролі на VBA-макроси Word/Excel 97. Для макросів Office 2003 є комерційна версія програми.

4. Advanced Outlook Password Recovery. Паролі MS Outlook.

Для визначення паролю документу (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.1) в якому необхідно вибрати захищений файл та підібрати необхідні параметри пошуку і подати команду почати перебір із підменю пароль. Можливі три режими переборів паролів:

1. 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.
2. 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 „#”.
3. Атака за словарем. Цей режим включає використання для порівняння готових паролів, які знаходяться в додатковому словнику. Використовується в тому випадку коли необхідно використати найменше часу на знаходження паролю, але не завжди приводить до необхідного результату.

Рис.1. Діалогове вікно програми Advanced Office 97 Password Recovery.

Використання опції почати з може бути корисним, коли відомі деякі символи паролю. Після успішного опрацювання паролю програмою буде виведене діалогове віконце (рис.2) з вказанням знайденого паролю та деякими параметрами пошуку.

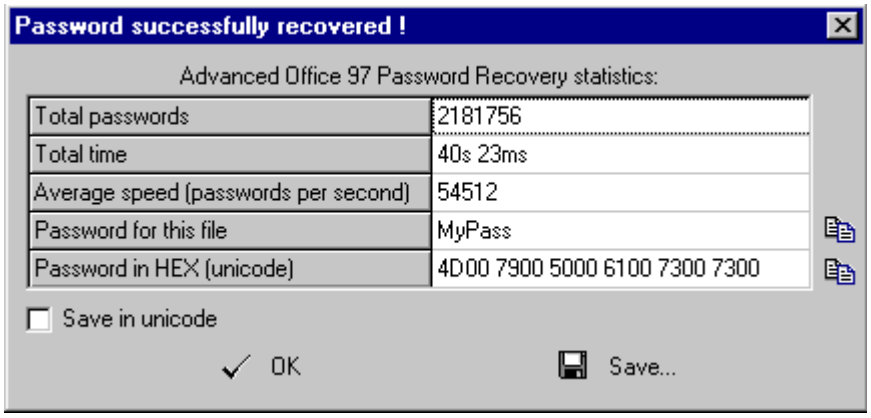


Рис.2 Діалогове вікно результатів пошуку.

Час пошуку залежить від параметрів, приклад яких наведено в табл.1

Табл.1

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 букви пробіли	6	62,523,502,592	17 годин
Цифри, маленькі букви пробіли	7	94,931,877,888	26 годин

2. Хід роботи

1. Створити файли в Microsoft Word, Excel, Access та встановити паролі, які містять 6 латинських символів .

2. Знайти вказані паролі за допомогою програми Advanced Office 97 Password Recovery.
3. Створити файли в Microsoft Word, Excel, Access та встановити паролі, які містять 10 латинських символів та спеціальні символи.
4. Знайти вказані паролі за допомогою програми Advanced Office 97 Password Recovery.

3. Контрольні питання:

1. Які програмні продукти застосовуються для пошуку паролів?
2. Вимоги до паролів документів Microsoft Office.
3. Складові діалогово віконця програми Advanced Office 97 Password Recovery.
4. Режими підбору паролів та їх характеристики.
5. Маски пошуку паролів.
6. Залежність часу пошуку паролю від його параметрів.
7. Складові діалогово віконця програми Advanced ZIP Password Recovery.

РОЗДІЛ 3
Захист інформації шифруванням

Лабораторна робота 14
Шифрування даних за допомогою архіваторів та пошук паролів

Мета роботи – Засвоїти принципи і технологію роботи з шифрованими архівами та програмами дешифраторами паролів.

Ознайомитись з поняттям, принципом роботи та призначенням головного меню програм дешифраторів паролів Ultra Zip Password Cracker 1.00 та Advanced ZIP Password Recovery 2.2 .

План

1. Теорія
1.1 Шифровані архіви
1.2. Програми відновлення паролів:
2. Хід роботи
3. Контрольні питання

1. Теорія
1.1. Шифровані архіви

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 чи на рівні дисків. До програм першого типу можна віднести архіватори типу ARJ і RAR, що 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.

1. Архів ARJ:

Захист архіву паролем 123: arj a -g123 name - створення архіву.

Витяг з архіву з паролем 123: arj e -g123 name.arj

2. Архів ZIP:

Захист архіву паролем 45: pkzip a-s45 name - створення архіву.

Витяг з архіву з паролем 45: pkunzip a-s45 name.zip

3. Архів WinRar:

Protect Archive from Damages (Захистити архів від ушкоджень) – дана команда вносимо архів додаткові дані, що будуть запобігати його від ушкоджень.

Lock Archive (Заблокувати архів) – після того, як дана команда була обрана, архів стає заблокованим від внесення в нього яких-небудь змін.

4. 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 ви можете знайти "програми-ломалки" для зашифрованих архівів. Наприклад, архів типу ZIP “зламується” на потужному комп'ютері за кілька хвилин, при цьому від користувача не потрібно високої особливої кваліфікації.

1.2. Програми відновлення паролів:

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. "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. 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:

1 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.
2 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 „#”.
3 Атака за словарем. Цей режим включає використання для порівняння готових паролів, які знаходяться в додатковому словнику. Використовується в тому випадку коли необхідно використати найменше часу на знаходження паролю, але не завжди приводить до необхідного результату.

2. Хід роботи

1. Створити в редакторі Microsoft Word файл під назвою Student на диску “D” наступного змісту:
2. Провести процес архівації відповідно до пунктів 1-4 теорії без застосування паролів та з їх застосуванням.
3. Спробувати відкрити архіви програмами із пакета Microsoft Office без процесу розархівації.
4. Спробувати відкрити архіви програмами із пакета Microsoft Office після процесу розархівації.
5. Створити архів за допомогою програми WinZip та встановити пароль, який містять послідовно: 5,10,15 латинських символів.
6. Створити архів за допомогою програми WinRar та встановити пароль, який містять послідовно: 5,10,15 латинських символів
7. Знайти вказані паролі за допомогою програми Advanced ZIP Password Recovery.

Рис.1 Діалогове вікно програми Advanced ZIP Password Recovery.

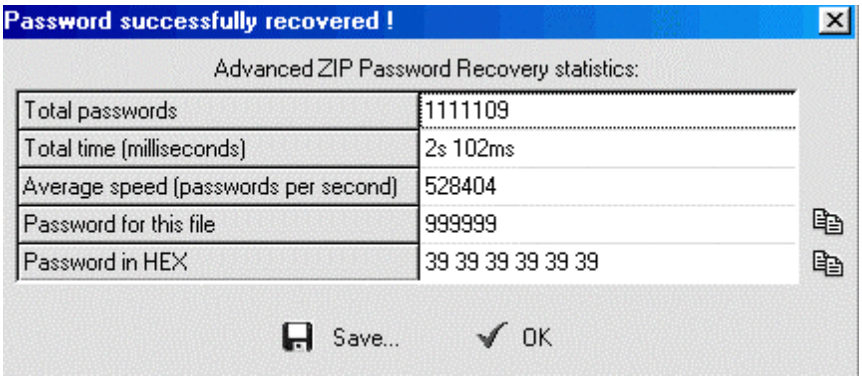


Рис.2. Діалогове вікно результатів пошуку.

3. Контрольні питання:

1. Порядок встановлення паролів на архівні файли
2. Порядок пошуку паролів в архівах із декількома файлами, які мають різні паролі.

Лабораторна робота 15
Шифрування даних за допомогою спеціальних програм та утиліт.

Мета роботи ═засвоїти принципи, технологію роботи шифрування та дешифрування файлів.

ПЛАН

1. Теорія
1.1 Програма Super File Encryption (Шифрування Файлу Високої якості)
1.2 Робота з утилітою: (T-CEC Pro).
1.2.1 Правила використання.
1.3 Система шифрування даних BestCrypt
1.3.1 Використання в Мережі
1.3.2 Поняття контейнера
1.3.3 Використання генератора ключів
1.3.4 Робота зі схованим і оригінальним контейнерами
2. Хід роботи
3. Контрольні питання

1. ТЕОРІЯ

1.1 Програма Super File Encryption (Шифрування Файлу Високої якості)

Потужна та зручна в роботі програма призначена для того, щоб зашифрувати і захистити ваші дані – зручна для офісів, які тримають важливі документи. Щоб зашифрувати або розшифровувати файли/папку, просто клацніть на файлах, і виберіть команду Зашифрувати або Розшифрувати . Програмне забезпечення також дозволяє Вам 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. 1) .

Примітка: при першому запуску програми вікно буде мати два поля в які необхідно внести ваш початковий пароль.

Рис. 1. Початкове вікно введення паролю.

Після запуску програми з'явиться діалогове вікно (рис. 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. 2). Для дешифрування файлу (ів) необхідно їх вказати в діалоговому діалоговому вікні (рис. 2) і натиснути клавішу **Decrypt**. Після цього програма проведе дешифрування файлу (ів). Для зміни паролю адміністратора і вибору параметрів шифрування необхідно натиснути клавішу **Optima** і вибрати зазначені параметри (рис.3) і змінити пароль (рис. 4). У вікні

рис. 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.

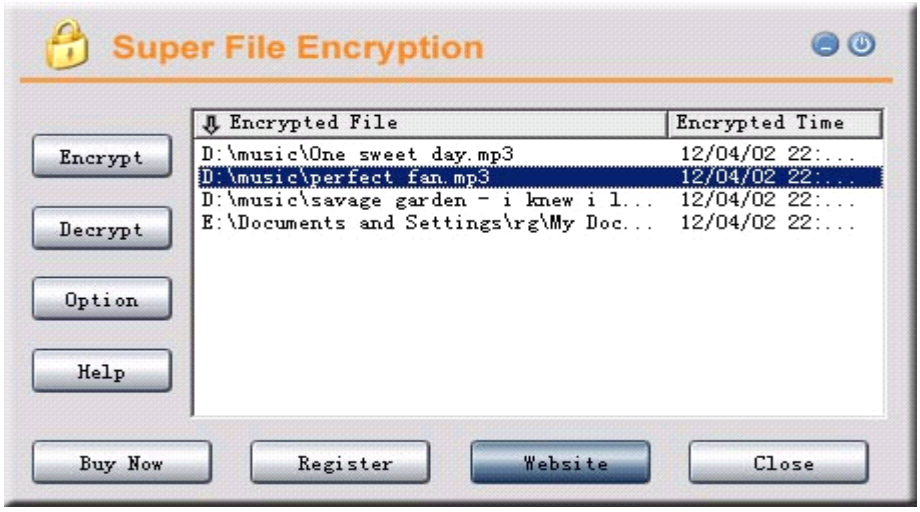


Рис. 2. Вікно програми

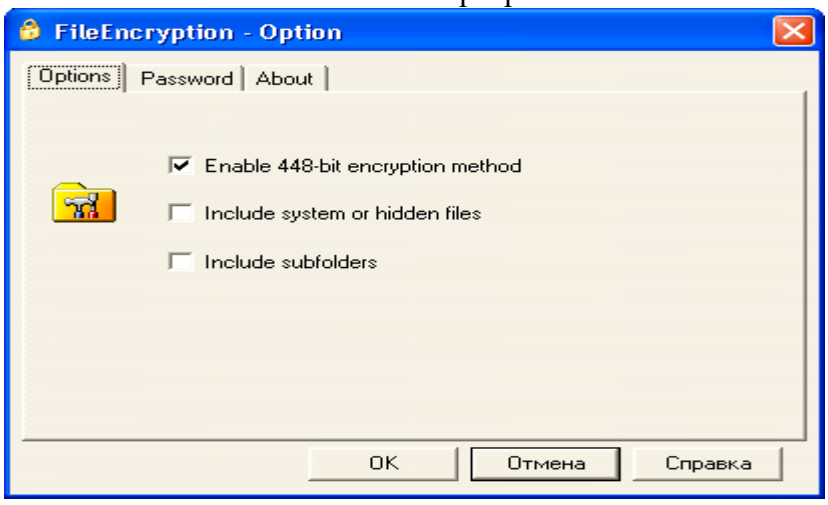


Рис. 3. Вікно добору параметрів шифрування.

Рис. 4. Вікно зміни паролю.

Ви можете перевірити результати шифрування , наприклад, через провідника Windows (рис. 5)

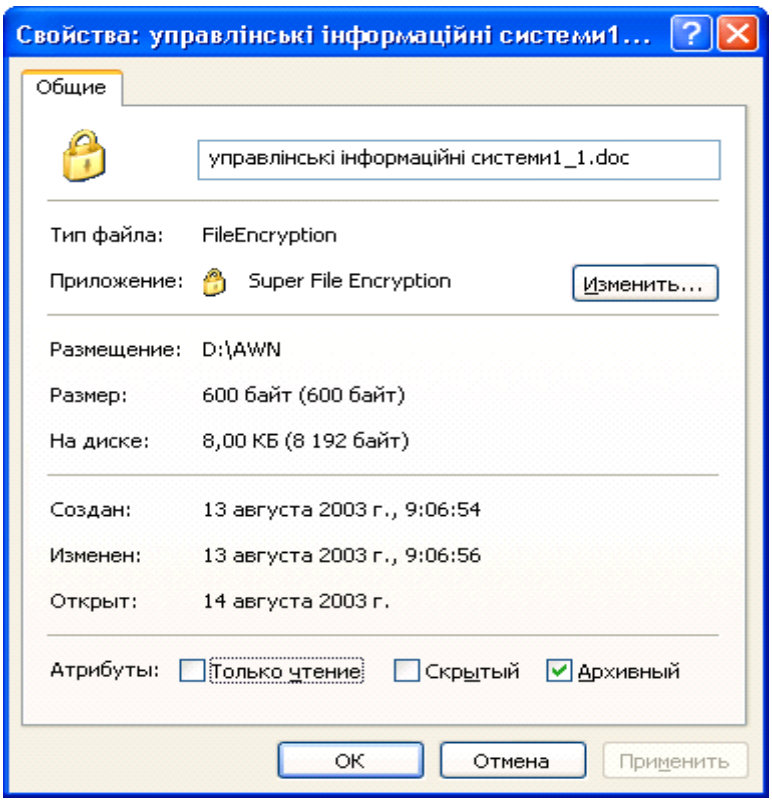


Рис. 5. Перевірка результатів шифрування з використанням провідника Windows

1.2 . 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. 6)

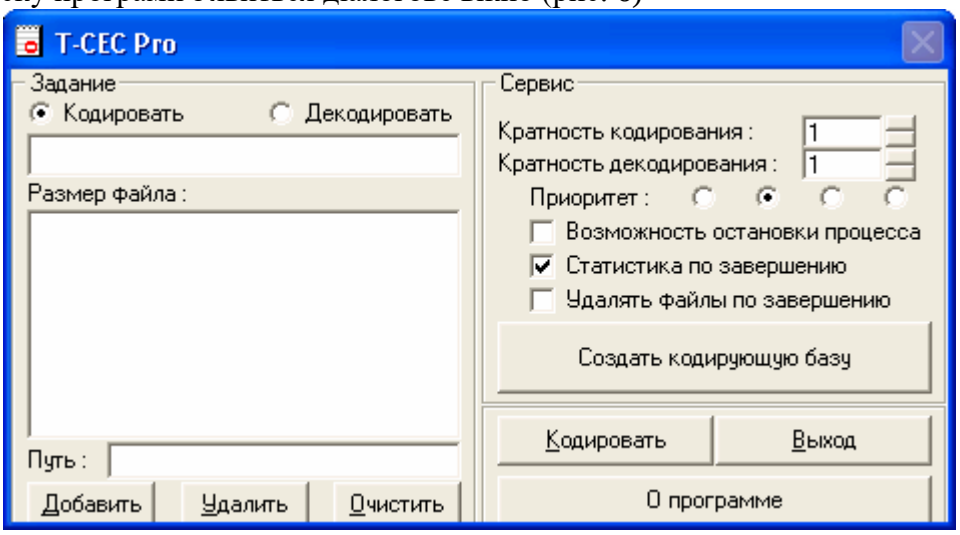


Рис. 6. Вікно утиліти

1.2.1 Правила використання.

- У верхній частині вікна вибирається операція (**кодировать/декодировать**);
- вибирається файл (и) за допомогою кнопки **Добавить**;
- список можна редагувати за допомогою кнопки **Удалить**;
- список можна очистити за допомогою кнопки **Очистить**;
- далі треба створити базу, що кодує, (розмір бази = 256 byte) (використовуємо відповідну кнопку);
- далі натискаємо кнопку **кодировать/декодировать** 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 залізти в контекстне меню усіх файлів, для цього треба подивитися **О программе** (натискаємо відповідну кнопку) (рис. 7.);

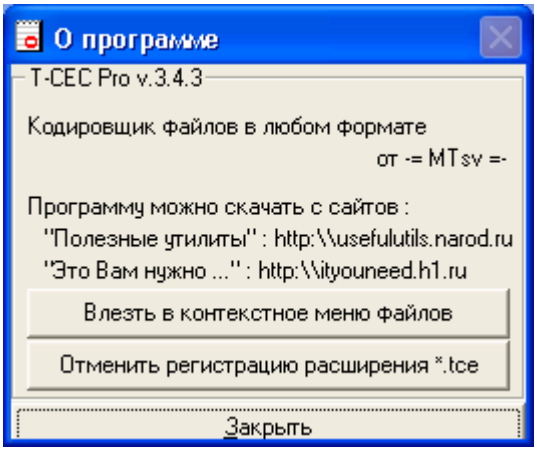


Рис. 7. Вікно **О программе**

Примітка: Якщо пошкодите базу, то утратите всі закодовані в ній документи робіть кілька копій одної і тієї ж бази. База повинна бути одна для кодування і декодування.

1.3 Система шифрування даних BestCrypt

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

Метод шифрування даних BestCrypt використовує алгоритми шифрування відомий міжнародний: Blowfish, Twofish, Rijndael і GOST, забезпечує безпрецедентний захист проти неправомочного доступу даних. Після, як створено контейнер, дані ніколи не зберігаються в відкритому стані. Вони захищені і зашифровані, яким методом би Ви не копіювали чи переміщували дані в контейнер.

BestCrypt використовує наступні алгоритми шифрування:

- алгоритм Blowfish -- у способі Формування ланцюжка Блоку Шифру з ключовою довжиною на 256 битів;
- Twofish алгоритм -- у способі Формування ланцюжка Блоку Шифру з ключовою довжиною на 256 битів;
- Rijndael алгоритм -- у способі Формування ланцюжка Блоку Шифру з ключовою довжиною на 256 битів;

- ГОСТ 28147-89 (російський Федеральний Стандарт Шифрування) у способі Зворотного зв'язку Шифру з ключовою довжиною на 256 битів.

Алгоритм Blowfish був розроблений Брюсом Шнеиром у 1993 р. 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).

BestCrypt система дозволяє користувачеві вибирати алгоритм Blowfish , Rijndael, ГОСТ або Twofish, щоб забезпечити безпеку даних, втому числі, і з як використанням всіх алгоритмів одночасно.

1.3.1 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 і звертатися до контейнерів файлу. Цей диск мережі може бути розділений комп'ютером з будь-якою операційною системою, наприклад ПОДІБНІ UNIX операційні системи (OSF/1, LINUX, BSD, SunOS, ЕКС-АН-ПРОВАНС і інші), Novell, Windows NT, Windows 95, Windows 3.xx і інші.

1.3.2 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. Ви повинні визначити пароль, коли Ви створюєте контейнер і використовувати той же самий пароль, коли Ви відкриваєте дійсний (віртуальний) диск, зв'язаний з контейнером. Використовуючи BestCrypt Пульт керування Ви можете змінити (замінити) пароль для зазначеного контейнера.

Зверніть увагу: Якщо Ви забудете пароль для ваших зашифрованих даних, Ви абсолютно втратите здатність одержати доступ до них.
Цей метод шифрування не дозволяє Вам "повертати" інформацію, не знаючи паролю. Не забудьте пароль! Наприклад, запишіть це на папері, і помістіть цей папір в сейф.

BestCrypt має сильну, убудовану схему шифрування і не містить ніякого "люка". "Люк" – назва (ім'я) 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. Але не BestCrypt. Єдиний шлях одержати доступ до даним, захищеним BestCrypt полягає в тому, щоб мати відповідний пароль.

Після запуску програми з'являється діалогове вікно (рис. 8) . Для шифрування файлів спочатку ви повинні створити контейнер, для цього з під меню Контейнер уводиться команда **Новый Контейнер** і вказується його розміщення, ім'я та інші параметри (рис. 9).

На кожен контейнер установлюється пароль (рис. 10), або проводиться його зміна за необхідністю.

1.3.3 Використання генератора ключів

Використання цієї області, дозволить Вам змінити ключовий алгоритм генератора, що у даний час використовується BestCrypt системою, 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 Ви можете залишить програму. Ваш секретний дійсний (віртуальний) диск X: тепер доступний точно так само як нормальний дисковод. Усе, що Ви пишете на диск, буде автоматично зашифровано і потім при необхідності дешифровано, коли Ви читаєте дані з диска.

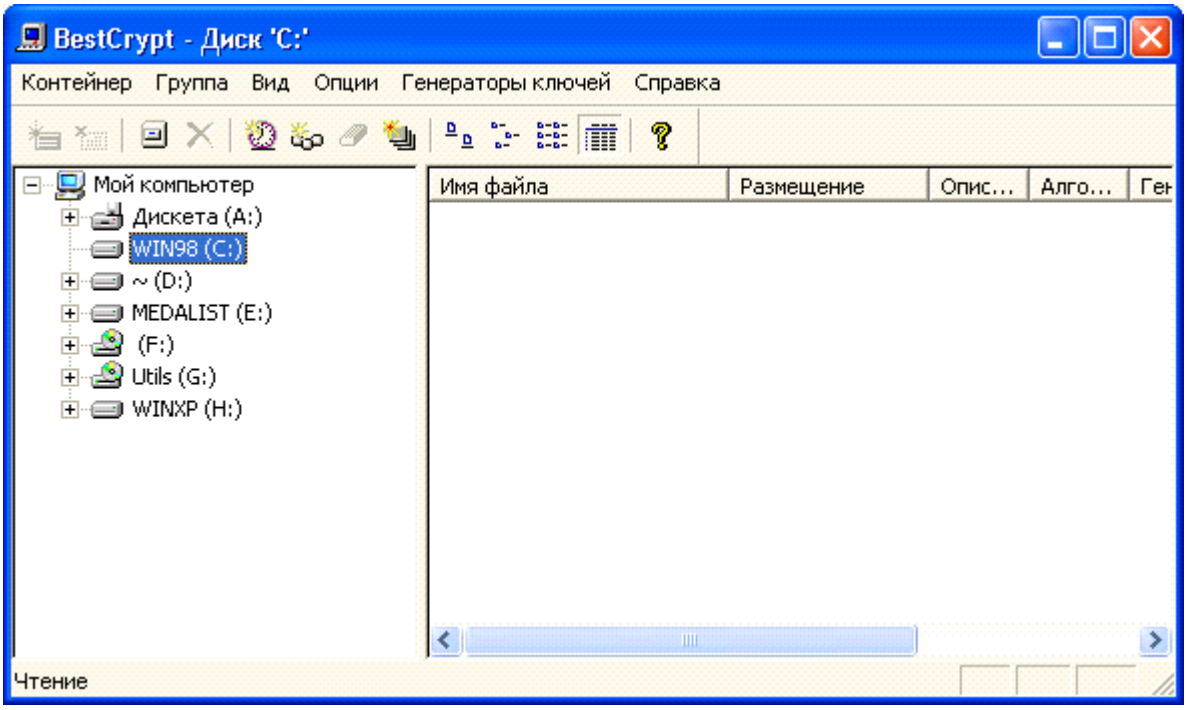


Рис. 8. Діалогове вікно програми.

Примітка. BestCrypt Пульт керування показує інформацію в контейнерах у групі Списку Контейнерів виразно для кожного користувача, що може почати роботу (ввійти в систему) на ваш комп'ютер. Наприклад, користувачі Джон і Аліса входять з різним іменами користувача, коли вони починають роботу (входять у систему). Якщо Джон створює контейнер 'Мій container.jbc' у деякому довіднику, наприклад, у C:\JOHN довіднику, BestCrypt Пульт керування не буде показувати контейнер, якщо Аліса починає роботу (входить у систему).

1.3.4 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 дешифрування ключа шифрування з ключового блоку даних. Програмне забезпечення використовує ключ для забезпечення прозорого шифрування даних у третій частині контейнера.

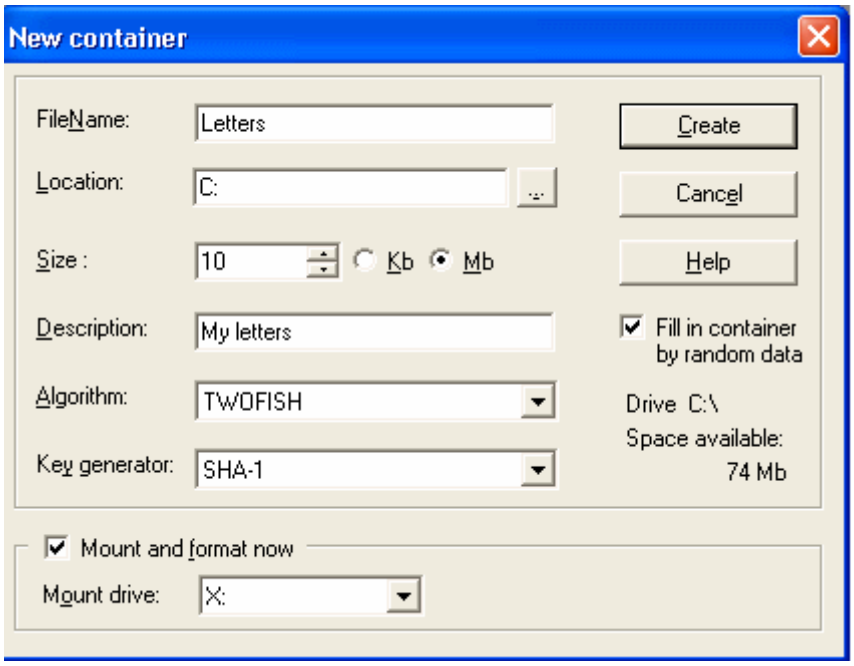


Рис. 9. Вікно вибору параметрів нового контейнера.

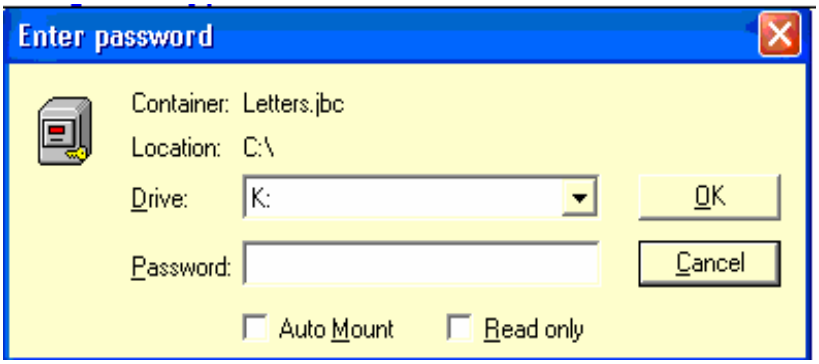


Рис. 10. Вікно встановлення паролю на контейнер.

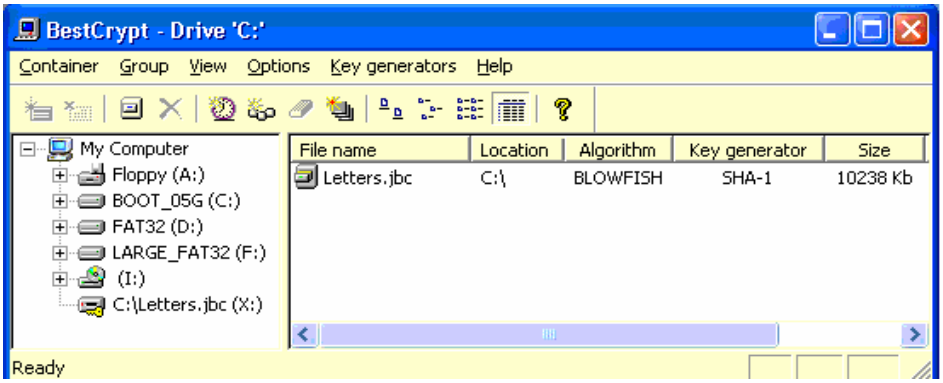


Рис. 11. Вікно зі створеним контейнером.

Якщо Ви створюєте 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 будь-який інший чи ключ ні. Запам'ятаєте, вільний дисковий простір у межах контейнера самостійно зашифрований як випадкові дані.

Так, заміна деяких випадкових даних новим випадково згенерованим 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 не підходить для установки оригінального контейнера, BestCrypt перевіряє існування схованої частини в контейнері і використовує значення випадкових даних, згенерованих з пароля, для витягу ключа шифрування із 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: Зверніть увагу на це повідомлення: якщо воно не з'являється, значить схована частина не встановлена!

3. Увага!

I. Ви можете записати деякі дані в оригінальний контейнер перед створенням схованої частини. Але як тільки Ви створили ваш схований контейнер, ніякі дані не повинні коли-небудь, записуватися в оригінальний контейнер. Якщо ви зробите запис в оригінальний контейнер, схована частина може бути ушкоджена!

2. Хід роботи

1. Проведіть шифрування двох довільних файлів з диску “C” вашого комп'ютер програмою Super File Encryption.
2. Проведіть дешифрування двох довільних файлів з диску “C” вашого комп'ютер програмою Super File Encryption.
3. Перевірте результати шифрування з іншої програми.
4. Проведіть шифрування та дешифрування двох довільних файлів з диску “C” вашого комп'ютер утилітою (T-CEC Pro).
5. Створіть на диску “C” вашого комп'ютера довільний контейнер програмою BestCrypt.
6. Скопіюйте декілька файлів в контейнер з сервера та перевірте можливість доступу до них без знання пароля та з наявним паролем.

3. Контрольні питання

1. Призначення програми Super File Encryption .
2. Порядок шифрування файлів в програмі Super File Encryption.
3. Порядок дешифрування файлів в програмі Super File Encryption.
4. Порядок підбору параметрів шифрування та дешифрування файлів.
5. Призначення утиліти (T-CEC Pro).
6. Порядок шифрування дешифрування файлів утилітою (T-CEC Pro).
7. Призначення системи шифрування даних BestCrypt.
8. Які алгоритми шифрування підтримує BestCrypt?
9. Короткі характеристики алгоритмів шифрування, які підтримує BestCrypt?
10. Поняття контейнера в системі шифрування даних BestCrypt.

11. Призначення генератора ключів в системі BestCrypt.
12. Особливості роботи зі Схованим і Оригінальним контейнерами.

Лабораторна робота 16
Шифрування даних за допомогою операційної системи Windows XP.

Мета роботи ═ засвоїти принципи, технологію роботи шифрування та перевірки підпису файлу в операційної системи Windows XP.

ПЛАН

1. Теорія
1.1 Загальні відомості про шифровану систему Windows XP.
1.2 Шифрування файлу чи каталоги
1.3 Розшифрування файлу чи каталоги
1.4 Шифрування та дешифрування файлів та каталогів на віддаленому комп'ютері.
1.5 Шифрування та дешифрування файлів та каталогів на віддаленому комп'ютері.
1.6 Використання програми перевірки підпису файлу
2. Хід роботи
3. Контрольні питання

1. ТЕОРІЯ

1.1 Загальні відомості про шифровану систему Windows XP.

Файлова система (EFS) забезпечує ядро технології шифрування файлів, використовуваної для збереження шифрованих файлів на томах файлової системи NTFS. Після того як файл чи каталог зашифровані, із ними працюють так само, як і з іншими чи файлами 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 подібно 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 чи скопіювати зашифрований файл або папку 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» чи «схований». Якщо шифрується каталог, усі файли і підкаталоги, створені в зашифрованій папці, автоматично шифруються. Рекомендується використовувати шифрування на рівні каталоги.

Файли й каталоги можуть також бути зашифровані чи 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 томах 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 каталоги, файл чи каталог перетворяться до стану без стиску.

Зашифровані файли можуть стати розшифрованими, якщо файл копіюється чи переміщається на файлову систему, яка не є томом NTFS.
При переміщенні незашифрованих файлів у зашифровану папку вони автоматично шифруються в новій папці. Однак зворотна операція не приведе до автоматичної розшифрування файлів. Файли необхідно явно розшифрувати.
Не можуть бути зашифровані файли з атрибутом «Системний» і файли в структурі каталогів системний кореневий каталог.

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

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

1.2 Шифрування файлу чи каталоги

Відкрийте провідник Windows. Клацніть правою кнопкою миші чи файл папку, що потрібно зашифрувати, і виберіть із контекстного меню команду **Свойства**. На вкладці **Общие** натисніть кнопку **Другие** (рис. 1). Установіть прапорець **Шифровать содержимое для защиты данных** (рис. 2).

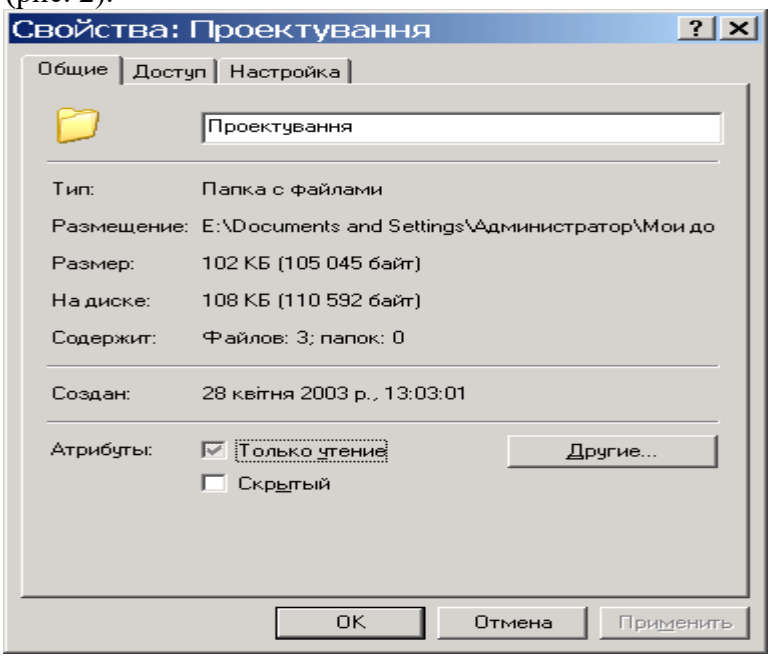


Рис. 1. Вікно властивостей каталогу.

Стиснуті файли й каталоги не можуть бути зашифровані. Якщо шифрування виконується для стиснутого файлу чи каталоги, файл чи каталог перетворяться до стану без стиску. Не можуть бути зашифровані файли з атрибутом **Системний** і файли в структурі каталогів системний кореневий каталог. Коли шифрується окремий файл, система запросить підтвердження необхідності зашифрувати також і папку, що містить цей файл. Якщо підтвердження отримане, усі файли і підкаталоги, що додаються в папку в майбутньому, будуть зашифровані при додаванні.

Коли шифрується каталог, система запросить підтвердження необхідності зашифрувати також файли і підкаталоги в даній папці. Якщо підтвердження отримане, усі файли і підкаталоги, розташовані в папці, шифруються, так само як і усі файли і підкаталоги, що будуть додані в папку в майбутньому. Якщо обране шифрування тільки каталоги, усі файли і підкаталоги в даній папці залишаються незашифрованими. Однак будь-які файли і підкаталоги, що додаються в папку в майбутньому, будуть зашифровані при додаванні.

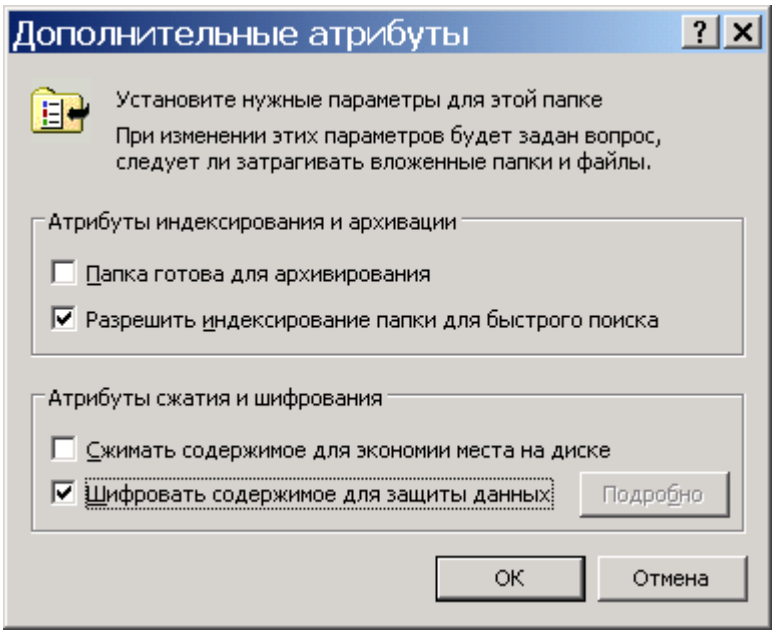


Рис. 2. Вікно вибору процесу шифрування.

1.3 Розшифрування файлу чи каталоги

Відкрийте провідник Windows. Правою кнопкою миші клацніть зашифровану папку чи диск, потім виберіть команду **Свойства**. На вкладці **Общие** натисніть кнопку **Дополнительно**. Зніміть прапорець **Шифровать содержимое для защиты данных**. Коли розшифровується каталог, система запросить підтвердження необхідності розшифровувати також файли і підкаталоги в даній папці. Якщо обране розшифровування тільки каталоги, зашифровані файли й каталоги в розшифрованій папці залишаються зашифрованими. Однак нові файли й каталоги, створювані в розшифрованій папці, не будуть зашифровуватися автоматично.

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

Щоб зашифрувати файл чи папку на віддаленому комп'ютері необхідно відкрити провідник Windows. У меню **Сервис** виберіть команду **Подключить сетевой диск** і потім виконуйте інструкції у діалоговому вікні **Подключить сетевой диск**. Клацніть правою кнопкою миші файл чи папку, що потрібно зашифрувати, і виберіть із контекстного меню команду **Свойства**. На вкладці **Общие** натисніть кнопку **Дополнительно**.
Установіть прапорець **Шифровать содержимое для защиты данных**.
Примітка. 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 каталоги, файл чи 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 папці. 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.

1.5 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 не підписані файли (рис. 3) й одержувати наступні відомості про їх:

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

Відкрийте вікно **Проверка підписи файла**. Якщо використати в діалоговому вікні (рис. 4) кнопку Д**ополнительно**, то це дасть можливість пошуку різноманітних файлів (рис 5) та можливість вибору журналу і параметрів його ведення. Щоб запустити програму перевірки підпису файлу, виберіть у меню **Пуск** команду **Виполнить**, уведіть **sigverif** і натисніть кнопку **ОК** (рис 4).

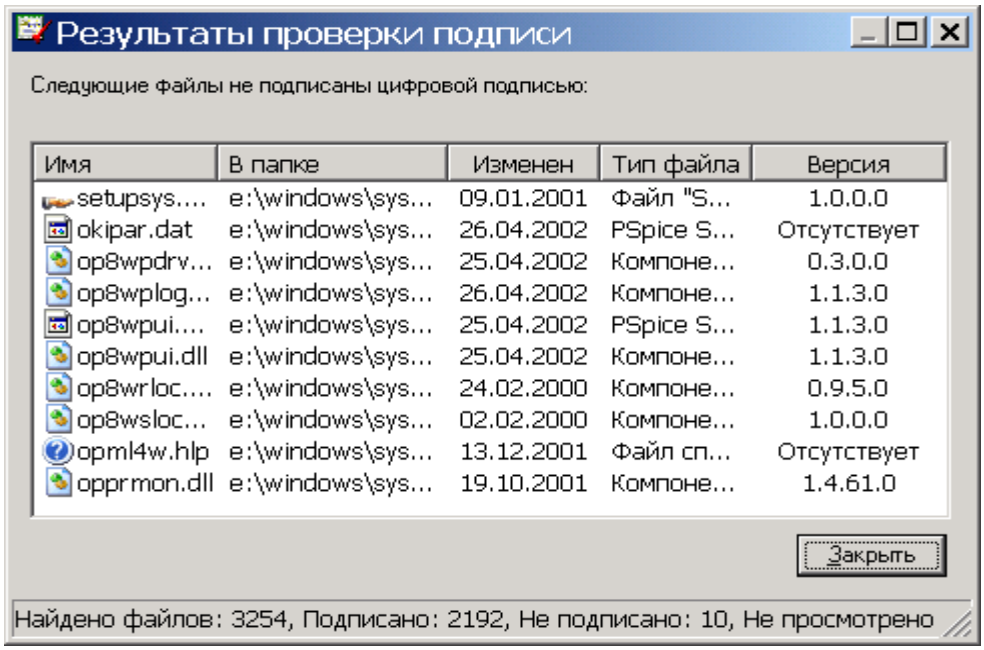


Рис.3 Вікно зі списком системних файлів без цифрового підпису фірми Microsoft.

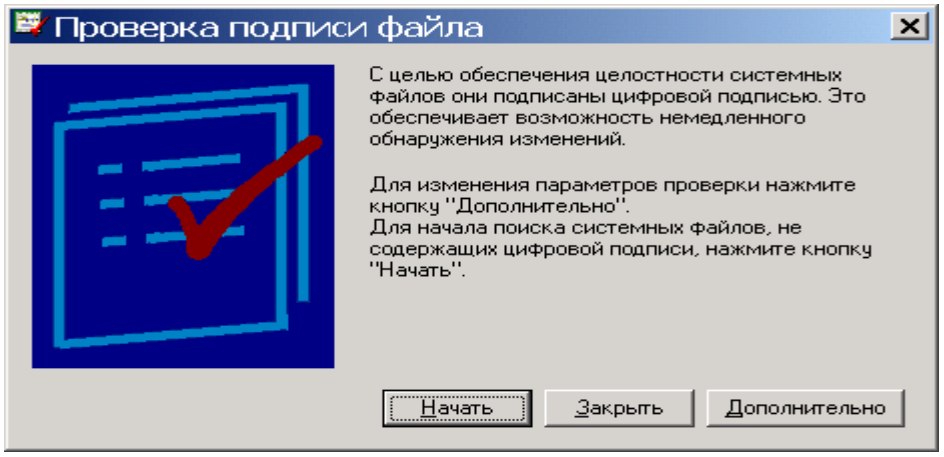


Рис. 4. Вікно перевірки підпису файлу.

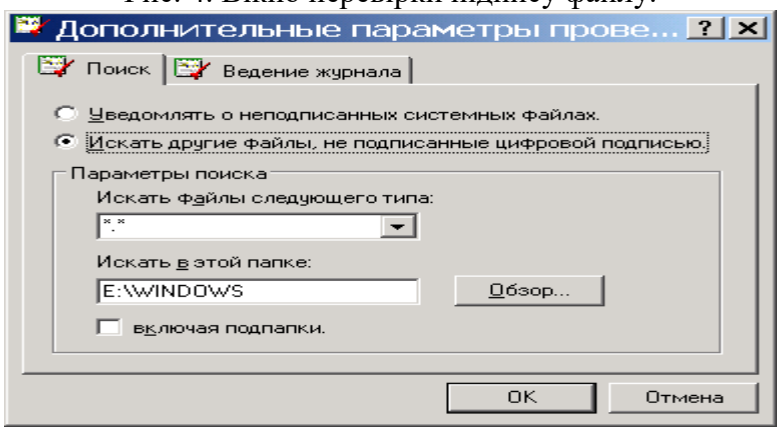


Рис. 5. Вибір параметрів пошуку.

2. Хід роботи

1. Проведіть шифрування файлів та каталогів за вказівкою викладача.

2. Проведіть дешифрування файлів та каталогів.
3. Проведіть шифрування файлів та каталогів за вказівкою викладача на віддаленому комп'ютері.
4. Проведіть дешифрування файлів та каталогів на віддаленому комп'ютері.
5. Проведіть перевірку використання на вашому комп'ютері програм та системних файлів і файлів за вказівкою викладача, які не мають цифрового підпису.

3. Контрольні питання

1. В якій файловій системі можливий процес шифрування?
2. Чому рекомендується разом із процесом шифрування використовувати атрибути для захисту файлової системи?
3. Вимоги до файлів, які підлягають шифруванню.
4. Порядок шифрування файлів та каталогів на комп'ютері.
5. Порядок дешифрування файлів та каталогів на комп'ютері.
6. Порядок шифрування файлів та каталогів на віддаленому комп'ютері.
7. Використання програми перевірки підпису файлу.
8. Для чого потрібна перевірка підпису файлу?

Лабораторна робота 17
Резервування систем інформації в Norton Ghost

Мета роботи – засвоїти принципи й елементи резервування систем інформації в Norton Ghost. Ознайомитись із рівнями резервування та відновлення системи.

ПЛАН

1. Теорія

1.1 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. 1) або головного меню Windows.

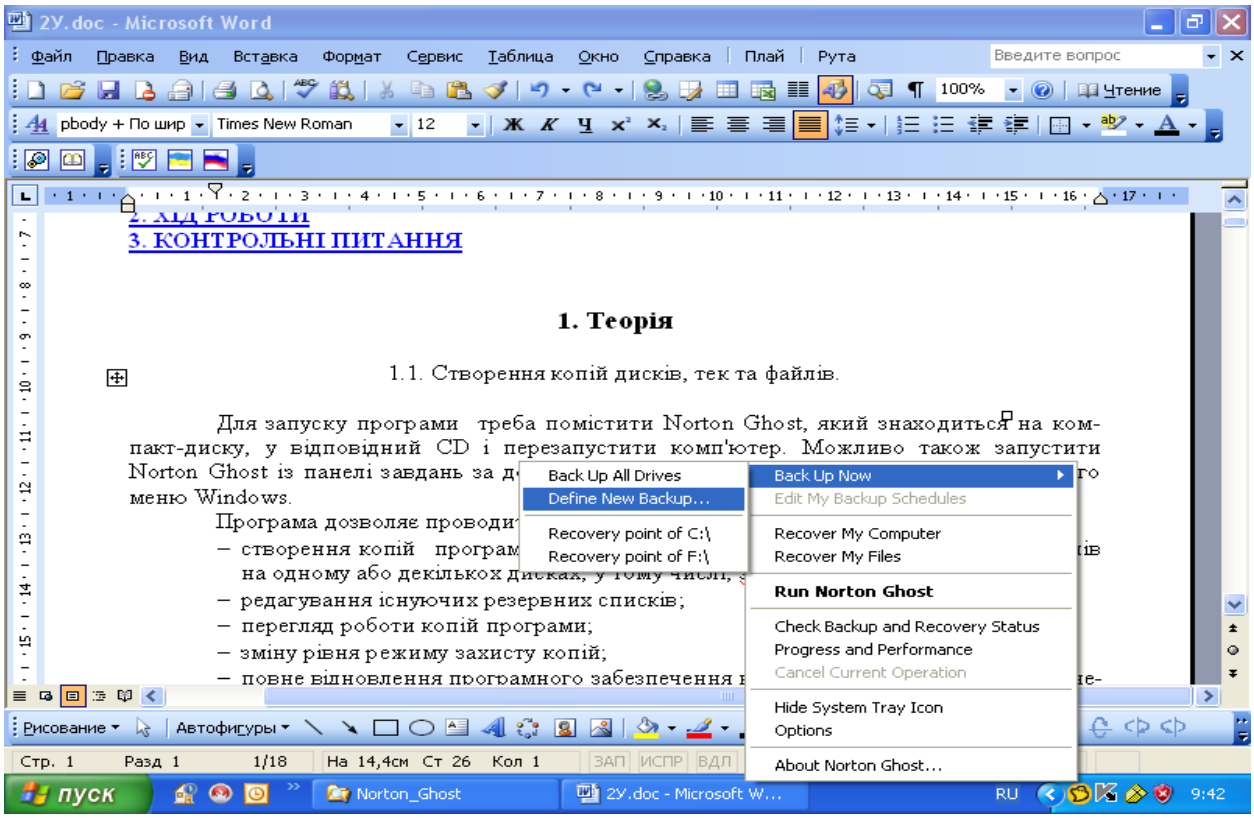


Рис. 1. Вікно виклику команд програми

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. 2-4) дозволяє мати доступ до:

Backup-резервна група: надає доступ до всіх ключових резервних особливостей програми, потрібного для конфігурування, планування й підтримки параметрів комп'ютера.

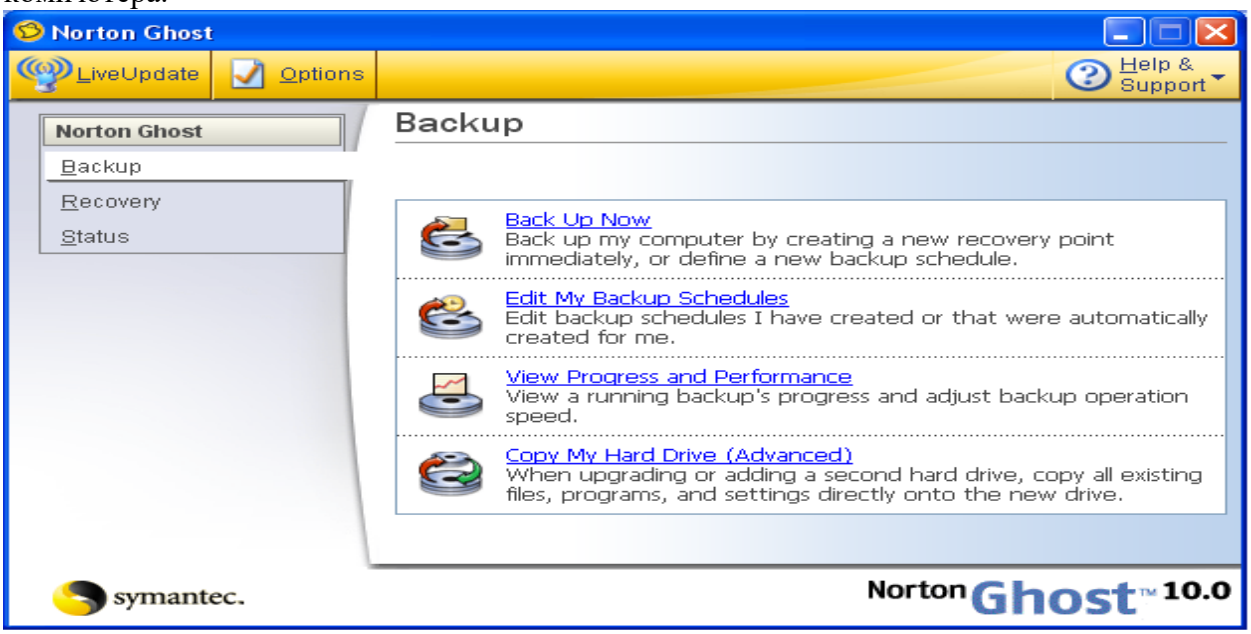


Рис. 2. Вікно резервної групи

Рис. 3. Вікно відновлення

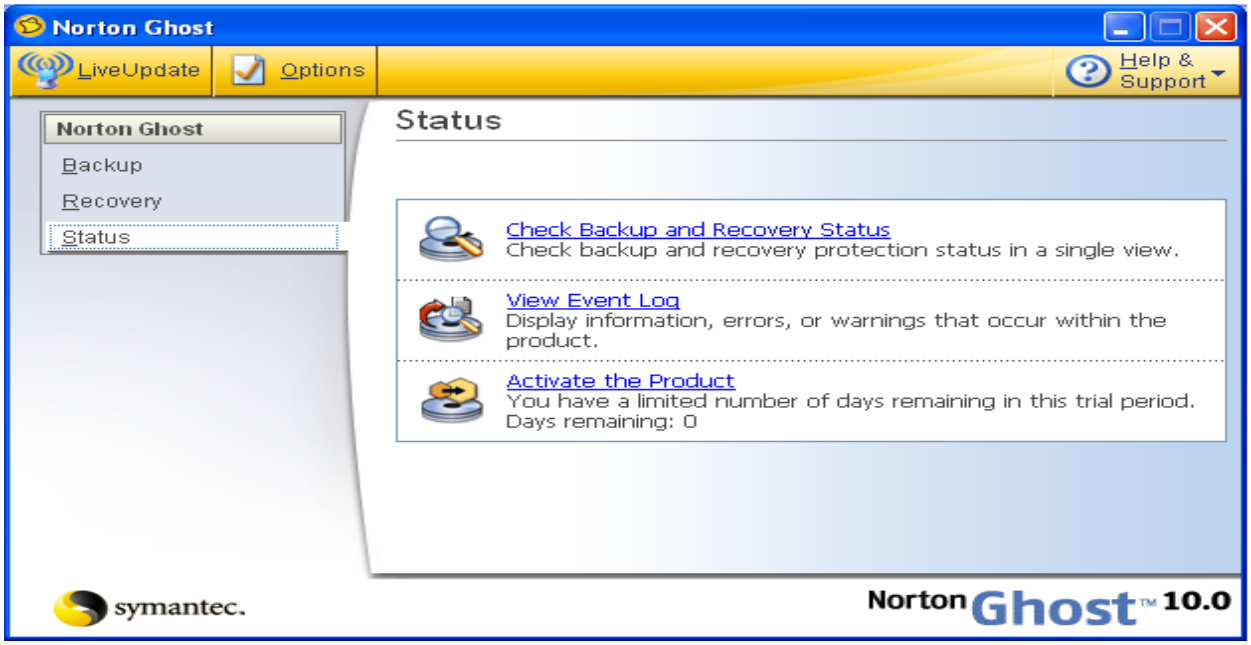


Рис. 4. Вікно статусу

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.

Група Backup надає доступ до наступних ключових резервних особливостей (табл. 1).

Таблиця 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. 2).

Таблиця 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. 3).

Таблиця 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) 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. 6. Адреса оновлення програми: http://www.symantec.com/partitionmagic.

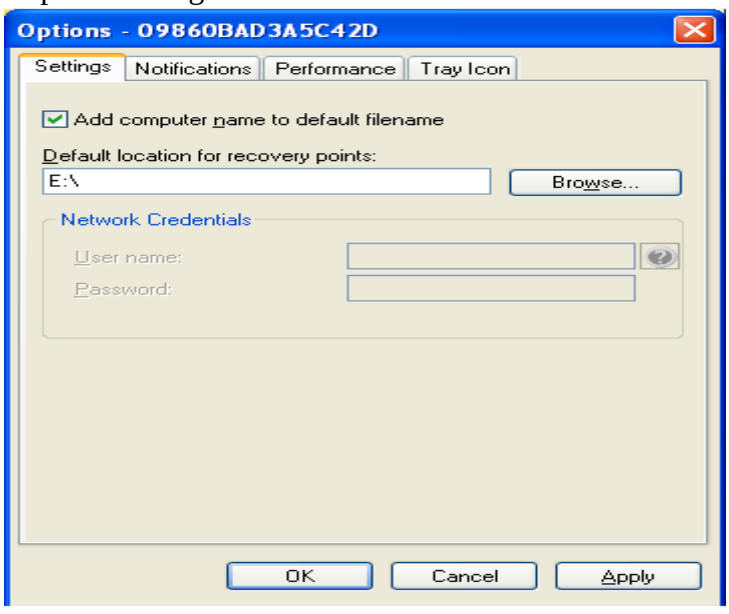


Рис. 5 Вікно налагодження

Таблиця 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.

1.2 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. 7). З'явиться вікно майстра (рис. 8).

3. Клацніть кнопку **Next** у вікні майстра. У наступному вікні (рис. 9) виберіть диск, копія якого буде створюватися та клацніть кнопку **Next**. У наступному вікні (рис. 10) відберіть **Recovery point set** (набір пункту оновлення, він рекомендований за умовчанням, але не активний, якщо запущений один із процесів створення копії), або Independent recovery point (Незалежний пункт оновлення) та клацніть кнопку **Next**. У наступному вікні майстра (рис. 11)

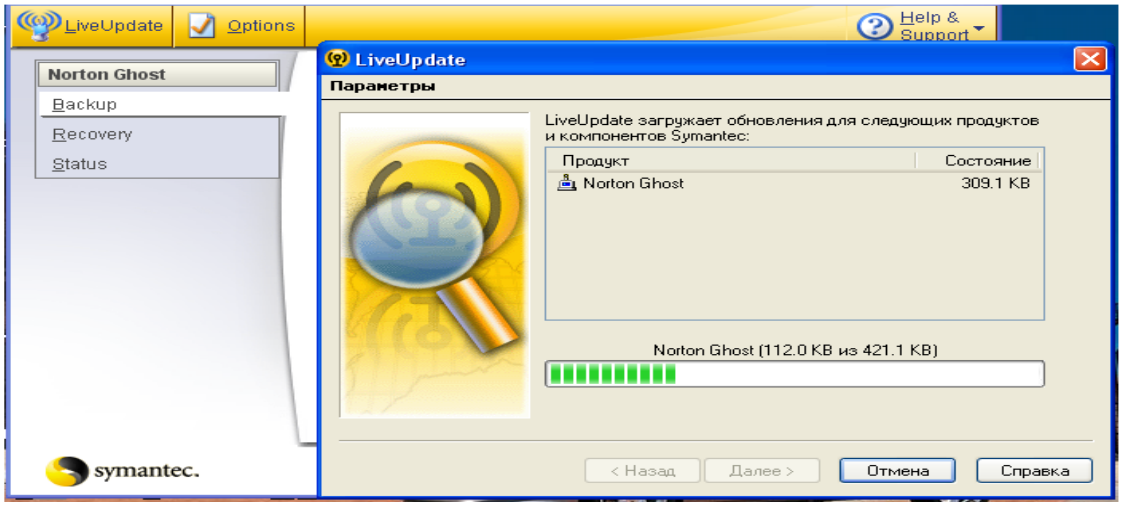


Рис. 6 Вікно оновлення програми

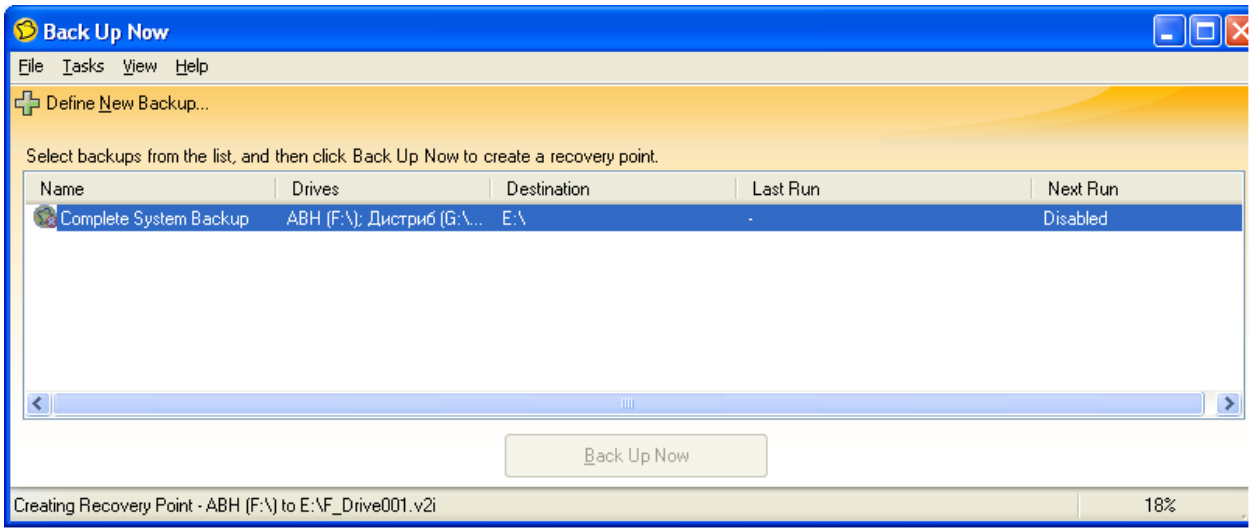


Рис. 7. Вікно Back Up Now

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. 12). Має, можливість кодування пароля, та розбиття копії диска на декілька файлів з указанням їх розмірів, а також ігнорування несправних секторів на дисках.

Рис. 8 Вікно майстра створення копії

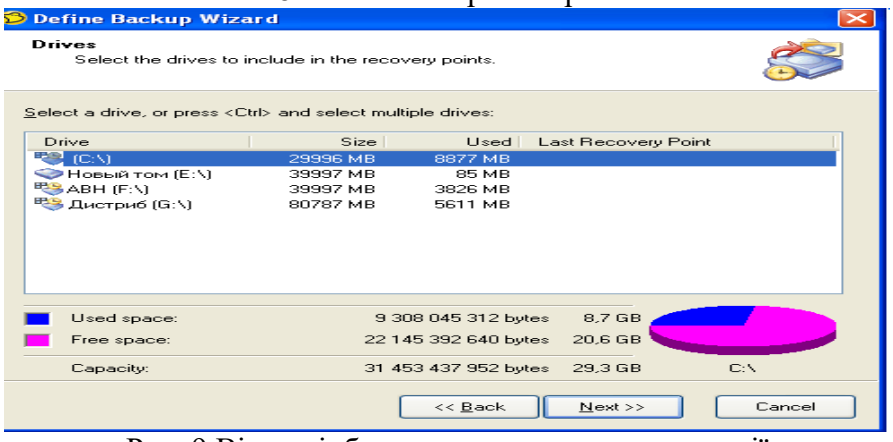


Рис. 9 Вікно відбору диска для створення копії

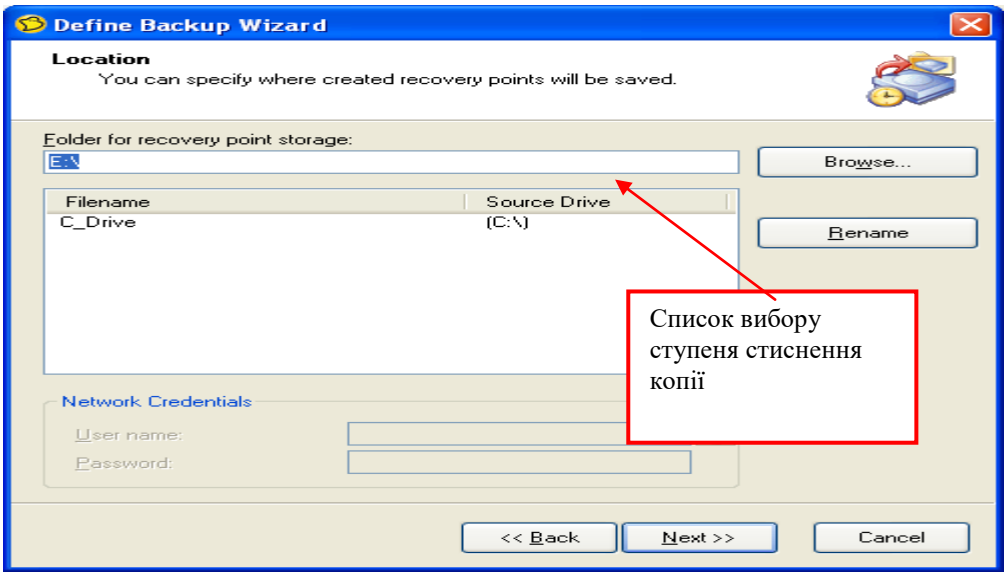


Рис. 10 Вікно відбору диска, каталогу або файлу для створення копії

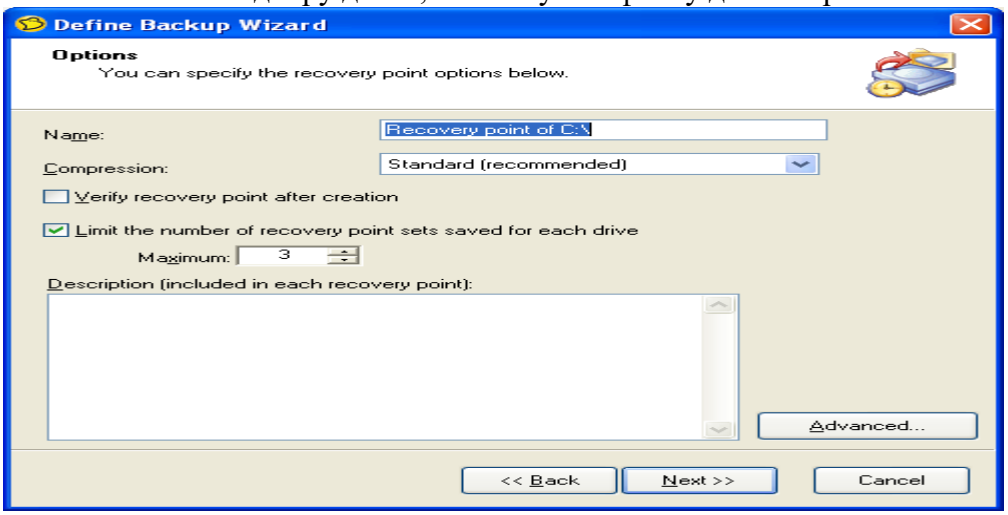


Рис. 11. Вікно відбору параметрів створення копії

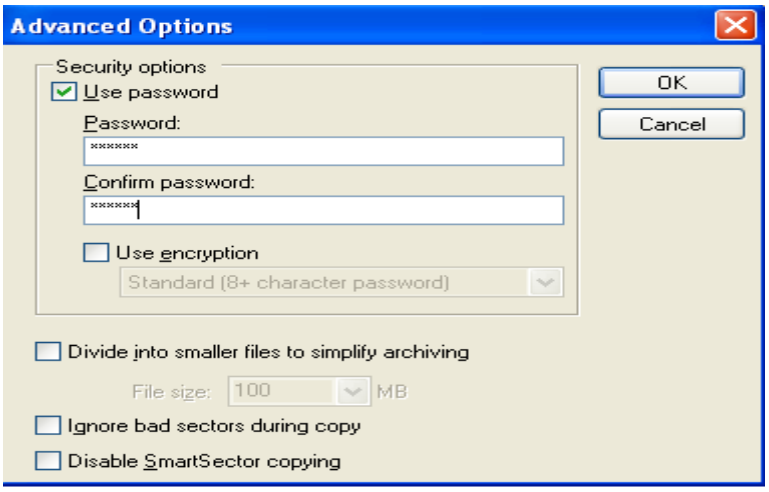


Рис. 12. Вікно встановлення пароля та відбору інших додаткових параметрів

Клацніть кнопку **Next**, після чого з'явиться нове діалогове вікно майстра (рис. 13) 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 (рис14), 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 (рис15).

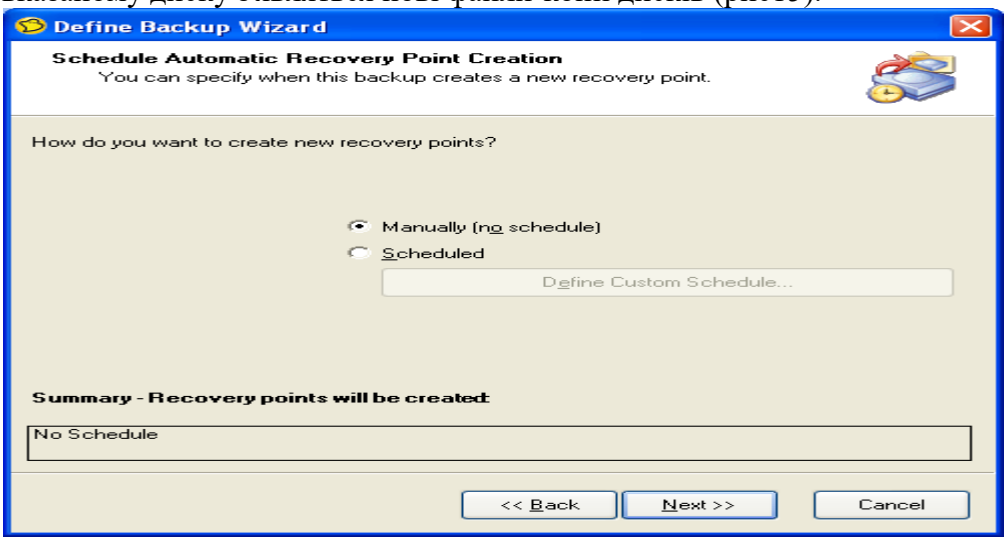


Рис. 13. Вікно відбору режиму копіювання

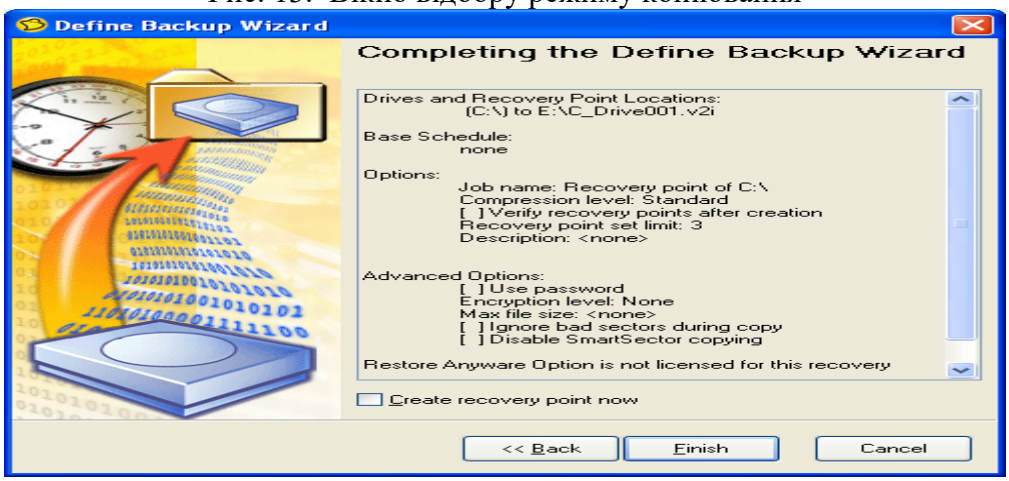


Рис. 14. Вікно перегляду параметрів копіювання

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.

1.3 Перевірка копій під час збереження

У групі **Recovery** введіть команду **Recover My Files**. З'явиться діалогове вікно (рис. 16) Виділіть копію, яку треба перевірити та натисніть кнопку **Browse Contents** після чого можна перевірити дерево каталогів та файли (рис. 17), вибравши, наприклад, із контекстного меню відповідні команди (рис. 18).

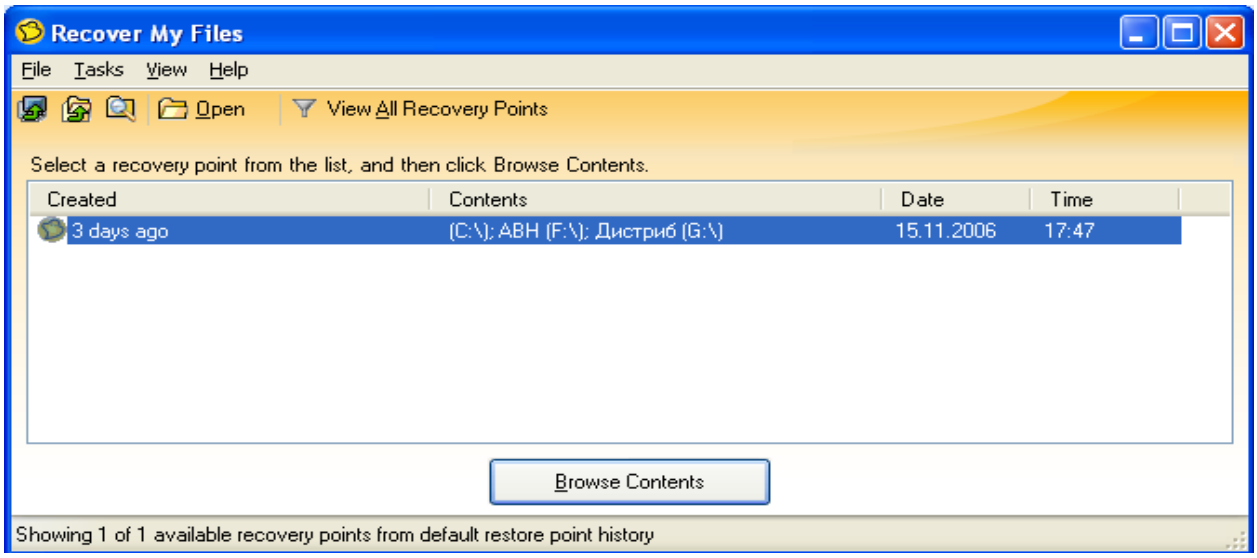


Рис. 16 Вікно перевірки копії диска

1.4 Зміна рівня захисту копії

У групі **Status** введіть команду **Check Backup and Recovery Status** з'явиться діалогове вікно з копіями (рис. 19), відберіть потрібну копію та введіть команду Add protection для визову майстра (рис. 20), за допомогою якого на окремих кроках відбираються параметри захисту.

1.5 Визначення властивостей копії

У групі **Recovery** подайте команду **Explore Recovery Points (Advanced)** у вікні, що з'явиться (рис. 21) відберіть потрібну копію та в контекстному меню введіть команду **Properties** з'явиться вікно властивостей копії (рис. 22).

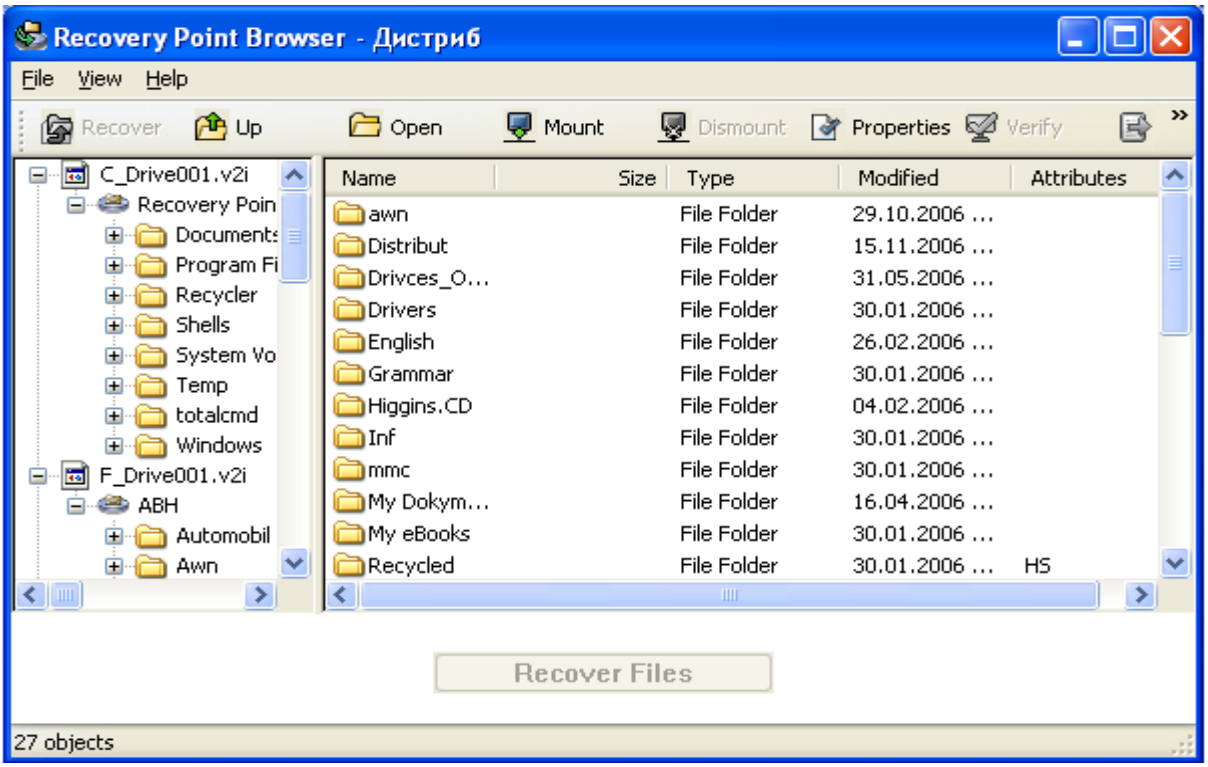


Рис. 17. Вікно дерева копії

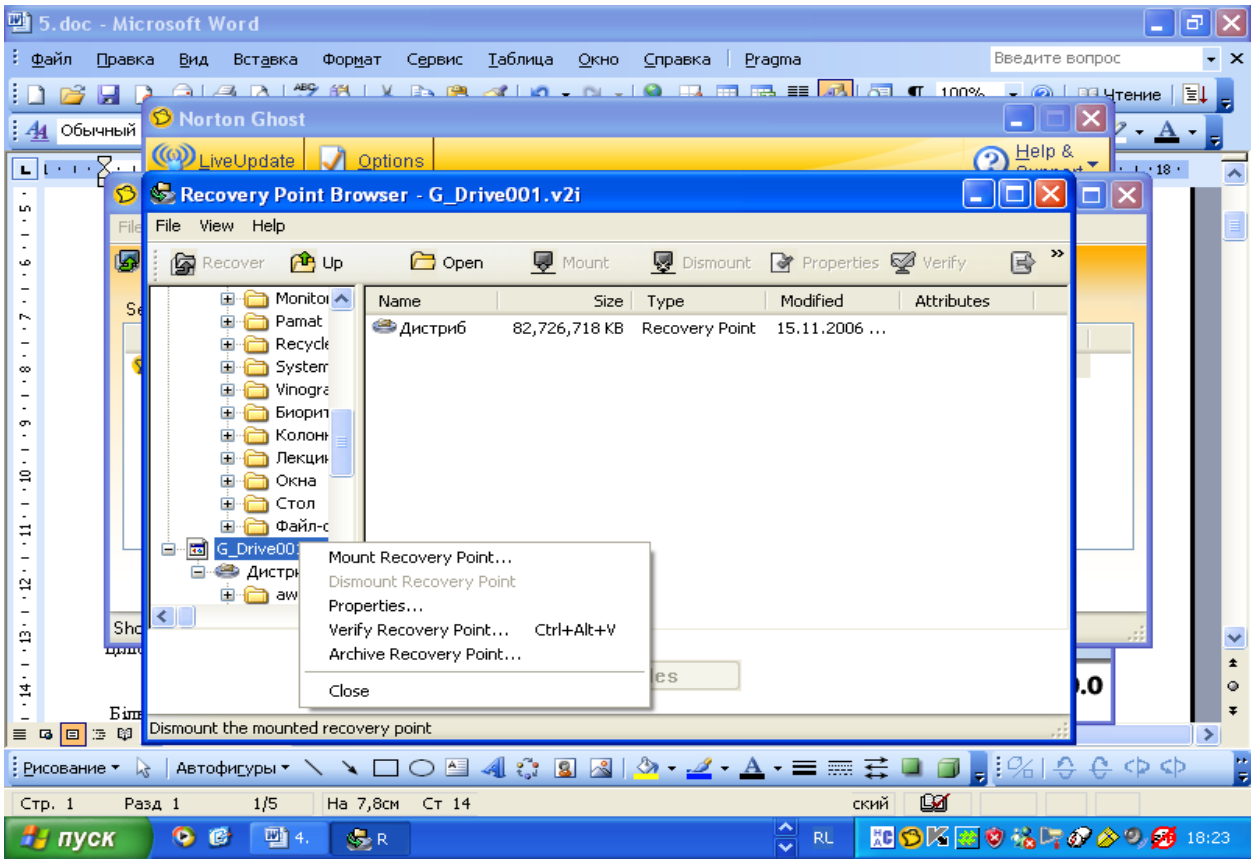


Рис. 18. Контекстне меню перевірки.

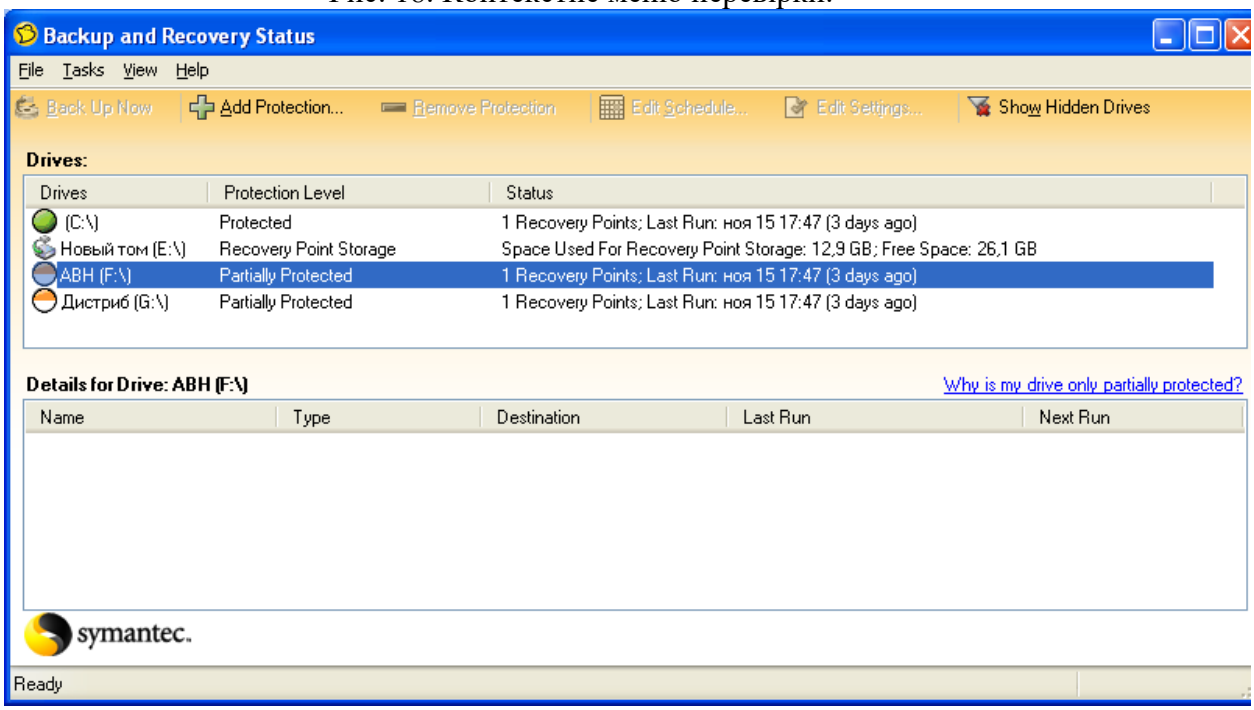


Рис. 19. Вікно відбору копії

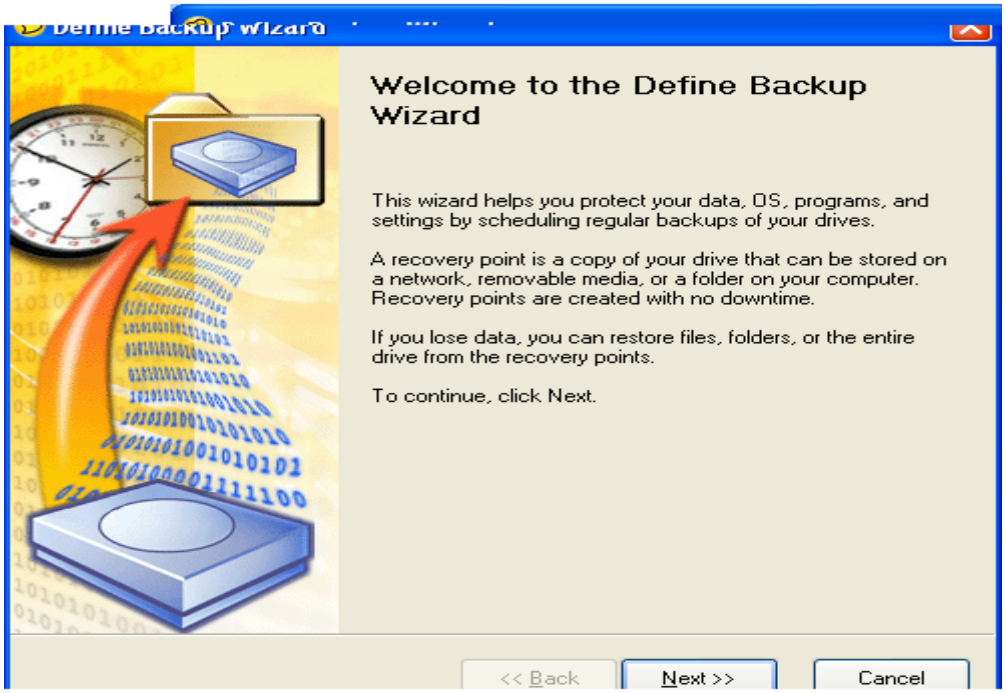


Рис. 20. Вікно майстра встановлення захисту

1.6 Видалення непотрібних копій

У групі **Recovery** ввести команду **Optimize Recovery Point Storage** з'явиться вікно (рис. 23),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. 25).

Оптимізація простору жорсткого диска, який використовується для зберігання пунктів оновлення комп'ютера

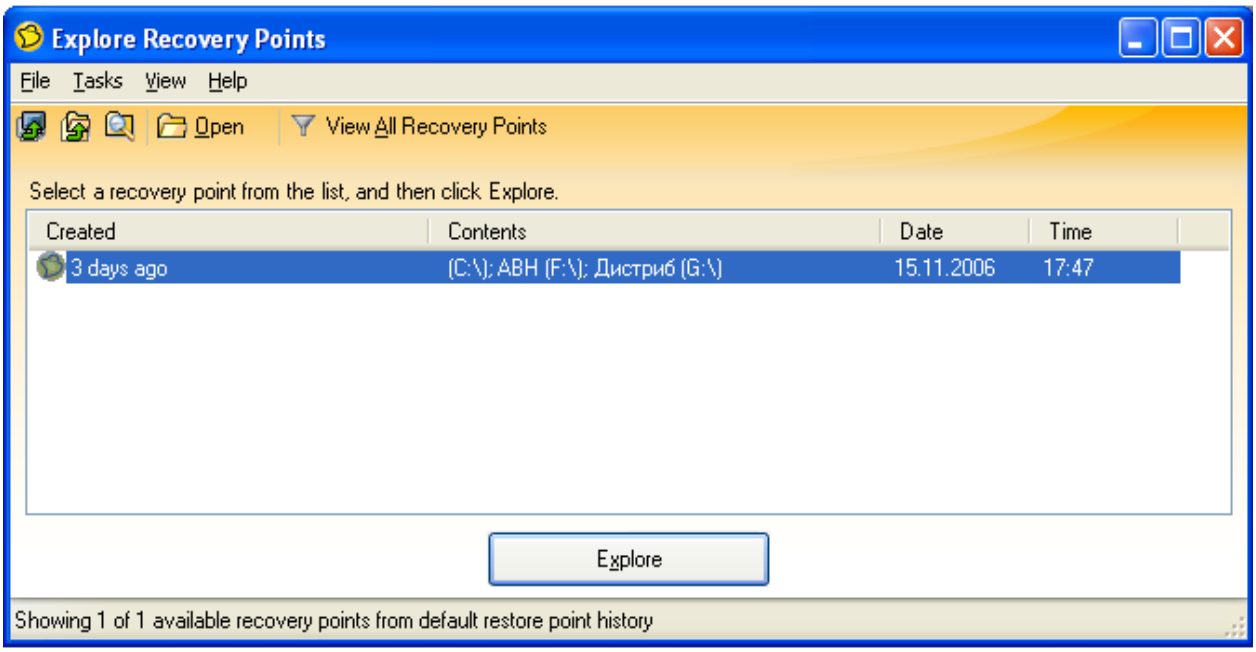


Рис. 21 Вікно відбору копії

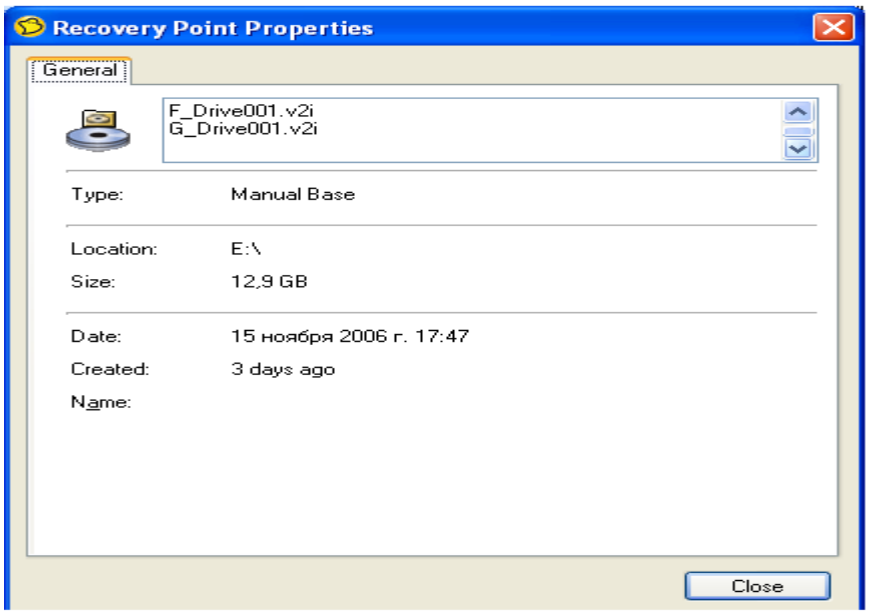


Рис. 22 Вікно властивостей копії

У групі **Recovery** введіть команду **Optimize Recovery Point Storage** з'явиться вікно (рис. 26) відберіть команду **Options** (правий нижній куток) та у вікні, що з'явиться (рис. 27) 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.

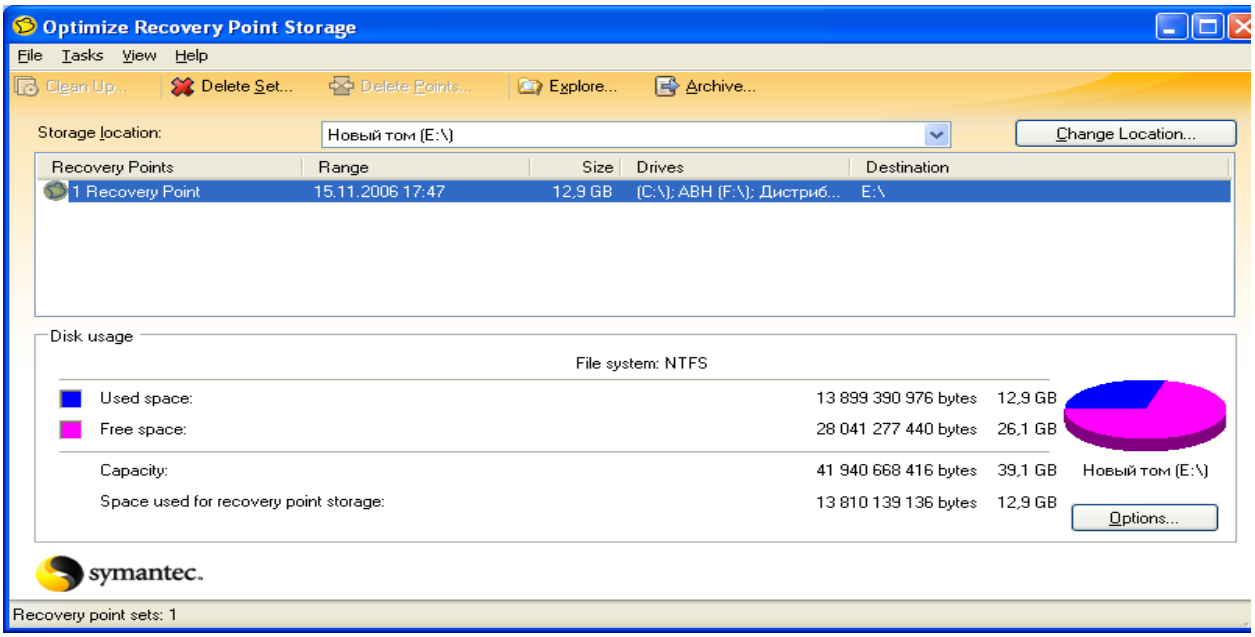


Рис. 23. Вікно відбору копії для видалення

Рис. 24. Вікно підтвердження видалення копії

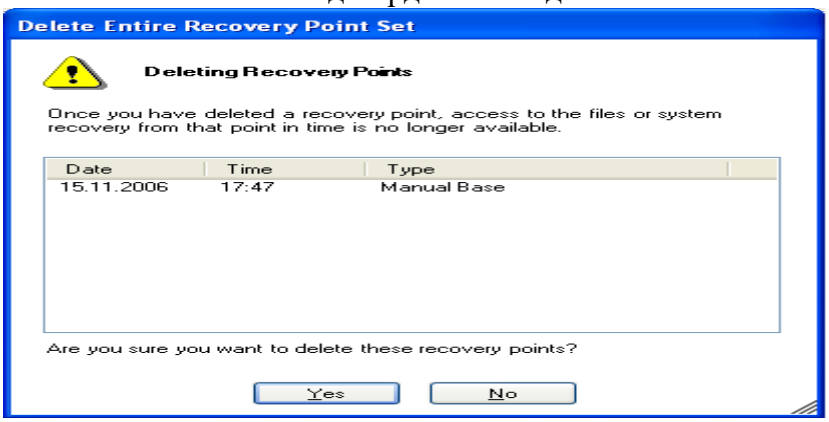


Рис. 25. Вікно остаточного видалення копії

1.7 Зміна місця розташування копій

У групі **Recovery** введіть команду **Optimize Recovery Point Storage** введіть команду **Change Location** у вікні, що з'явиться (рис. 28) необхідно вказати нове місце розташування копій (в тому числі змінні носії інформації та мережеві ресурси) і ввести команду **ОК**.

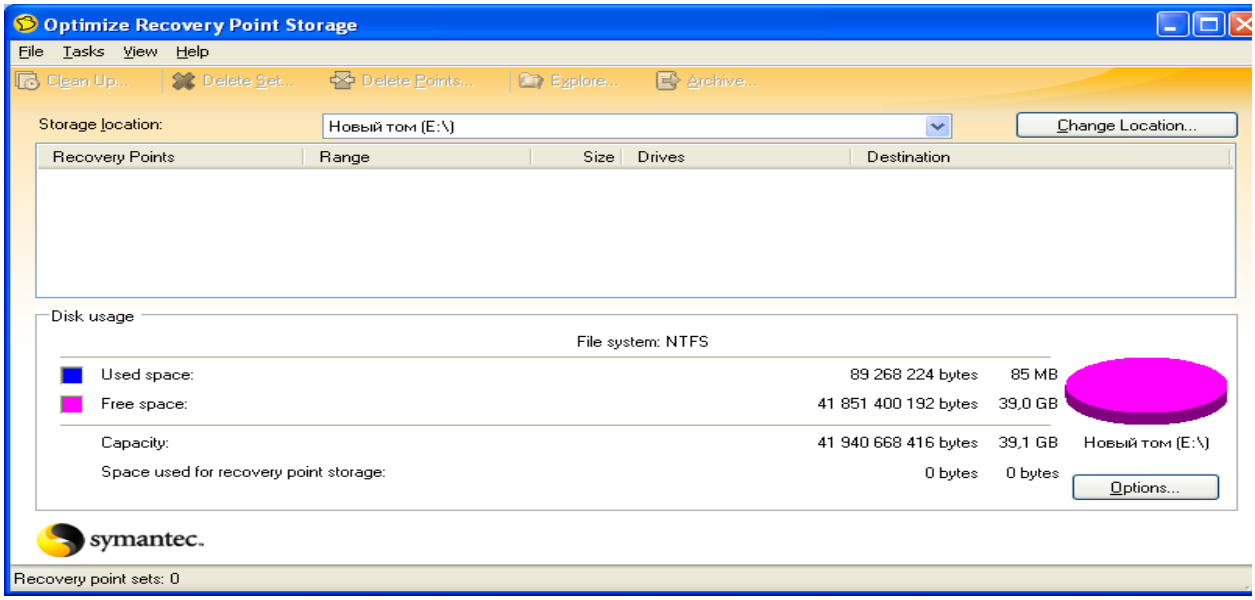


Рис. 26. Вікно Optimize Recovery Point Storage

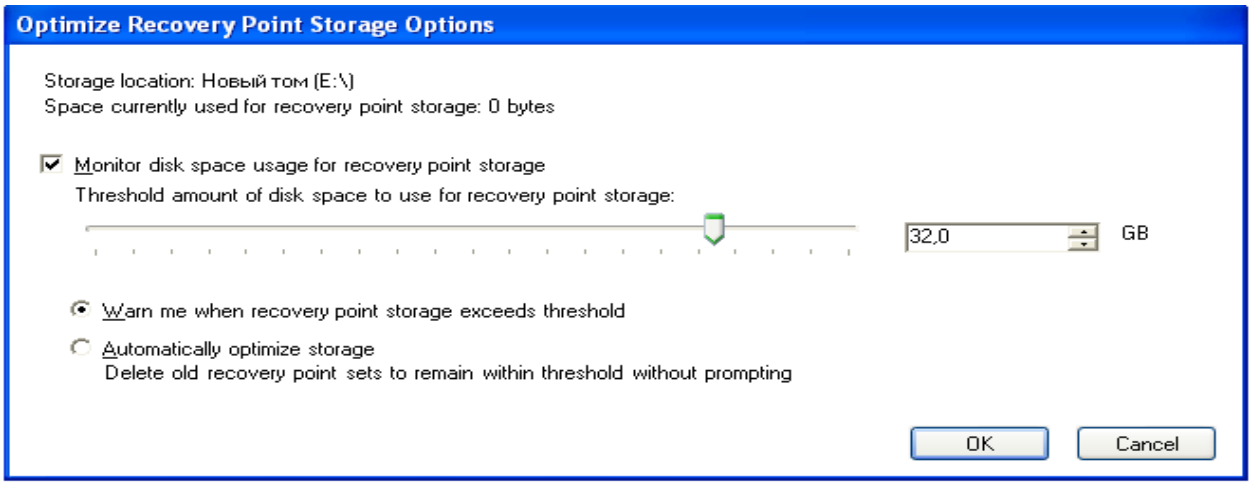


Рис. 27. Вікно відбору необхідних параметрів диска

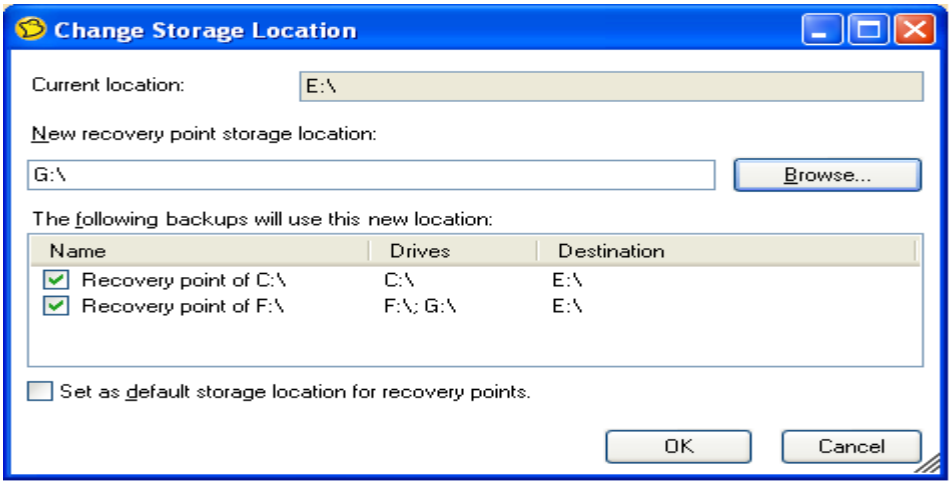


Рис. 28. Вікно відбору нового місця зберігання копій

1.8 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. 29), відберіть у ньому потрібні копії та подайте команду **Recover My Computer**, у діалоговому вікні, що з'явиться (рис. 30) виберіть режими відновлення **Express** (автоматичне відновлення) та **Custom** (вибіркове відновлення). При виборі останнього з'явиться вікно майстра відновлення (рис. 31), за допомогою якого за кілька етапів його роботи можна відібрати потрібні параметри відновлення.

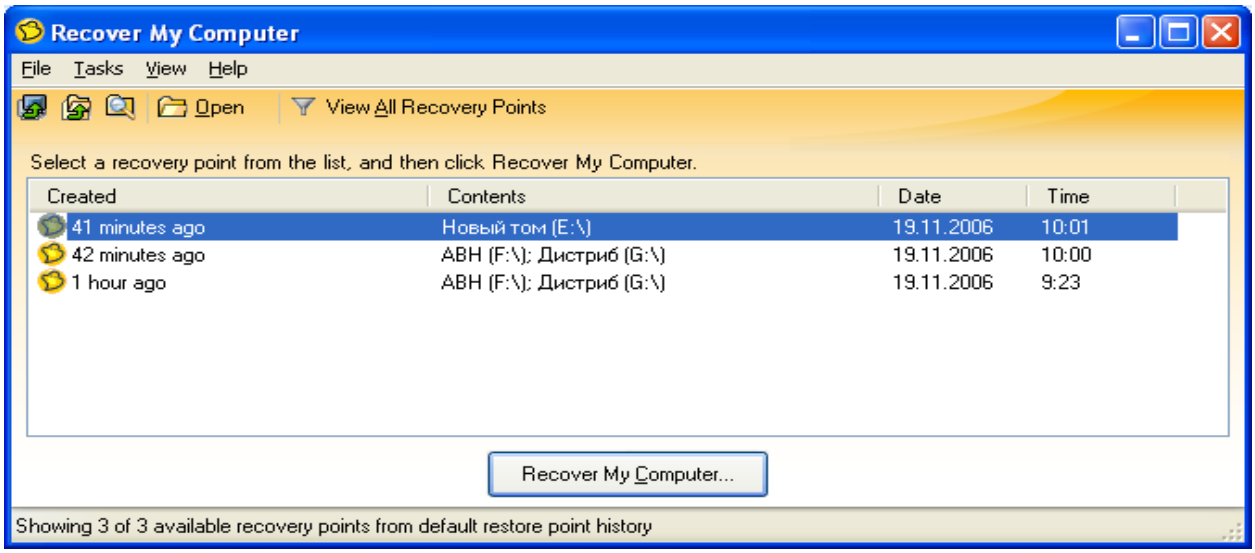


Рис. 29. Вікно відбору копій для відновлення комп'ютера

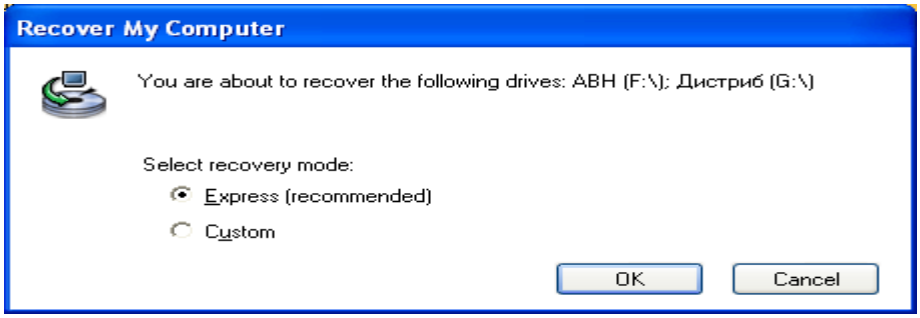


Рис. 30. Вікно відбору режимів відновлення комп'ютера

1.9 Відновлення копій файлів та каталогів

У групі **Recover** введіть команду **Recover My Files** з'явиться діалогове вікно (рис. 32) виберіть пункт оновлення зі списку та введіть команду **Browse Contents**.

У вікні, що з'явиться (рис. 33) відберіть файли або каталоги, які треба оновити та введіть команду **Recover Files** та в наступному вікні (рис. 34) 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.

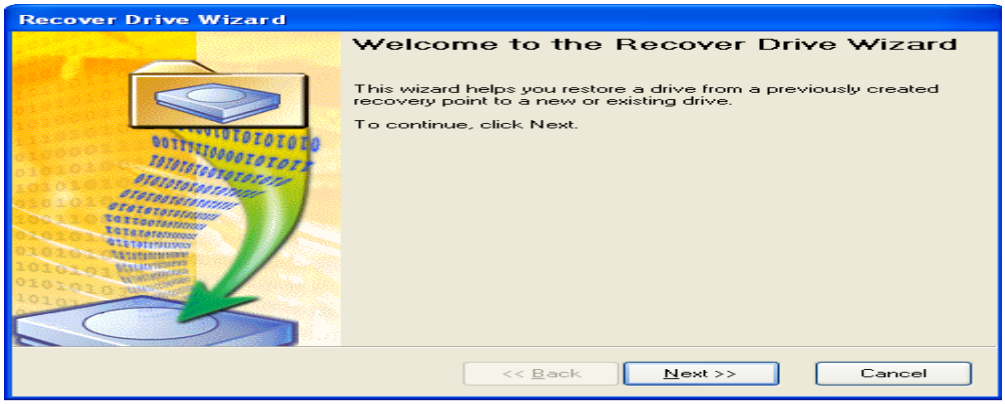


Рис. 31. Вікно майстра відновлення комп'ютера

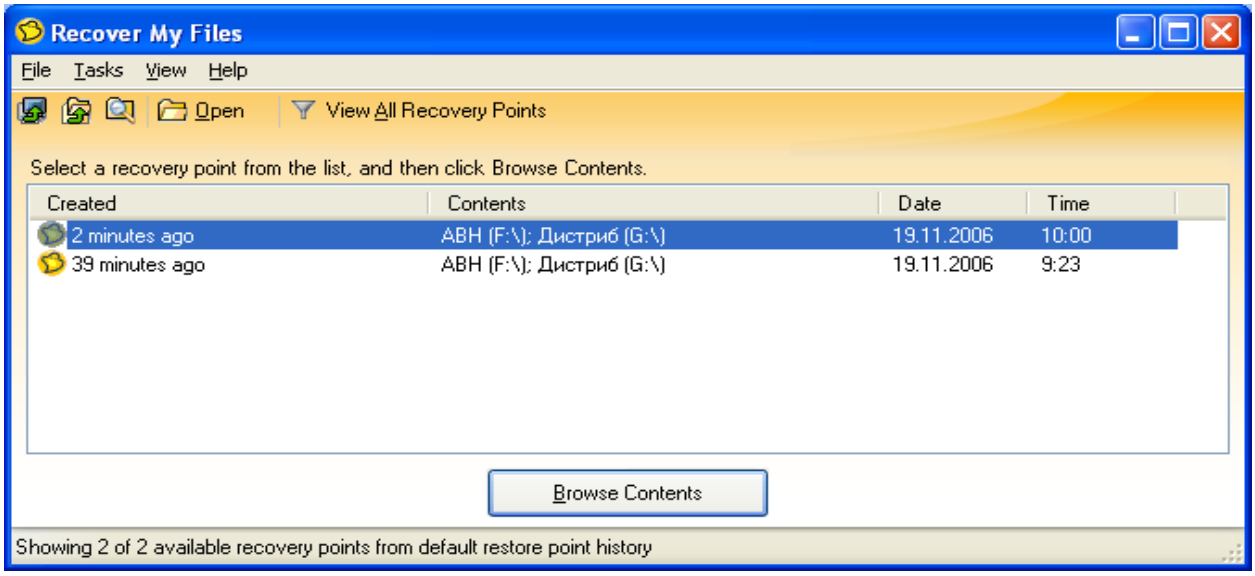


Рис. 32 Вікно Recover My Files

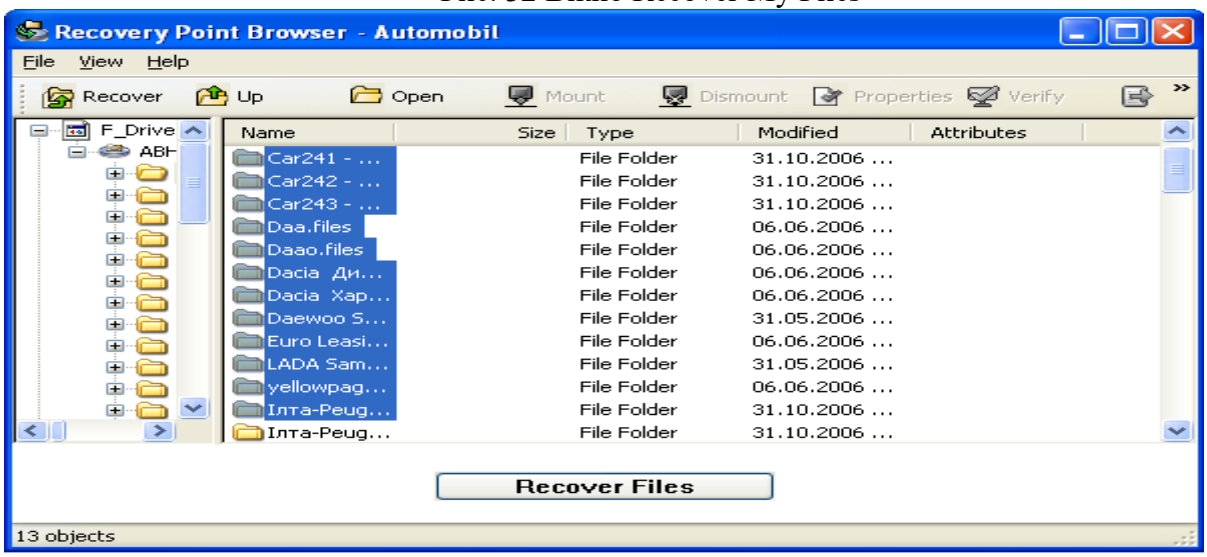


Рис. 33 Вікно відбору каталогів та файлів для оновлення

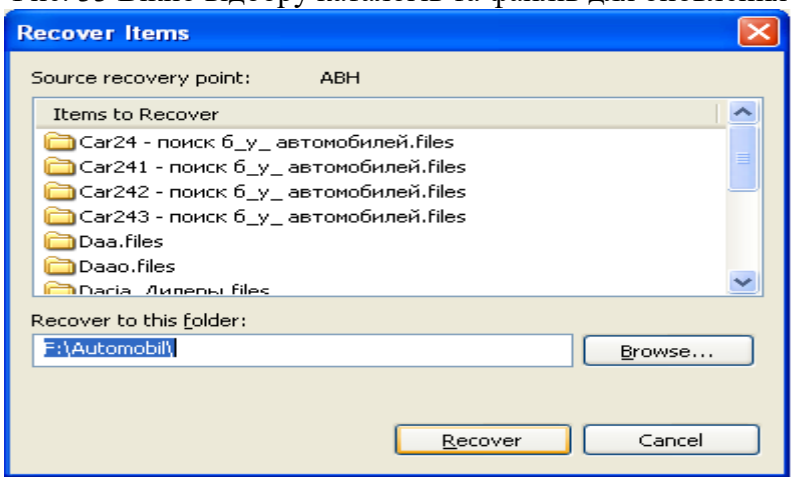


Рис. 34. Вікно указання місця відновлення файлів та каталогів

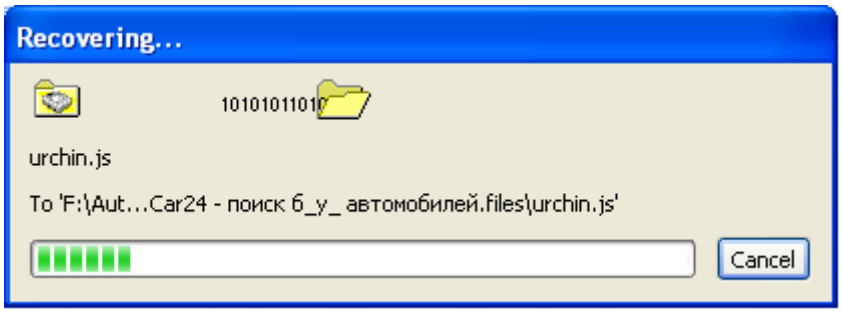


Рис. 35. Процес відновлення файлів та каталогів

2. Хід роботи

1. Створіть копію диска С.
2. Встановити пароль на копію.
3. Провести перевірку стану копії.
4. Проведіть видалення копії (до видалення показати копію викладачу).
5. Створіть копію каталога Мої документи.
6. Відновіть каталог.
7. Створіть копію файлу лабораторної роботи (скопіюйте файл перед створенням копії в каталог Мої документи.
8. Відновіть файл.

3.Контрольні питання

1. Призначення програми Norton Ghost.
2. Призначення команд групи Backup.
3. Призначення команд групи Recover.
4. Призначення команд групи Status.
5. Діалогове вікно Options.
6. Послідовність створення копії диска.
7. Послідовність створення копії каталоги.
8. Послідовність створення копії файлу.
9. Як провести перевірку копій під час збереження?
10. Як провести зміну рівня захисту копії?
11. Як переглянути властивості копії?
12. Як проводиться видалення непотрібних копій?
13. Як проводиться оптимізація простору жорсткого диска, який використовується для зберігання пунктів оновлення комп'ютера?
14. Як проводиться зміна місця розташування копій?
15. Як проводиться відновлення комп'ютера?
16. Як проводиться відновлення копій файлів та каталогів

Лабораторна робота 18
Криптографія з відкритим ключем.

Мета роботи: Навчитися проводити пошук ключів та розробляти алгоритми і програму для шифрування/дешифрування даних з відкритим ключем.

1. Теорія

Традиційні методи шифрування мають ряд проблем, які вирішуються шляхом застосування криптографічних методів шифрування з відкритим ключем.

Перша проблема полягає в генерації й розподілі ключів, які застосовуються при традиційнім шифруванні.

Друга проблема, не пов'язана з першою, (це проблема цифрових підписів). Іншими словами, чи можна розробити метод, за допомогою якого обидві сторони могли б переконатися в тому, що цифрове повідомлення було відправлено даною конкретною особою?

Алгоритми шифрування з відкритим ключем залежать від двох ключів: одного ключа для зашифрування й іншого ключа, пов'язаного з першим, для дешифрування (рис. 1). З погляду обчислень нереально визначити ключ дешифрування, знаючи тільки використовуваний криптографічний алгоритм і ключ зашифрування.

Криптографічні системи з відкритим ключем залежать від деякої оберненої математичної функції зі спеціальними властивостями. Складність обчислення такого роду функцій може залежати не лінійно від числа бітів у ключі, і рости значно швидше в залежності від довжини ключа. Тому довжина ключа повинна бути досить великою. Однак чим довше ключі, тим більше часу потрібно для виконання процесів зашифрування/дешифрування. Тому алгоритми криптографії з відкритим ключем у цей час в основному застосовуються в керуванні ключами й цифровому підписі.

Складності обчислень в основному складаються зі складностей практичної реалізації деяких операцій з теорії чисел. Поняття й методи теорії чисел є абстрактними, і їх часто досить важко зрозуміти інтуїтивно без використання прикладів. Тому й пропонується дана лабораторна робота, після виконання якої надалі більш ефективно можна буде розуміти й освоювати розглянуті конкретні найпоширеніші криптографічні методи з відкритим ключем.

2. Хід роботи

2.1 Завдання. Пошук найбільшого загального дільника (алгоритм Евкліда)

2.1.1 Теорія, основні поняття й визначення

1. Нагадаємо, що c, відмінне від нуля, ділить a, якщо $a = m \times c$ для деякого m, де c, a і

m є цілими числами.

Таким чином, c ділить a, якщо ділення виконується без залишку. Це пишеться так: a/c. C називають дільником a.

2. Ціле число p>1 називається простим числом, якщо його дільниками є тільки числа ± 1 і ± p.

3. Запис gcd (a, b) буде позначати найбільший загальний дільник чисел (НЗД) a і b.

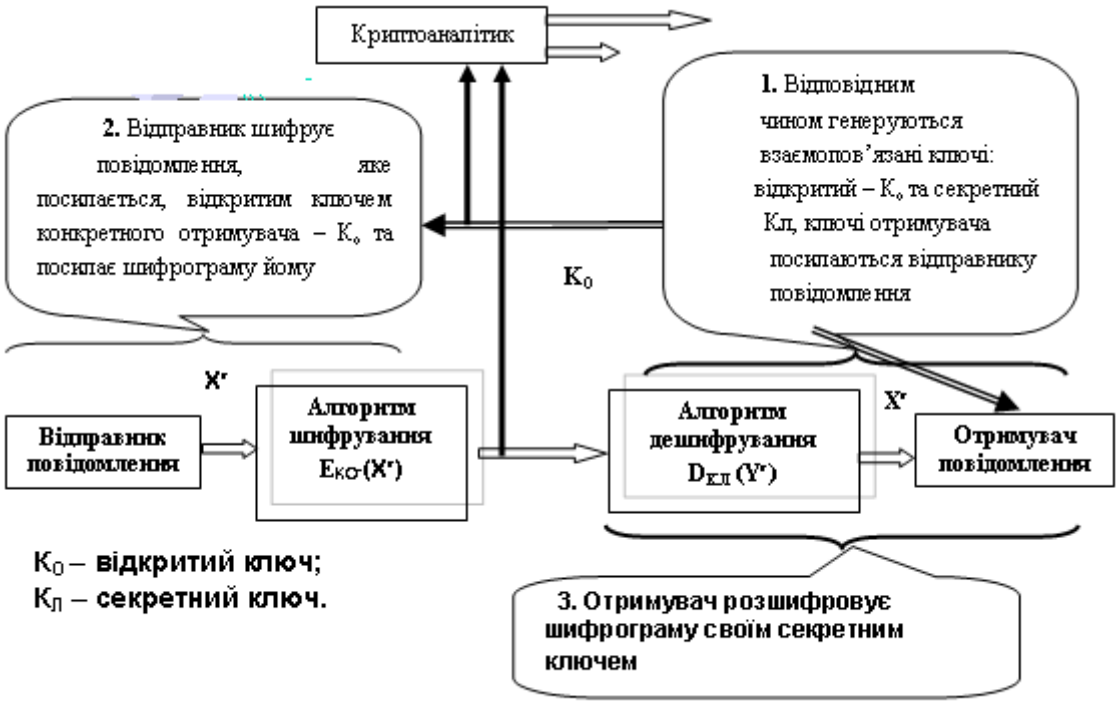


Рис.1 Криптографічна система з відкритим ключем

4. Позитивне ціле число c є найбільшим загальним дільником чисел a і b, якщо:

- c є дільником a і b;
- будь-який дільник a і b є дільником c.

gcd (a, b) = max [k таких, що k|a і k|b].

Приклад: gcd (60, 24) = gcd (60, 24) = 12.

5. Будь-яке ціле число a > 1 може бути розкладене на множники і єдиним способом презентовано у вигляді

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t},$$

де $p_1 < p_2 < \ldots < pt$ є простими числами й де кожна $\alpha_i > 0$.

Приклад: 3600 = 24 × 32 × 52.

6. Цілі числа a і b є взаємно простими, якщо вони не мають загальних простих дільників, тобто якщо їх єдиним загальним дільником є 1. Інакше кажучи, числа a і b є взаємно простими, якщо gcd (a, b) = 1.

7. Якщо a є цілим, а z – позитивним цілим, то a mod z визначається як залишок від розподілу a на z. Тоді для будь-якого цілого числа a можна написати:

a = (a/z((z + (a mod z),

де $\lfloor a/z \rfloor$ означає найбільше ціле число, що не перевищує (a/z).

Приклад: 11 mod 7 = 4.

11 = (11/7((7 + 4 = 1 (7 + 4))).

8. Два цілі числа a і b є порівнянними за модулем n, якщо (a mod n) = (b mod n). Це записується так: $a \equiv b \bmod n$.

Приклад: $73 \equiv 4 \bmod 23$, тому що залишки від розподілу чисел 73 і 4 на 23 збігаються.

2.1.2 Алгоритм Евкліда (знаходження найбільшого загального дільника)

Алгоритм Евкліда – знаходження найбільшого загального дільника ґрунтується на наступній теоремі.

Для будь-якого ненегативного числа X і будь-якого позитивного числа Y справедливо наступне: gcd (X, Y) = gcd (Y, X mod Y), (1)
де X>Y>0.

Щоб визначити найбільший загальний дільник, наведену вище рівність (1) необхідно використовувати багаторазово (до одержання значення Y = 0). Нижче приводиться розкритий запис:

gcd (X, Y) = gcd (Y, X mod Y) = gcd (Y, $X - \lfloor X/Y \rfloor \times Y$)).

Приклад: gcd (18, 12) = gcd (12, 18 mod 12) = gcd (12, $18 - 1 \times 12$) = gcd (12, 6).

gcd (12, 6) = gcd (6, 12 mod 6) = gcd (6, $12 - 2 \times 6$) = gcd (6, 0).

Відповідь: gcd (18, 12) = 6.

Алгоритм Евкліда приводиться на рис. 2.

Розглянемо конкретний приклад і розв'яжемо поставлене завдання згідно з наведеним алгоритмом обчислення EUCLID (d, f) [1]. В алгоритмі d> f> 0 і досить розглянути тільки позитивні цілі числа, тому що gcd (a, b) = gcd ($|a|$, $|b|$).

Приклад. Знайти EUCLID (d, f) для d = 1970, f = 1066.

EUCLID (1970, 1066) = ?

gcd (X, Y) = gcd (Y, X mod Y)

X ←d = 1970, Y ←f = 1066,

Y ≠ 0.

R = X mod Y = 1970 mod 1066 = 904 (залишок від ділення 1970 на 904).

X = Y = 1066.

Y = R = 904.

Y ≠ 0.

R = X mod Y = 1066 mod 904 = 162. (залишок від ділення 1066 на 904).

X = Y = 904.

Y = R = 162.

Y ≠ 0.

R = X mod Y = 904 mod 162 = 94. (залишок від ділення 904 на 162).

X = Y = 162.

Y = R = 94.

Y ≠ 0.

R = X mod Y = 162 mod 94 = 68. (залишок від ділення 162 на 94).

X = Y = 94.

Y = R = 68.

Y ≠ 0.

R = X mod Y = 94 mod 68 = 26. (залишок від ділення 94 на 68).

X = Y = 68.
Y = R = 26.
Y ≠ 0.
R = X mod Y = 68 mod 26 = 16. (залишок від ділення 68 на 26).
X = Y = 26.
Y = R = 16.
Y ≠ 0.
R = X mod Y = 26 mod 16 = 10. (залишок від ділення 26 на 16).
X = Y = 16.
Y = R = 10.

Y ≠ 0.
R = X mod Y = 16 mod 10 = 6. (залишок від ділення 16 на 10).
X = Y = 10.
Y = R = 6.

Y ≠ 0.
R = X mod Y = 10 mod 6 = 4. (залишок від ділення 10 на 6).
X = Y = 6.
Y = R = 4.

Y ≠ 0.
R = X mod Y = 6 mod 4 = 2. (залишок від ділення 6 на 4).
X = Y = 4.
Y = R = 2.

Y ≠ 0.
R = X mod Y = 4 mod 2 = 0. (залишок від ділення 4 на 2).
X = Y = 2.
Y = R = 0.
Відповідь: gcd (1970, 1066) = 2.

Рис. 2 Алгоритм знаходження найбільшого загального дільника

Виконати завдання за схемою наведеною вище. При цьому вибрати два числа d і f, таких, що d> f і d>200, а f>100. Визначити за заданим алгоритмом Евкліда вручну, з використанням калькулятора (або склавши програму на будь-якій мові програмування), найбільший загальний дільник чисел d і f – EUCLID (d, f).

2.2 Подільність

Нехай x – дійсне число. Через $\lfloor x \rfloor$ будемо позначати найбільше ціле число, яке не перевищує x.

Теорема. Нехай a та b – цілі числа, при чому b > 0. Тоді існують такі числа q та r, які визначаються однозначно, що $a = b * q + r$, при чому $0 \le r < q$. Число q називається неповною часткою, а r – залишком від ділення a на b.

Доведення. Очевидно, що $0 < \frac{a}{b} - \left\lfloor \frac{a}{b} \right\rfloor < 1$ або $0 < a - b\left\lfloor \frac{a}{b} \right\rfloor < b$. Якщо ввести позначення $q = \left\lfloor \frac{a}{b} \right\rfloor$ та $r = a - b\left\lfloor \frac{a}{b} \right\rfloor$, то це і доводить теорему.

Означення. Нехай a та b – цілі числа. Будемо говорити що a ділиться на b, або b ділить a, якщо існує таке ціле число *c*, що *a* = *bc*. Це будемо позначати так: b | a (b ділить a) або a ⋮ b (a ділиться на b).

Приклад. -4 | 20 або 20 ⋮ -4, тому що 20 = (-4) * 5.

Властивості подільності. Нехай a, b та c – цілі числа. Тоді

1. a | a.
2. Якщо a | b та b | a, то a = ±b.
3. Якщо a | b та b | c, то a | c.
4. Якщо a | b та a | c, то a | (bx + cy) для всіх x, y ∈ Z.

2.3 Алгоритм Евкліда

Обчислення найбільшого спільного дільника (НСД) двох чисел a та b базується на наступному факті: якщо a та b – додатні цілі числа, a > b, тоді НСД(a, b) = НСД(b, a mod b). У випадку, коли a < b маємо: НСД(a, b) = НСД(b, a mod b) = НСД(b, a).

ВХІД: два невід'ємних числа a та b.
ВИХІД: НСД(a, b)

```
int nsd(int a, int b)
{
  int temp;
  while (b != 0)
  {
    temp = a % b;
    a = b;
    b = temp;
  }
  return a;
}
```

Приклад. Обчислення НСД(4864, 3458).

4864 = 1* 3458 + 1406
3458 = 2 * 1406 + 646
1406 = 2 * 646 + 76
114 = 1 * 76 + 38
76 = 2 * 38 + 0

Алгоритм Евкліда можна розширити для знаходження таких цілих чисел x та y, що a * x + b * y = d.

ВХІД: два невід'ємних числа a та b, a і b.
ВИХІД: d = НСД(a, b) та такі цілі числа x та y, що a * x + b * y = d.

```
void nsdrozsh(int a, int b, int *x, int *y, int *k)
{
  int p, q, r, s, m, n;
  m = a; n = b; p = 1; q = 0; r = 0; s = 1;
  while (m!=0 && n!=0)
  {
    if (m >= n)
    {  m = m - n; p = p - r; q = q - s;  }
```

```
  else
  {  n = n - m; r = r - p; s = s - q;  }
 }
 if (m == 0)
 {  *k = n; *x = r; *y = s;  }
 else
 {  *k = m; *x = p; *y = q;  }
}
```

Приклад. Розширений алгоритм Евкліда. Обчислення НСД(4864, 3458).

Q	r	x	y	a	b	x_2	x_1	y_2	y_1
				4864	3458	1	0	0	1
1	1406	1	1	3458	1406	0	1	1	1
2	646	2	3	1406	646	1	2	1	3
2	114	5	7	646	114	2	5	3	7
5	76	27	38	114	76	5	27	7	38
1	38	32	45	76	38	27	32	38	45
2	0	91	128	38	0	32	91	45	128

Результат: НСД(4864, 3458) = 38, при цьому 4864 * 32 + 3458 * (-45) = 38.

Для обчислення найменшого спільного кратного (НСК) можна використати формулу:

$$a * b = НСД(a, b) * НСК(a, b).$$

Приклад. Знайти НСК(12, 18). Скориставшись наведеним алгоритмом, знайдемо, що НСД(12, 18) = 6. Отже 12 * 18 = 6 * НСК(12, 18). Звідки НСК(12, 18) = (12 * 18) / 6 = 36.

3. Контрольні питання

1. Яка послідовність пошуку загального дільника?
2. Яка послідовність пошуку найбільшого загального дільника?
3. Як розробляється програма пошуку найбільшого загального дільника?
4. Як розробляється програма шифрування та дешифрування?

4. Додаток (Приклад програми шифрування та дешифрування)

4.1 Реалізація зсуву букв у програмі

Це можна зробити, представивши кожну букву у вигляді числа (яке називається порядковим числівником, від англ. ordinal) і потім додаванням або відніманням із цього числа сформувати нове число (і нову букву). ASCII (вимовляється як ask-ee” і є американським стандартним кодом для обміну повідомленнями) – це код, який зіставляє кожний символ із числом від 32 до 127. Числа менше 32 “недруковані”, тому ми не будемо їх використовувати. Заголовні букви від “A” до “Z” в ASCII мають номери від 65 до 90. Малі літери від “a” до “z” мають номера від 97 до 122. Числам від “0” до “9” відповідають ASCII номера від 48 до 57 (табл. 2)

Таблиця 2

Таблиця ASCII символів

32	(space)	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o		

І так, якщо ми прагнемо змістити “A” на три позиції, то спочатку перетворимо його в число (65). Потім до отриманого числа додамо 3. Після цього перетворимо число 65+3=68 назад у букву (“D”). Скористаємося стандартними функціями мови Python chr() і ord() для перетворень між буквами й числами.

4.2 Функції chr( ) і ord( )

Функція chr() (похідна від “char”, скорочене “character”, “символ”) ухвалює в якості параметра ціле ASCII число й повертає рядок, що полягає з єдиного символу. Функція ord() (скорочене від “ordinal”) у якості параметра ухвалює рядок, що полягає з одного символу, і повертає ціле ASCII значення для цього символу.

Виконаєте наступні команди в інтерактивному режимі:

```
>>> chr(65)
'A'
>>> ord('A')
65
>>> chr(65+8)
'I'
>>> chr(52)
'4'
>>> chr(ord('F'))
'F'
```

```
>>> ord(chr(68))
68
>>>
```

Функції chr() і ord() ми будемо використовувати в нашій програмі.

4.3 Вихідний текст програми шифрування / дешифрування

```
# Caesar Cipher
MAX_KEY_SIZE = 26
def getmode():
while True:
print('Do you wish to encrypt or decrypt a message?')
mode = raw_input().lower()
if mode in 'encrypt e decrypt d'.split():
return mode
else:
print('Enter either "encrypt" or "e" or "decrypt" or "d".')
def getmessage():
print('Enter your message:')
return raw_input()
def getkey():
key = 0
while True:
print('Enter the key number (1-%s)' % (MAX_KEY_SIZE))
key = int(raw_input())
if (key >= 1 and key <= MAX_KEY_SIZE):
return key
def gettranslatedmessage(mode, message, key):
if mode[0] == 'd':
key = -key
translated = ''
for symbol in message:
if symbol.isalpha():
num = ord(symbol)
num += key
if symbol.isupper():
if num > ord('Z'):
num -= 26
elif num < ord('A'):
num += 26
elif symbol.islower():
if num > ord('z'):
num -= 26
elif num < ord('a'):
num += 26
translated += chr(num)
else:
translated += symbol
return translated
```

```
mode = getmode()
message = getmessage()
key = getkey()
print('Your translated text is:')
print(gettranslatedmessage(mode, message, key))
```

4.4 Пояснення до вихідного тексту програми

```
# Caesar Cipher
MAX_KEY_SIZE = 26
```

Перший рядок – це звичайний коментар, який пропускається інтерпретатором. MAX_KEY_SIZE – це змінна, яка містить число 26. MAX_KEY_SIZE служить нагадуванням, що в програмі використовується ключ в інтервалі від 1 до 26.

```
def getmode():
while True:
print('Do you wish to encrypt or decrypt a message?')
mode = raw_input().lower()
if mode in 'encrypt e decrypt d'.split():
return mode
else:
print('Enter either "encrypt" or "e" or "decrypt" or "d".')
```

Функція getmode() (за допомогою нескінченного циклу) дозволяє користувачеві задати режим роботи програми: шифрування (encrypt e) або дешифрування (decrypt d). Функція, що вертається raw_input() (метод lower() повертає рядок у нижньому регістрі) значення зберігається в mode. Умовне вираження перевіряє, чи містить уведений рядок mode один з елементів списку [‘encrypt’, ‘e’, ‘decrypt’, ‘d’], отриманого в результаті виконання ‘encrypt e decrypt d’.split(). Можна використовувати список, але для спрощення введення найчастіше використовують метод split().

Виконайте в інтерактивному режимі інтерпретатора Python:

```
>>> ‘encrypt e decrypt d'.split()
['encrypt', 'e', 'decrypt', 'd']
```

split() може ухвалювати вхідний параметр – роздільник, за замовчуванням роздільником є пробіл.

```
>>> ‘encrypt <> e <> decrypt <> d'.split(‘<>’)
['encrypt ', ' e ', ' decrypt ', ' d']
```

Наступна ділянка коду:

```
def getmessage():
print('Enter your message:')
return raw_input()
```

Функція getmessage() одержує від користувача рядок для шифрування або дешифрування й використовує цей рядок як значення що повертається.

```
def getkey():
key = 0
while True:
print('Enter the key number (1-%s)' % (MAX_KEY_SIZE))
key = int(raw_input())
if (key >= 1 and key <= MAX_KEY_SIZE):
return key
```

Функція getkey() дозволяє вказати ключ, який буде використовуватися для шифрування або дешифрування повідомлення. Цикл while повторюється доти, поки користувач не введе дійсний ключ, тобто, що попадає в інтервал від 1 до MAX_KEY_SIZE.

Оператор % призначений для роботи з рядками, він відіграє роль функції sprint у мові С.

Виконайте в інтерактивному режимі інтерпретатора Python:

```
>>> name = “Ivan”
>>> “My name is %s!” % name
‘My name is Ivan!’
>>>
```

У прикладі рядок “Ivan” підключається до зазначеного рядка, заміщаючи специфікатор %s. Функція raw_input() повертає введений користувачем рядок, який необхідно перетворити в число (за допомогою int()), щоб далі працювати із числовими значеннями. Функція getkey() повертає значення зазначеного користувачем ключа.

```
def gettranslatedmessage(mode, message, key):
if mode[0] == 'd':
key = -key
translated = ''
```

gettranslatedmessage() – функція, яка займається шифруванням і дешифруванням у програмі. На вхід функції надходять три параметри:

mode – установлює режим шифрування або дешифрування,

message – відкритий текст (або зашифрований текст), який треба зашифрувати (або дешифрувати),

key – ключ, який використовується в процесі шифрування.

Перший рядок функції визначає режим шифрування або дешифрування. Якщо першою буквою змінної mode є ‘d’, то встановлюється режим дешифрування. Єдина відмінність між двома режимами полягає в знаку ключа. Якщо в якості ключа було обрано ціле число 22, тоді для режиму дешифрування воно встановлюється як -22. translated – рядок, який буде містити кінцевий результат: шифротекст (якщо ми використовували режим шифрування) або відкритий текст (якщо икористовувався режим дешифрування). Ми будемо приєднувати рядки до цієї змінної, формуючи результат. Змінна повинна бути визначена за допомогою деякого рядка, перш ніж ми зможемо використовувати її для приєднання рядків. isalpha() – рядковий метод, який повертає True, якщо рядок складається з букв нижнього або верхнього регістру від A до Z. Якщо рядок містить будь-які символи не верхнього регістру , тоді isalpha() поверне False.

Виконайте наступні вираження в інтерактивному режимі:

```
>>> 'Hello'.isalpha()
True
>>> 'Forty two'.isalpha()
False
>>> 'Fortytwo'.isalpha()
True
>>> '42'.isalpha()
False
>>> ''.isalpha()
False
>>>
```

Далі ми скористаємося методом isalpha().

```
for symbol in message:
if symbol.isalpha():
num = ord(symbol)
num += key
```

У циклі ми пробігаємо за всіма буквами (символами) рядка повідомлення. Рядки обробляються як списки, що містять рядки, які полягають із одиничних символів. Наприклад, для рядка ‘Hello’ список буде мати вигляд [‘H’, ‘e’, ‘l’, ‘l’, ‘o’]. На кожній ітерації під час виконання циклу, symbol буде мати значення букви з message.

Шифруються й дешифруються тільки букви з message, тому необхідна перевірка всіх символів. Числа, знаки, розділові знаки й інші символи залишаються в первісному вигляді. Змінна num містить числове значення, відповідне до букви, що зберігається в змінній symbol. Потім значення з num “зміщається” на значення з key, це вираження еквівалентне num = num + key.

Далі, у програмі використовуються рядкові методи isupper() і islower(). Вони дуже схожі на методи isdigit() і isalpha(). isupper() повертає True, якщо його рядок містить, принаймні, одну заголовну букву й не містить букв у нижньому регістрі. islower() повертає True, якщо рядок містить, принаймні, одну букву в нижньому регістрі й не містить заголовних букв. А якщо ні, то ці методи повертають False. Наявність небуквених символів, таких як числа й пробіли, не впливає на результат.

Спробуйте ввести наступні вираження в інтерактивному режимі інтерпретатора Python.

```
>>> 'HELLO'.isupper()
True
>>> 'hello'.isupper()
False
>>> 'hello'.islower()
True
>>> 'Hello'.islower()
False
>>> 'LOOK OUT BEHIND YOU!'.isupper()
True
>>> '42'.isupper()
False
>>> '42'.islower()
False
>>> ''.isupper()
False
>>> ''.islower()
False
>>>
```

Продовжимо вивчати код програми.

```
if symbol.isupper():
if num > ord('Z'):
num -= 26
elif num < ord('A'):
num += 26
```

Цей код перевіряє, чи symbol є буквою у верхньому регістрі. Якщо це так, то потрібно подбати про два особливих випадках. Що відбудеться, якщо symbol є буквою ‘Z’ і був заданий ключ рівний 4? У цьому випадку значенням num буде символ ‘’ (числове

значення символу ‘’ рівно 94). Але ‘’ не є буквою, тому в цьому випадку нам необхідно починати відлік з початку алфавіту.

Ми перевіряємо вихід за межі числового значення, що відповідає останній букві алфавіту (“Z”) і якщо така перевірка закінчується успішно, то зменшуємо числове значення на 26, за кількістю букв в англійському алфавіті. Після цього значення змінної num стане рівним 68, що відповідає в ASCII значенню ‘D’.

```
elif symbol.islower():
if num > ord('z'):
num -= 26
elif num < ord('a'):
num += 26
```

Якщо symbol – буква в нижньому регістрі, то програма виконує код, схожий з виконуваним раніше. Єдина відмінність у використанні ord(‘z’) і ord(‘a’) замість ord(‘Z’) і ord(‘A’).

У режимі дешифрування ми можемо одержати випадок, коли num стане менше, ніж найменше можливе значення (в ASCII число 65, відповідне до букви ‘A’). У цьому випадку ми додаємо до num 26 і, тим самим, ураховуємо зсув.

```
translated += chr(num)
else:
translated += symbol
```

Змінна translated служить “накопичувачем” результуючого рядка. Якщо symbol містить букву верхнього або нижнього регістрів, то після перетворення вона додається до результуючого рядка translated. У випадку, коли symbol містить символ, відмінний від букви, він додається до translated, не піддаючись перетворенню, у вихідному виді.

```
return translated
```

В останньому рядку функції gettranslatedmessage() вертається результуючий рядок translated.

```
mode = getmode()
message = getmessage()
key = getkey()
print('Your translated text is:')
print(gettranslatedmessage(mode, message, key))
```

Це основна частина програми. Ми викликаємо кожну із трьох раніше вказаних функцій, щоб одержати значення mode, message і key. Потім ці три значення передаються як вхідні параметри у функцію gettranslatedmessage(), яка повертає результат (перетворений текст), виведений на екран користувача. Що треба змінити в алгоритмі, щоб програма перебирала всі ключі й виводила відповідні їм дешифровані повідомлення?

Підказка:

Для реалізації програми можна скористатися, наприклад, циклом for у зв'язку з функцією range, range генерує індекси в циклі for. Спробуйте ввести наступні вираження в інтерактивному режимі інтерпретатора Python.

```
>>> range(5)
[0, 1, 2, 3, 4]
>>> range(1, 5)
[1, 2, 3, 4]
>>> for i in range(3):
… print
```

```
0
1
2
>>>
```

Лабораторна робота 19
Криптоаналіз

Мета роботи : Вивчення підстановочного шифру й методу частотного криптоаналізу.

1. Теорія
2. Хід роботи.
3. Контрольні питання
4. Додаток

1. Теорія

Найбільш простий тип криптограм – це так звані підстановочні криптограми. Які кожній букві алфавіту зіставляють певний символ (частіше теж букву) і при кодуванні всяку букву тексту заміняють на відповідний їй символ. Розшифрування (криптоаналіз) подібних криптограм не становить великої проблеми. Усе ґрунтується на тому, що різні букви природньої мови – української, російської, англійської мов або якої-небудь іншої зустрічаються в осмислених текстах неоднаково часто. Теж саме вірно й для знаків, що зіставляються їм. У ще більшій мірі це відноситься до буквосполучень із двох або декількох букв. Лише деякі з них часто вживаються, багато інших взагалі не вживаються. Аналізуючи частоту появи тих або інших знаків і їх комбінацій можна з великою впевненістю відновити букви зашифрованого тексту. Цей метод називається частотним аналізом. Він ґрунтується на підрахунку частоти появи зашифрованих знаків. У таблиці 1 зазначені відносні частоти букв української мови. Як випливає із таблиці буква, що найбільше часто зустрічається, українському алфавіті – це О. Її відносна частота, рівна 0,090, означає, що на 1000 букв українського тексту доводиться в середньому 90 букв О. У такому ж змісті розуміються відносні частоти й інших букв. У таблицю 1 не включений символ пробіл.

Таблиця 1

Частота появи букв

В українській мові					
Буква	Частота	Буква	Частота	Буква	Частота
а	0.062	л	0.035	ц	0.004
б	0.014	м	0.026	ч	0.012
в	0.038	н	0.053	ш	0.006
г	0.013	о	0.090	щ	0.003
д	0.025	п	0.023	и	0.016
е	0.072	р	0.040	ь	0.014
ж	0.007	с	0.045	є	0.003
з	0.016	т	0.053	ю	0.006
і	0.062	у	0.021	я	0.018
й	0.010	ф	0.002	пробіл	0.174
к	0.028	х	0.009		

Розглянемо криптограму:

Игфхсхрюм грголк ні хлояню зоб тлзфхгргргирсжс нуютхсгожсумхц гоі л е лрєюш еютгзнгш елр фнгзрльюм

Для розшифрування підрахуємо скільки разів в шифрограмі зустрічається кожна буква (табл. 2).

Таблиця 2

Частота символів у шифрограмі

и	г	ф	х	р	ю	м	о	л	н	з	б	т	х	с	ж	у	ц	і	е	є	ю	ш	ь
2	10	3	5	7	4	3	3	5	3	2	1	3	3	4	2	1	1	1	3	1	3	2	1

Найбільш часто зустрічається символ **Г**, скоріше за все означає букву **О**, або **А**. Зробивши таке припущення, розглянемо наступний за частотою символ Р. В криптограмі маємо двосимволове співвідношення **ГР**.

Якщо **Р** це **Н** (оскільки попередня голосна), то в співвідношенні **ГР** (криптограма) **О** означає приголосну. Із найбільш вірогідних варіантів вибираємо **Л** або **Т**. В цьому випадку допускає осмислений аналіз слово **грголк** в шифровці. Проведемо варіанти підстановки **ОНО…, ОЛО…, АЛО…** або **АНА…** (замість невідомих букв підставлені крапки). Розглянемо останній варіант. У словнику є всього лише кілька слів з 6 букв із таким початком: АНАЛІЗ, АНАЛОГ, АНАНАС, АНАТОМ. З них годиться лише перше. Тому Символ **О** в шифрограмі означає букву **Л, Л – І, К – З.**

Розшифровано чотири символи шифрограми **О** в шифрограмі означає букву **Л, Л – І, К – З.**

Розглянемо слово **гоі.** Відомий тільки другий символ **.Л.** Припустимо, що першиц і третій символи це голосні. Перший символ може бути **А, Е** або **О.** Випробуємо букву **А.** Тоді отримаємо **АЛ.** Слід припустити, що третій символ **Е**. Слово **АЛЕ.** Тому символу **І** треба спів ставити букву **Е.**

Підставимо відомі букви в слово **хлояню.** Отримаємо **.ІЛ...** Слід припустити, що перший символ – приголосна, четвертий – приголосна. Першим символом може бути буква **Х** або **Т**. Підставимо їх в слово, отримаємо варіанти **ХІЛ…** або **ТІЛ…** . Зі словника отримаємо найбільш підходяще слово **ТІЛЬКИ**. Стають відомі наступні символи шифрограми **Х – Т, Я – Ь, Н – К, Ю – И**.

Можно побачити, що шифрограма має зміщення на три символи, та отримана методом підстановки. Тому далі легко розшифровуються всі інші символи і в результаті отримаємо наступне повідомлення:

Частотний аналіз корисний не тільки для підстановочного криптоалгоритму, але і в інших випадках він складніший

2. Хід роботи.

1. Зашифрувати довільний текст за допомогою шифру Цезаря, (букви циклічно зсовуються на декілька кроків). Запропонувати метод розшифрування більш простий ніж частотний аналіз.
2. Провести шифрування тексту (**вид його погодити з викладачем**) методом підстановочного шифру.

3. Контрольні питання

1. Опис алгоритму шифрування
2. Опис алгоритму криптоаналізу
3. Опис лістингу програми

4. Додаток

Таблиці розподілу літер

В українській мові					
Буква	Частота	Буква	Частота	Буква	Частота
а	0.062	л	0.035	ц	0.004
б	0.014	м	0.026	ч	0.012
в	0.038	н	0.053	ш	0.006
г	0.013	о	0.090	щ	0.003
д	0.025	п	0.023	и	0.016
е	0.072	р	0.040	ь	0.014
ж	0.007	с	0.045	є	0.003
з	0.016	т	0.053	ю	0.006
і	0.062	у	0.021	я	0.018
й	0.010	ф	0.002	пробіл	0.174
к	0.028	х	0.009		

В англійській мові					
Буква	Частота	Буква	Частота	Буква	Частота
a	0.0804	b	0.0154	c	0.0306
d	0.0399	e	0.1251	f	0.0230
g	0.0196	h	0.0549	i	0.0726
j	0.0016	k	0.0067	l	0.0414
m	0.0253	n	0.0709	o	0.0760
p	0.0200	q	0.0011	r	0.0612
s	0.0654	t	0.0925	u	0.0271
v	0.0099	w	0.0192	x	0.0019
y	0.0173	z	0.0009		

В російській мові

№	Буква	Відносна частота	№	Буква	Відносна частота	№	Буква	Відносна частота
0	А	0,062	10	К	0,028	20	Ф	0,002
1	Б	0,014	11	Л	0,035	21	Х	0,009
2	В	0,038	12	М	0,026	22	Ц	0,004
3	Г	0,013	13	Н	0,053	23	Ч	0,012
4	Д	0,025	14	О	0,090	24	Ш	0,006
5	Е	0,072	15	П	0,023	25	Щ	0,003
6	Ж	0,007	16	Р	0,040	26	Ы	0,016
7	З	0,016	17	С	0,045	27	Ь,Ъ	0,014
8	И	0,062	18	Т	0,053	28	Э	0,003
9	Й	0,010	19	У	0,023	29	Ю	0,006
						30	Я	0,018

РОЗДІЛ 4
Захист інформації в мережах за допомогою спеціального програмного забезпечення

Лабораторна робота 20
Захист інформації при застосуванні особистої системи мережевого захисту McAfee Personal Firewall Plus

Мета роботи – засвоїти принципи й елементи технології захисту інформації при використанні особистої системи мережевого захисту McAfee Personal Firewall Plus.

Навчитися встановлювати програму захисту, проводити конфігурування системи, вводити, видаляти, корегувати Ip адреси постійного та тимчасового доступу, проводити контроль за діями як із середини мережі так і зі сторони Інтернету.

План

1. Теорія
1.1. Призначення програми.
1.2. Системні вимоги
1.3. Установка програми
1.4. Запуск McAfee SecurityCenter
1.5. Конфігурування елементів системи мережевого захисту
1.6. Блокування спроби підключення до комп'ютера
2. Хід роботи
3. Контрольні питання

1. Теорія
1.1 Призначення програми.

Особиста Система мережевого захисту встановлює бар'єр між вашим 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 вас про потенційно ворожі події
- Забезпечувати детальну інформацію щодо підозрілого інтернетівського трафіку
- Забезпечувати розширену інтелектуальну обробку доступу. Особиста Система мережевого захисту спочатку відзначає, чи 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 ваших 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 - скажемо, у вашій пошті виявиться Аркуш, що містить вірус.

1.2. 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/.

1.3 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.

1.4. Запуск McAfee SecurityCenter

McAfee SecurityCenter - ваш універсальний обчислювальний центр захисту. Він забезпечує консолідоване представлення стану захисту вашого комп'ютера, і наявність вірусних тривог. Ви можете запустити Security Center від значка McAfee у вашій панелі задач (кнопка червоного кольору) використавши допоміжну клавішу маніпулятора типу “миш” рис. 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. Перед вами з'явиться діалогове вікно програми рис. 2.

1.5. Конфігурування елементів системи мережевого захисту

Вам не потрібно, як правило, формувати параметри мережевого захисту, тому що значення, які встановлені за умовчанням забезпечують адекватну безпеку проти вторгнення. Ви можете, проте, змінити параметри налагодження, за допомогою помічника установлення програми.

Помічник установлення дозволяє налагодити:

- вид тривог, які ви хочете одержувати
- захист від вірусів
- мережевий тип підключення
- прикладні рекомендаційні параметри налагодження

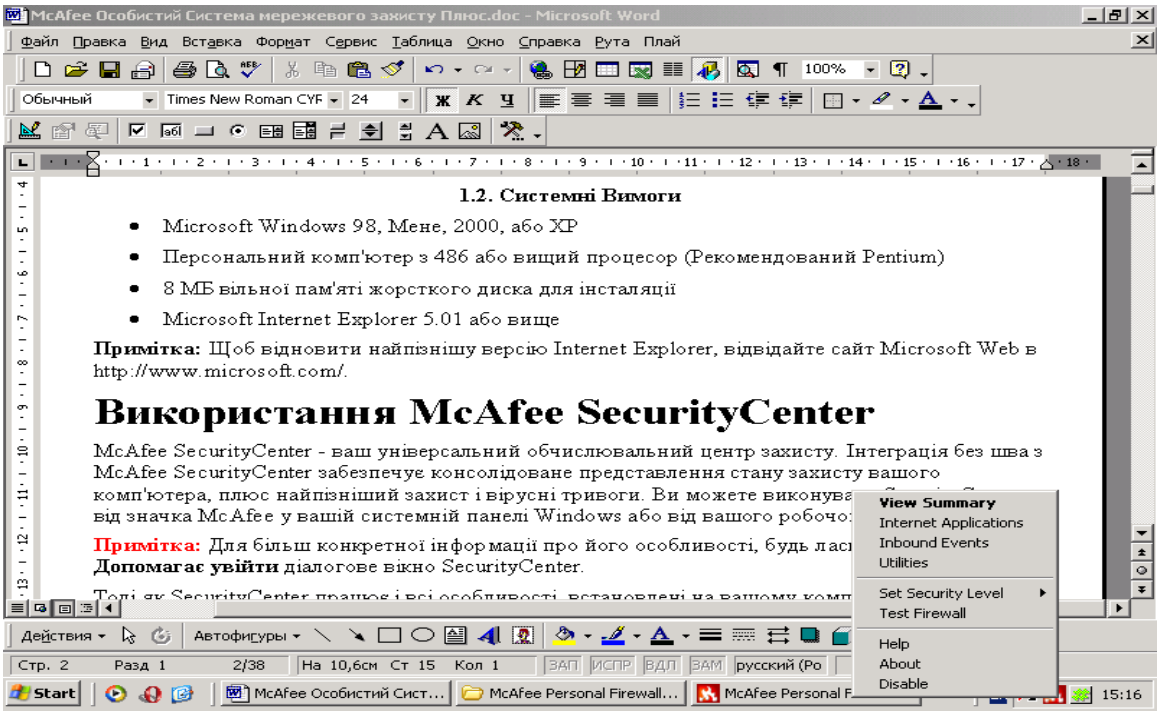


Рис. 1. Вікно запуску програми.

Рис. 2. Вікно програми.

Щоб звернутися до Помічника, клацніть значок **Security Settings**. Виконуйте команди діалогових вікон.

Установки:

Клацніть правою кнопкою миші кнопку (рис. 1) та введіть команду **Утилиты**.

Налагодження параметрів проводиться у діалоговому вікні **Utilities** (рис. 3). Установіть рівень захисту, переміщаючи засувку на бажаний рівень. Якщо ви – користувач системи новачок мережевого захисту, прийміть задане за умовчанням врегулювання Стандарту. Діапазони рівня захисту міняються від низького рівня (відкритий) до максимального (сувора ізоляція):

Таблиця 1.

Рівні захисту

Діапазони рівня захисту	**Опис**
Сувора ізоляція High (Lockdown)	Весь трафік зупинений. Це за суттю такий само режим, як не підключення вашого інтернет-з'єднання. Ви можете 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 застосування як посилати дані, так і одержувати непрошені дані на несистемних портах. Використовуйте це врегулювання, якщо ви - користувач системи новачок мережевого захисту.
Довіра Trusting	Усім підключенням автоматично довірено, коли вони початково намагаються звертатися до Інтернету. Проте, ви можете вибрати параметри, щоб бути повідомленим про нові підключення на вашому комп'ютері з тривогами. Використовуйте це врегулювання, якщо ви знаходите, що деякі ігри або потокові носії не працюють.
Низька фільтрація Open/No)	Ваша система мережевого захисту фактично відключена. Це врегулювання дозволяє весь трафік пропускати без фільтрації.

Примітка: налагодження параметрів можливе, якщо Ви володієте правами адміністратора системи.

- Record Intrusion Detection (IDS) Events in Inbound Events Log (система візуального зображення інформації). Якщо ви вибираєте 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 ви вибираєте цей налагоджувальний елемент, особиста система мережевого захисту дозволяє всі запити залишати без реєстрації у файлі Подій реєстрації, що прибувають.
- 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 ви повинні надати або блокувати доступ.
- Show Only Red and Green Alerts (покажіть тільки червоні й зелені тривоги) — зелені тривоги інформують вас про зміни, які були зроблені до особистої системи мережевого захисту. Наприклад, зелені тривоги можуть інформувати вас про підключення, які особиста система мережевого захисту автоматично надала, або про застосування будь-яких нових правил при доступі до Інтернету.

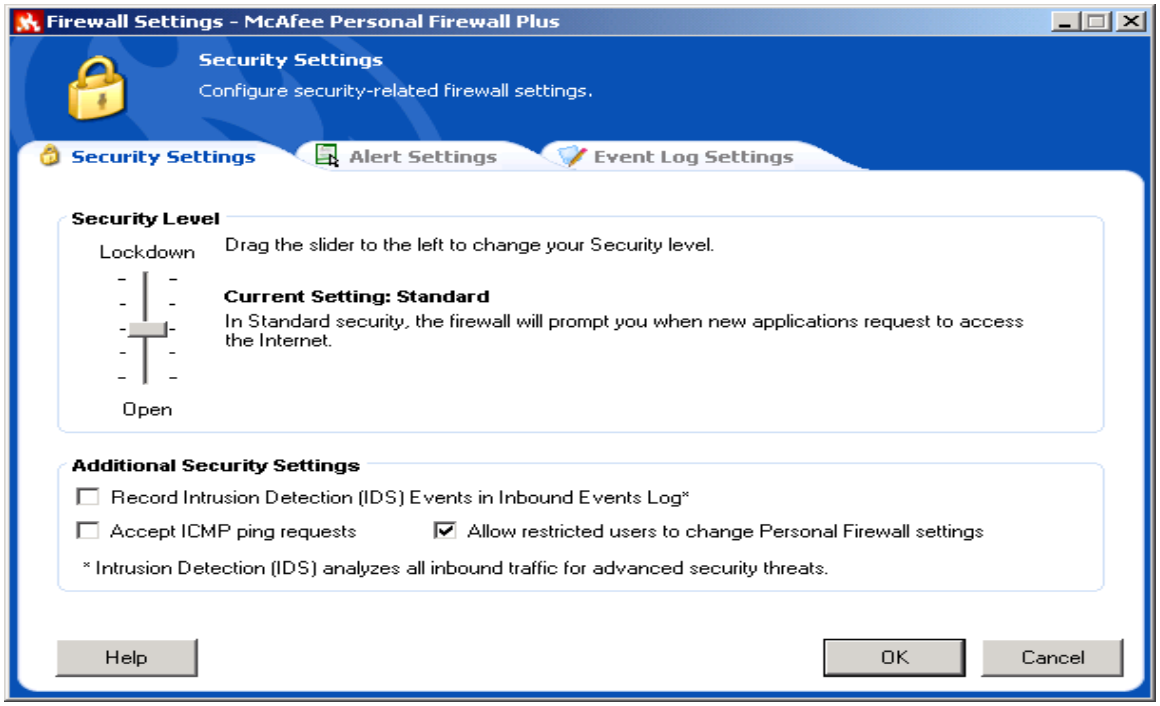


Рис. 3. Вікно утиліт.

- Show All Alerts (покажіть всі тривоги) — покази червоних, зелених, і блакитних тривог. Блакитні тривоги містять інформацію, яка не вимагає ніякої відповіді від вас.

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 прибуває, 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 Ви не відреагуєте на подію. .
- Animate slide-in alerts (активні включені для 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. Ви завжди будете попереджені 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, що прибувають. Якщо ви вибираєте, щоб зареєструвати події, особиста система мережевого захисту відображає події, що прибувають, на сторінці Подій основного вікна. За умовчанням, особиста система мережевого захисту реєструє всі типи події. Ви можете змінитися типи події для реєстрації. Для цього необхідно ввести команду Configure... і у вікні, що з'явиться (рис. 4) відібрати необхідні типи події, а також вказати номери портів показу в представленні подій, що прибувають, щоб показати початкові і призначені порти події у файлі Подій реєстрації.

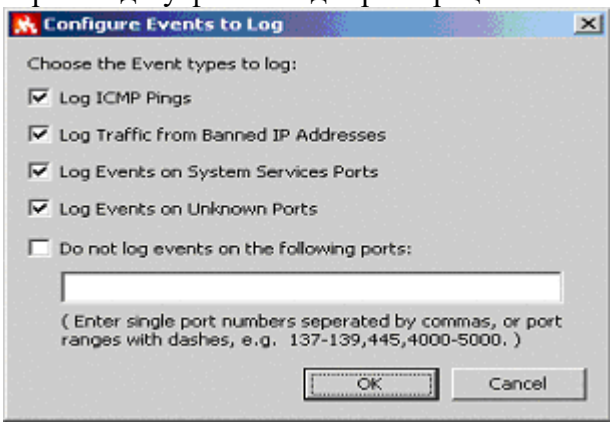


Рис. 4 Вікно вибору типів подій.

Довірені IP адреси

Список довірених адрес Ip дозволяє вам 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. Ваш комп'ютер поводитиметься нібито немає ніякої системи мережевого захисту.

Щоб додати Ip адреси до списку “Довірених Адрес Ip” необхідно:

Виконати дії за рис. 1. на вкладці **Summary** ввести команду **Trusted this IP Addresses**, в діалоговому вікні (рис. 5) увести необхідні 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 Ваш 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. 6) відібрати потрібні порти доступу, або добавити їх, якщо таких немає в системному списку, ввівши команду Add. Список портів наведено в додатку 1.

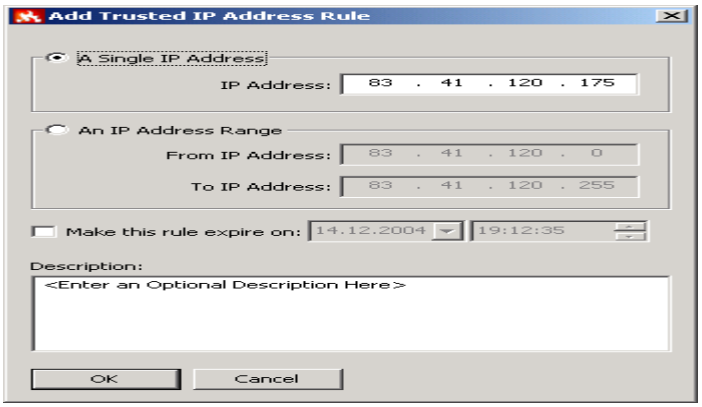


Рис. 5. Вікно введення Ip адреси.

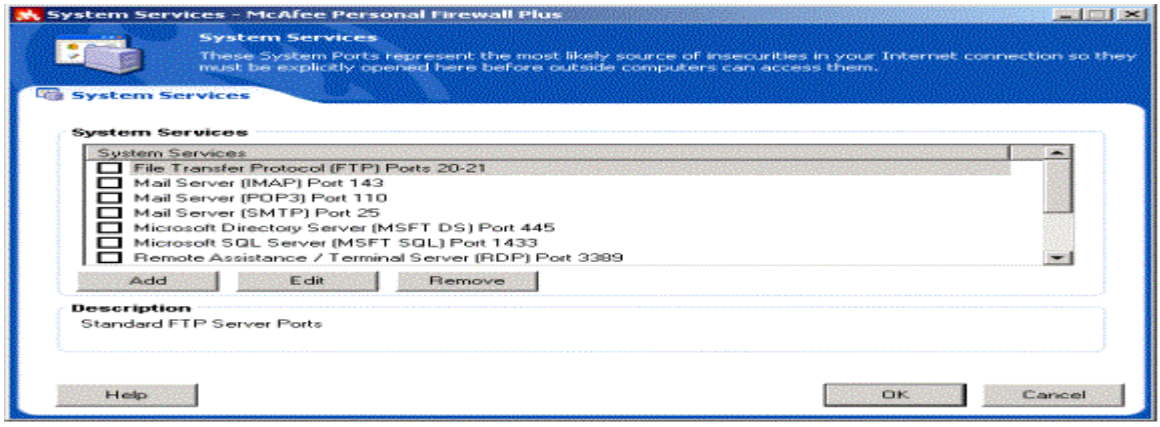


Рис. 6. Вікно вибору портів.

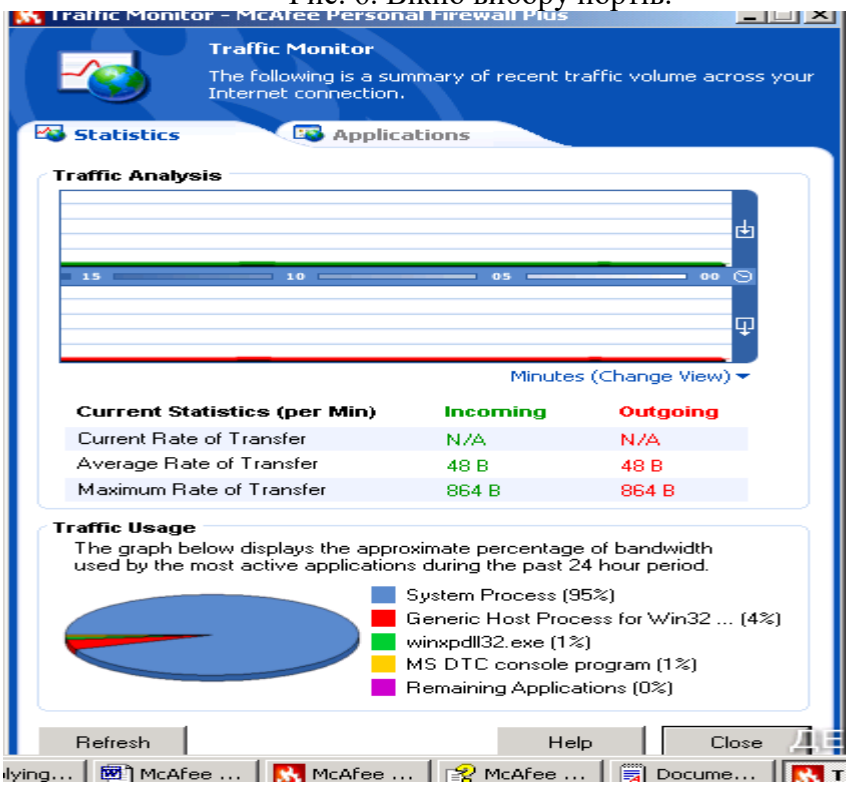


Рис. 7. Вікно моніторингу.

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), але ви можете уручну модифікувати екран, увівши команду Refrech. Для входу в указаний режим необхідно на вкладці **Утилити** ввести команду **Traffic Monitor**.

Вкладка Applications (Аналіз трафіку) показує інтернетівську діяльність у реальному часі на вашому 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. 8).

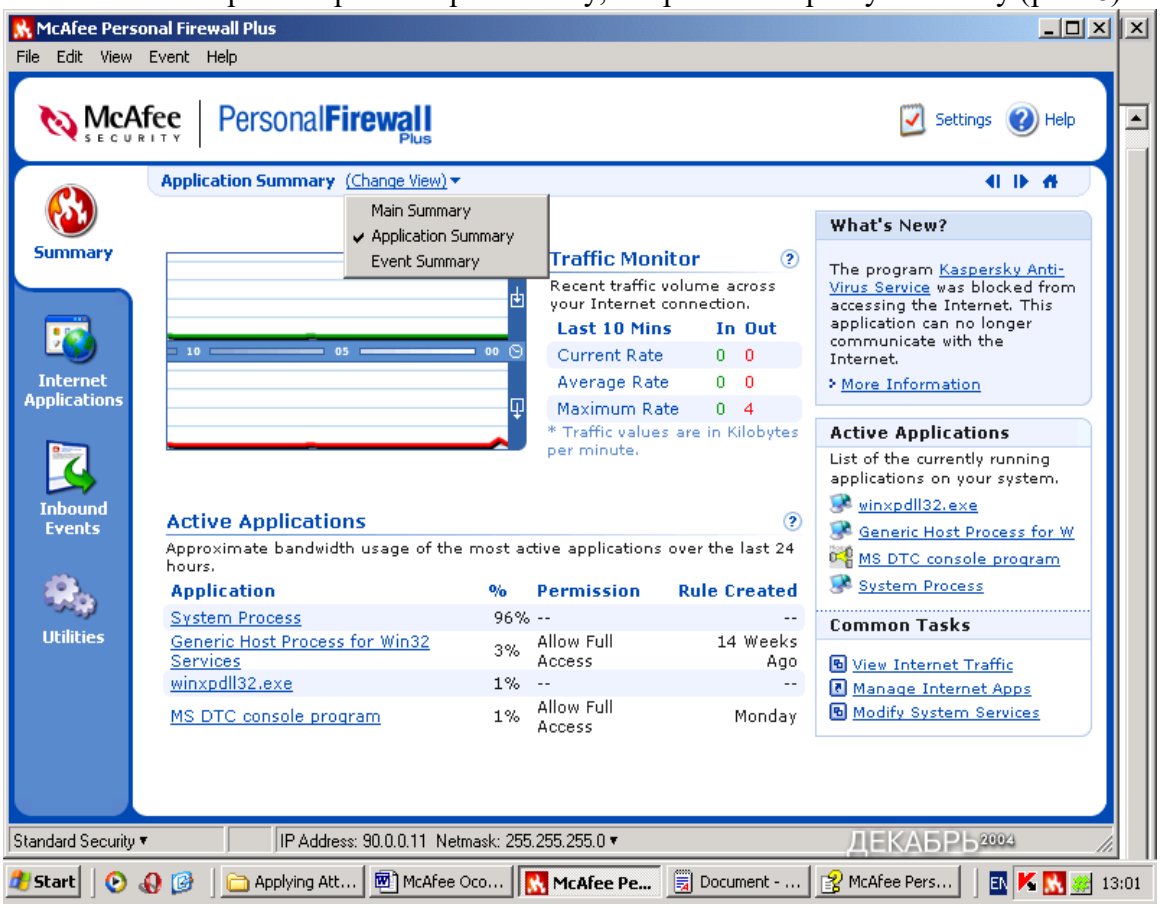


Рис. 8. Вікно відбору звітів.

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. 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. 9. Вікно роботи зі списком дозволів.

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.

Ви можете 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 вашої безпосередньої уваги. 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 Вам 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 вас про зміни, які були зроблені до особистої системи мережевого захисту. Наприклад, зелені тривоги можуть інформувати вас про нові надані доступи до Інтернету, або інформувати вас 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 вас (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)
-

1.6. Блокування спроби підключення до комп'ютера

Наприклад, після отримання сигналу тривоги розгляньте короткий опис події, далі виберіть із цих 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 вашого 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 ви не хочете обрати дію після того, як особиста система мережевого захисту вже виконала її.

2. Хід роботи

1. Установіть програму на свій комп'ютер, виконавши вказівки п. 1.3.
2. Проведіть запуск програми та уважно вивчіть головне меню програми й зміст вкладок.
3. Проведіть конфігурування програми за допомогою помічника установки.
4. За допомогою вікна Utilities встановіть за чергою різні рівні захисту (табл. 1).
5. Установіть на комп'ютері декілька груп користувачів та надайте їм різні права доступу.
6. Установіть візуальний режим відображення інформації.
7. Установіть на комп'ютері почергово різні типи тривог.
8. Установіть різні параметри в полі ”Smart Recommendations ”.

9. Уведіть довільні адреси в список довірених, та таких яким ви тимчасово довіряєте.
10. За допомогою системних послуг відкрийте порти 1433, 143, 110.
11. Проведіть моніторинг трафіку та його аналіз.
12. Закрийте відкриті порти.
13. Опрацюйте звіти. Запишіть головні події у зошит та проведіть їх аналіз.
14. Установіть за чергою різні типи дозволів.
15. Перегляньте файл Подій Реєстрації.
16. Установіть різні типи тривог.

3. Контрольні питання

1. Призначення програми McAfee Personal Firewall Plus.
2. Системні вимоги при інсталяції програми.
3. Порядок запуску McAfee SecurityCenter.
4. Два підходи до конфігурування елементів системи мережевого захисту
5. Конфігурування елементів системи мережевого захисту за допомогою помічника установки.
6. Вибір елементів у вікні утиліт.
7. Типи тривог та їх вибір.
8. Червоні тривоги, їх призначення.
9. Зелені тривоги, їх призначення .
10. Блакитні тривоги, їх призначення .
11. Призначення вкладки Event Log Settings.
12. Установлення Ip адрес.
13. Системні послуги.
14. Порти та їх відкриття, закриття.
15. Моніторинг трафіку.
16. Робота зі звітами.
17. Призначення вкладки Internet Applications.
18. Призначення вкладки Inbound Events.
19. Порядок бокування спроби підключення до комп'ютера в різних випадках.

Список портів див. додаток 2 до лабораторних робіт.

Лабораторна робота 21
Внутрішній мережевий захист із застосуванням програми LANguard Network Scanner.

1. Теорія

1.1 Уведення

Як правило внутрішній мережевий захист недооцінюється адміністраторами. Дуже часто, такий захист навіть не існує. Багато користувачів, як наприклад, працівники в межах компанії, не повинні мати доступу до машин один одного, до адміністративних функцій, до мережевих пристроїв або подібних прав. Звичайно на практиці це не досягнуто, і користувач із мінімальними навиками зможе зробити успішне проникнення і досягти віддалених адміністративних прав вашої мережі в межах декількох хвилин дослідження. Через необхідну гнучкість, яка потрібна для проведення операцій, внутрішні мережі не можуть надати максимальний захист. Проте без захисту взагалі, внутрішні користувачі можуть бути головною загрозою для багатьох корпоративних мереж. Користувач у межах компанії вже має доступ до багатьох ресурсів і йому не потрібно обходити мережевий захист або інші механізми захисту, які запобігають проникненню в мережу інтернетівським користувачам, щоб звернутися до внутрішньої мережі. Окрім внутрішніх користувачів, бідний мережевий захист означатиме, що одного разу хакер одержує володіння комп'ютером, який у межах вашої мережі, він або вона також має доступ до решти частини внутрішньої мережі. Багато “дірок” існують, які дозволяють хакерам проникнути різні протоколи, як наприклад, SMTP (електронна пошта) і http, до механізмів захисту обходу, як, наприклад, системи мережевого захисту. Такі напади дозволять досвідченішому нападаючому легко проникнути і перебрати адміністративні права через внутрішню мережу, зміст конфіденційної електронної пошти і документів може читатися, в комп'ютерах може бути викликана втрата інформації, можливий виток ділової інформації й інші проблеми.

Перелік можливих точок входу хакера в локальну мережу:

- послуги користувачів і відкриті порти
- дірки SNMP
- закулісні користувачі
- троянські коні або закулісне програмне забезпечення
- відкриті акції

- слабкі мережеві паролі
- перелік користувачів, послуги etc і т.п.

Вирішенню вказаних проблем сприяє програма LANguard Network Scanner

Програма призначена для сканування локальної мережі та її компонентів, вона, по-перше, гарантує виявлення хакерських атак, ідентифікацію всіх машин, зав'язаних в локальній мережі, інформацію про Netbios, відкриті порти, нерадивих користувачів, диски і каталоги, відображати уже установлені "хотфикси" (заплатки), які виправляють помилки в програмному забезпеченні або латають дірки; в програму включена обширна база даних з області відомих проблем безпеки, включаючи CGI, FTP і т. д.

Для встановлення програми LANguard Network Scanner необхідно:

- Windows (Windows 2000, NT або XP рекомендований)
- Установлений мережевий протокол Netbios
- ніяке програмне забезпечення особистої системи мережевого захисту не працює. Це могло б блокувати скануючий комп’ютер

Інсталяційна Процедура

1. Виконуйте подвійне клацання по файлу **lannetscan.exe**. Далі виберіть параметри установки за допомогою майстра.

2. У діалоговому вікні ліцензійної угоди, прийміть угоду і продовжуйте інсталяцію.

3. Виберіть місцеположення для LANguard і натисніть далі. LANguard будуть потрібні приблизно 10 МБ вільної пам'яті жорсткого диска.

4. Після того, як LANguard буде встановлений, ви можете звертатися до програми за допомогою ярлика на робочому столі, або з головного меню.

1.2 Сканування системи

Щоб запустити нове мережеве сканування:

В головному меню програми (рис. 1) введіть команду нове сканування з підменю **Файл**.

В діалоговому вікні, яке з'явиться (рис. 2) можна відібрати об'єкти сканування. Виберіть локальну мережу, щоб провести сканування внутрішньої мережі.

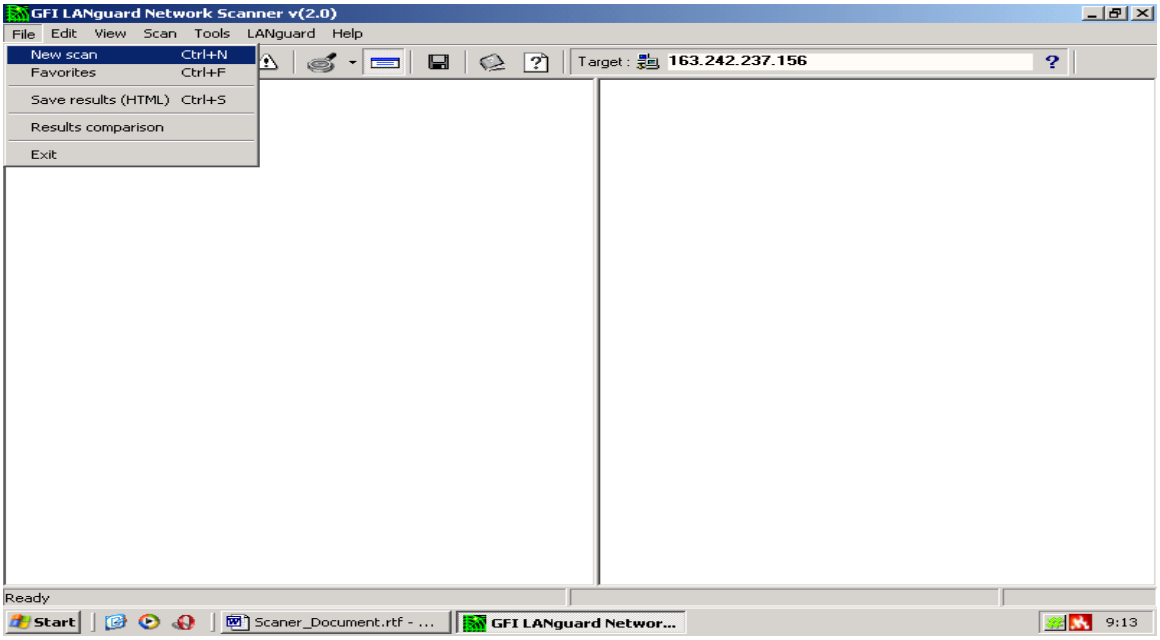


Рис. 1. Вікно програми.

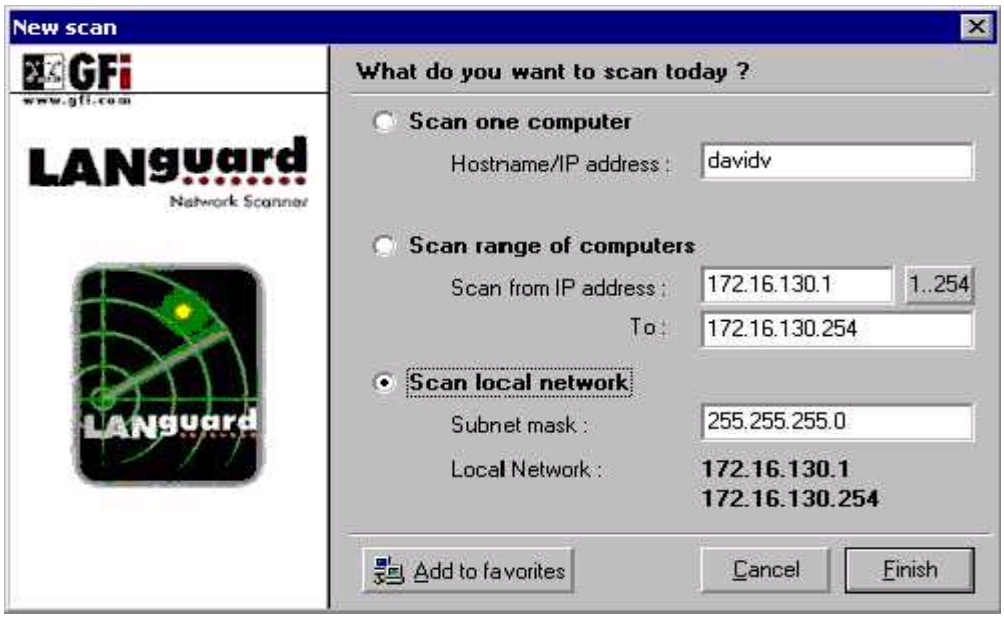


Рис. 2. Вікно вибору об'єктів для сканування.

Натисніть кнопку **Finish**. На панелі інструментів натисніть кнопку **Start Scanning**. Буде проведено сканування вашої внутрішньої мережі. Буде, за умовчанням, виконано дослідження Netbios, міжмережевого протоколу управління повідомленнями ICMP ping і запити SNMP.

1.3. Аналіз результатів

Приклад результатів сканування наведений на рис. 3.

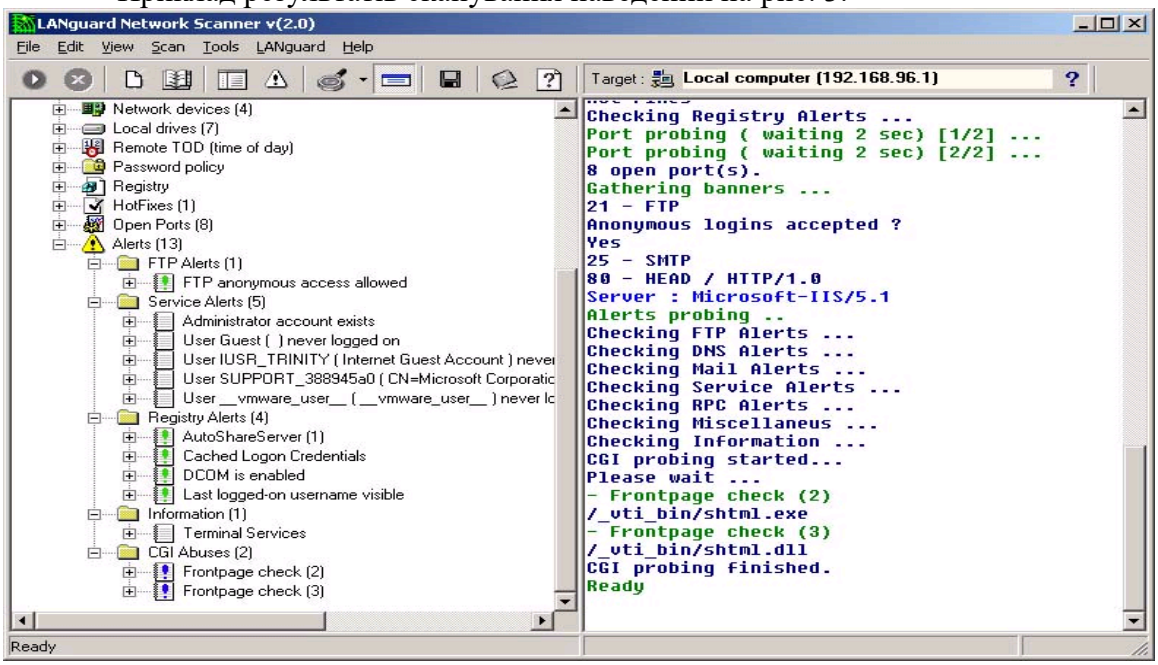


Рис. 3. Вікно результатів сканування мережі.

Після мережевої перевірки, ви бачитимете декілька рядків, що з'являються під кожним комп'ютером.

Дані, які можуть бути критичними:

1. Trusted Domains
2. Shares

3. Users, Groups and Services
4. Password Policy
5. Open Ports
6. Alerts

1. Trusted Domains (Довірені Домени)

Якщо цільовий комп'ютер(и) – входить до домену, то він буде мати записи про довірені домени. Будьте упевнені, що довірені домени, захищені і їм можна довіряти.

2. Shares (Мережеві ресурси)

Треба переконатися, що :

1. Ніхто не може відкрити адміністративний ресурс комп'ютера.
2. Анонімний доступ, не дозволений.
3. Теки автозапуску або подібні системні файли не відкриті. Це могло б дозволити менш привілейованим користувачам виконувати роботу на цільових машинах при запуску комп'ютера та наявності “Трояна” у теці автозапуску.

Згадані вище роздуми дуже важливі для машин, які є критичними до системної цілісності, як, наприклад, публічний контролер домену. Уявіть адміністратора, що відкрив теку (або тека, що містить теку автозапуску) запуску на PDC (Public Domain Controller) для користувачів. Одержавши правильні дозволи, користувачі можуть легко копіювати здійснимі програми, які будуть виконані на наступному діалоговому початку сеансу адміністратора.

3. Users, Groups and Services (Користувачі, групи й служби)

Скануючий комп’ютер перераховує користувачів і групи на машині. Закулісні користувачі або користувачі без підтримки в групах можуть отримати дозвіл доступу чорного ходу. Служби потрібно розглядати так само. Певні служби не повинні працювати на певних машинах, і тому повинні бути зупинені. Цей підхід прихильника мінімалізму виключає багато можливих “дірок” забороняючи хакерам вхід.

4. Password Policy (Політика паролів)

Рекомендовано, щоб політика паролів безпеки впроваджувалася, з тих пір, як вона буде являтися основним проектом захисту. Мінімальна довжина пароля повинна бути практичною, і мати число символів, наприклад, не менш восьми.

5. Open Ports (Відкриті порти)

В результаті роботи LANguard, що робить сканування портів на цільових машинах можна виявити , які порти відкриті, а які закриті. Звичайно, зрозуміло, що багато відкритих портів дозволяють проникнення через них хакерів до комп'ютерів. Кожен порт виконує визначену функцію обслуговування користувача таким чином, що, якщо служба має проблему захисту, хакер міг би запустити напад проти тієї служби, підключаючись до вказаного порту на цільовій машині, і виконати вхід до комп'ютера через запуск exploit. Тому порти, які не потрібні для нормальної роботи, потрібно закрити.

6. Alerts (Попередження)

У сканері LANguard, попередження – містять відомості про загрози і додаткову інформацію (Рис. 3). Такі загрози можуть включати проблеми http, Netbios, проблеми конфігурації, які можуть приводити до проблем захисту і так далі. Кожне з цих попереджень потрібно прийняти серйозно, і надати команди відповідно на те, як виключити проблему.

Дані, які можуть бути не критичними:

Вказані дані, як правило, можуть забезпечити підказки/інформацію до проблем захисту у вашій мережі. До них можна віднести:

1. NETBIOS Information
2. Username
3. MAC
4. TTL
5. LAN Manager
6. Domain
7. Computer Usage
8. Network devices
9. Remote TOD
10. Registry
11. Hot Fixes

1. NETBIOS Information (Інформація Netbios)

Імена Netbios - Це – імена служб, користувачів, що зареєстровані і комп'ютерів.

2. Username (Ім'я користувача)

Це ім'я користувача , який працює в даний час на вказаній машині, або машинного імені.

3. MAC

Це унікальна мережева адреса, яка присвоюється заводом -- виробником мережевим платам.

4. TTL (Time To Live), (Час для життя)

Тривалість життя мережевих пакетів, яка вказує відстань, або час, між сканером LANguard і цільовою машиною.

5. LAN Manager

Указує версію протоколу LAN Manager і операційної системи, яка використовується.

6. Domain (Домен)

Якщо цільова машина – член домену, це надасть вам можливість доступу до довіреного домену.

7. Computer Usage (Комп'ютерне використання)

Говорить вам про те, - цільова машина робоча станція або сервер.

8. Network devices (мережеві пристрої)

Указує список мережевих пристроїв, доступних на цільовій машині

9. Remote TOD

Це мережевий час на цільовій машині, який звичайно встановлений адміністратором.

10. Registry

Надає вам ім'я власника, оригінальне машинне ім'я і різну іншу машинну інформацію. Вказує список програм, що виконуються при запуску комп'ютера, програмне забезпечення як наприклад, Троянські коні і чорні ходи.

11. Hot Fixes (Оперативні виправлення)

Указує на уже встановлені оперативні “заплатки” і т. п.

1.4. Налагодження параметрів програми

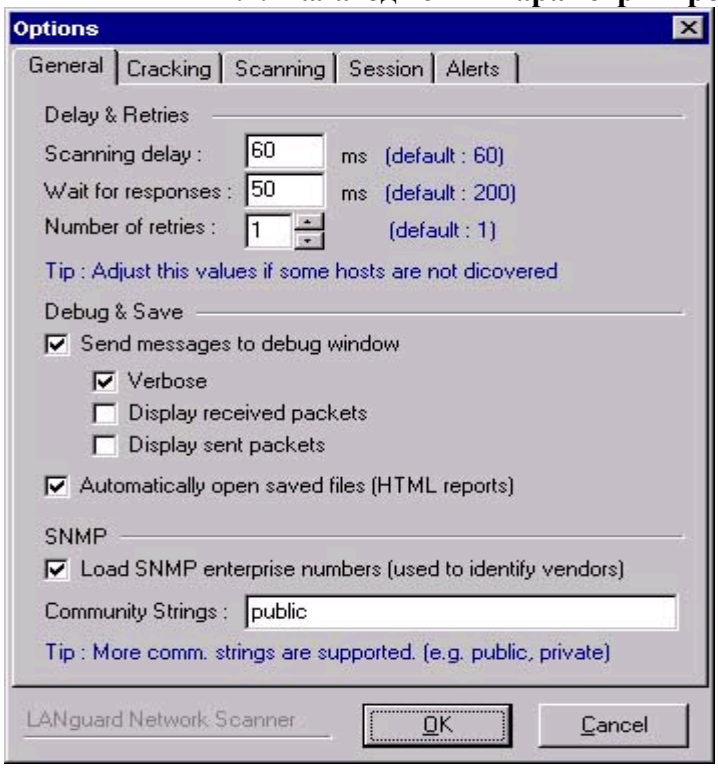


Рис. 4. Вікно налагодження параметрів програми

Для налагодження параметрів програми треба подати команду **Options** із під меню **Scan** з'явиться діалогове вікно рис. 4.

Загальні для налагодження елементи сканування:

Delay & Retries (Повторення й затримки)

Scanning delay (Затримка сканування) -- за умовчанням 60 мс.

Wait for responses (Чекання для відповідей) -- за умовчанням 200 мс.

Number of retries (Кількість повторів).

Debug & Save (Налагодження й збереження)

Send messages to debug windows (Посилати чи ні повідомлення у вікно налагодження)

Verbose (Докладно)

Display received packets (Відображати отримані пакети)

Display send packets (Відображати відправлені пакети)

Automatically open saved files (HTML reports) (Автоматично відкривати збережені файли (Повідомлення html)).

SNMP

Load SNMP enterprise numbers (user to identify venders) (Завантажувати номери SNMP підприємства (використовується для ідентифікації виробника мережевого обладнання)

Community Strings (Указати назву сімейства SNMP).

Вкладка Cracking (Злом) (рис. 5.)

Ця секція дозволяє користувачу формувати для налагодження елементи для злому мережевих ресурсів, щоб ідентифікувати слабкі паролі вказаних ресурсів.

User all characters for cracking (Використовувати всі символи для злому)

Username used for cracking (Ім'я користувача, яке використовується для злому). Це ім'я користувача яке використовується програмою Мережі LANguard для злому пароля на мережевому ресурсі.

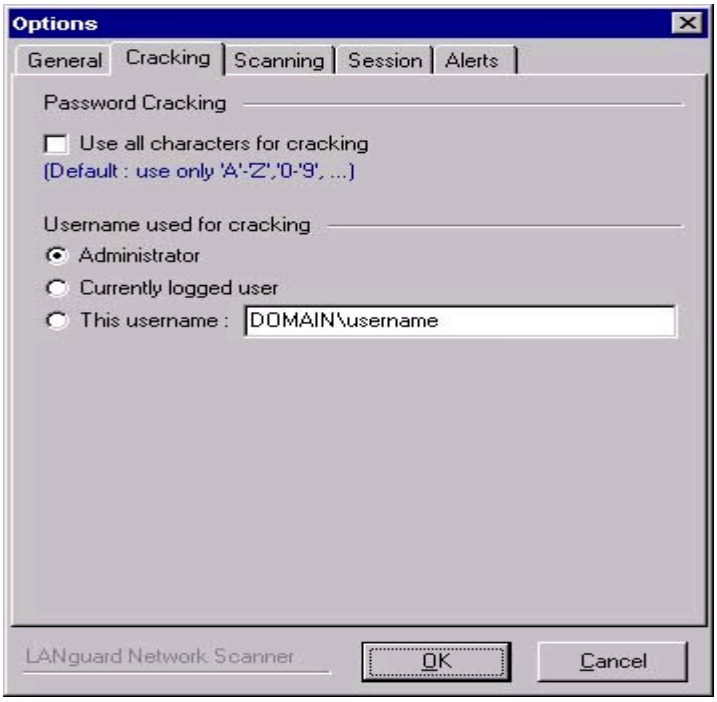


Рис. 5. Вікно вкладки злом.

Вкладка Сканування (рис. 6)

На даній вкладці користувач може конкретизувати методи, щоб використовувати для дослідження мережі. Тобто виявляти, які машини працюють. Деякі сервери, можуть не використовувати протоколи Netbios або SNMP, але вони відповідають на ping. Інколи пакети втрачаються при повільних нестабільних з'єднаннях. Користувач на таких мережах може використати більшу кількість спроб для отримання прийнятного результату. Тут формуються параметри, які порти переглядати, і, які функції Netbios виконуються на цільовій машині. За умовчанням, скануючий комп'ютер виконуватиме сканування портів при виявленні комп'ютера, який працює. Ви можете замінити задану за умовчанням установку параметрів сканування.

Вкладка Сесії

На вкладці можна встановити ідентифікатор особи для сканування, її привілеї, щоб використовувати запити Netbios. Якщо ви не маєте доступу до мережі, це означає, що мало або ніяка інформація не буде одержана. У такому разі, ви повинні вибрати НУЛЬОВУ сесію, яка дозволить анонімному користувачу перерахувати служби і так далі.

Вкладка Попередження (рис. 6)

На вкладці вибираються параметри:

Alerts probing (Дослідження попереджень)

Alerts probing enabled (дослідження попереджень включене)

Internal chechs enabled (ftp annon, weak passwords...) (Внутрішні перевірки включені)

CGI probing enabled (Уключити перевірку скриптів CGI)

Proxy support (Підтримка Proxy)

Send CGI reguests through this proxy (Посилати CGI запити через указаний Proxy)

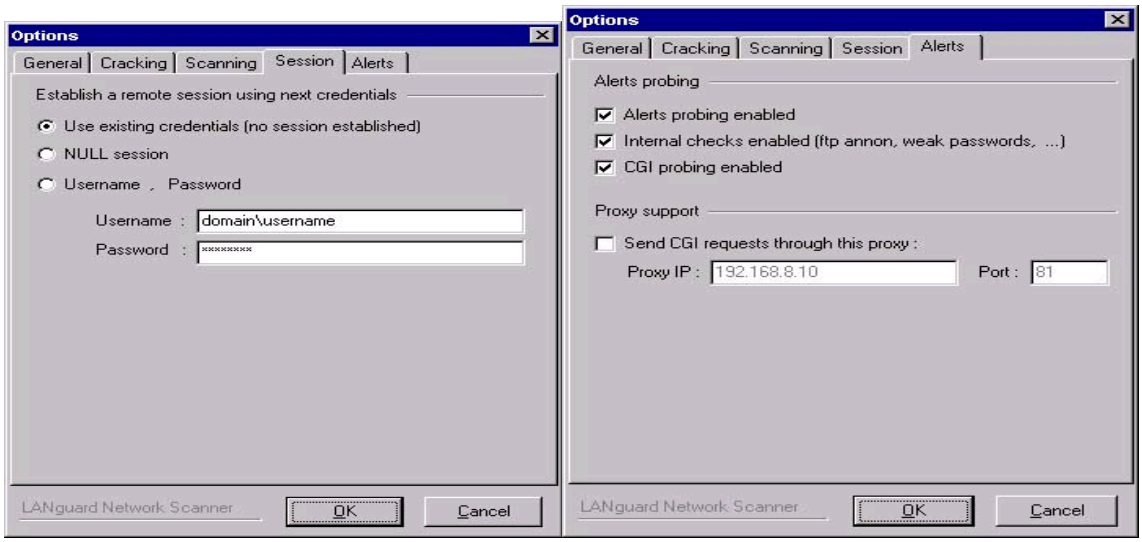


Рис. 6. Вкладка сканування та попередження

1.5 Порівняння результатів

Коли сканер LANguard зберігає висновок html, то також зберігає файл із розширенням xml, який використовується в модулі порівняння результатів.

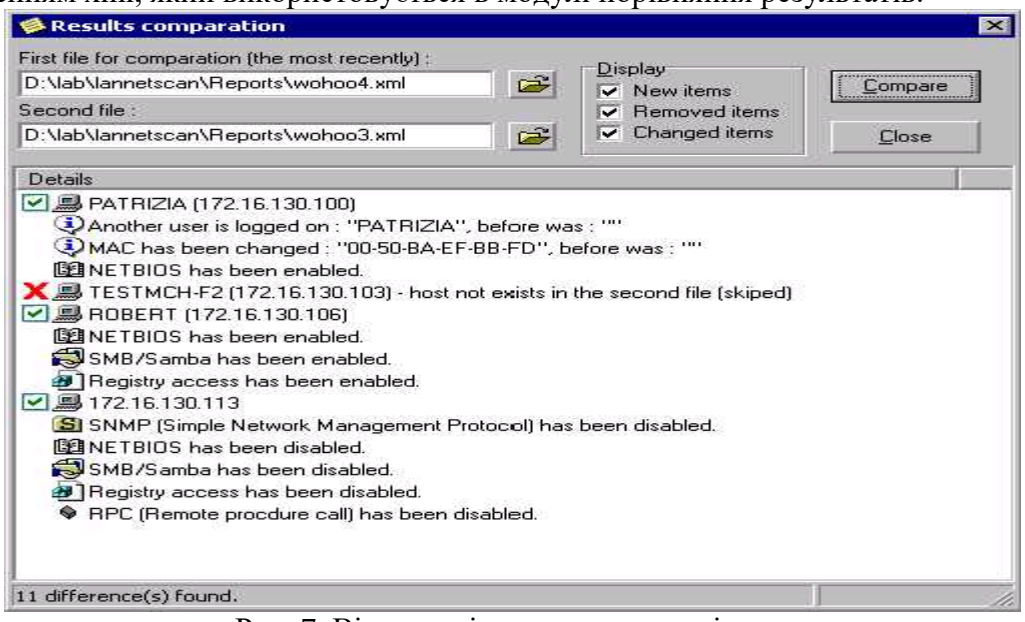


Рис. 7. Вікно порівняння результатів сканування.

Щоб порівняти два зразки, виберіть із підменю **Файл** команду порівняння результатів (до того вікно результатів сканування повинно бути активним у програмі). З'явиться вікно рис. 7. Виберіть два файли, що складаються з такого ж сканування у різний час, і введіть команду порівняння (клавіша **Compare** у даному вікні). Результати порівняння вкажуть Вам на те, що було добавлено або відключено і будь-які мережеві зміни, починаючи з останнього сканування.

1.6. Додаткові утиліти програми

Перевірка SNMP

Деякі мережеві пристрої мають рядки альтернативного або незаданого за замовчуванням сімейства. Перевірка SNMP дозволяє вам зламати слабкі суспільні рядки

(community strings). Уведіть команду **SNMP audit** із підменю **Tools** (рис. 8). Файл словника повинен містити список популярних суспільних рядків для перевірки.

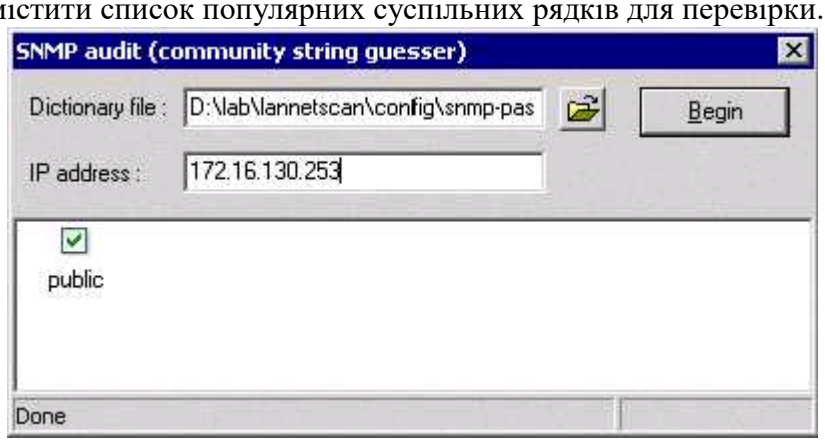


Рис. 8 Вікно аудиту SNMP

Пошук сервера імен доменів (DNS)

Введіть команду **DNS lookup** із підменю **Tools** (рис. 9). Цей інструмент визначає доменне ім'я комп'ютера за його відповідною IP адресою.

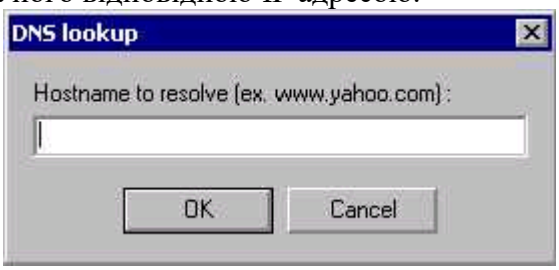


Рис. 9. Вікно визначення доменного імені за IP адресою.

Показ траси.

Уведіть команду **Traceroute** із підменю **Tools** (рис. 10). Це простий інструмент, який указує мережевий шлях між скануючим комп'ютером і цільовою машиною.

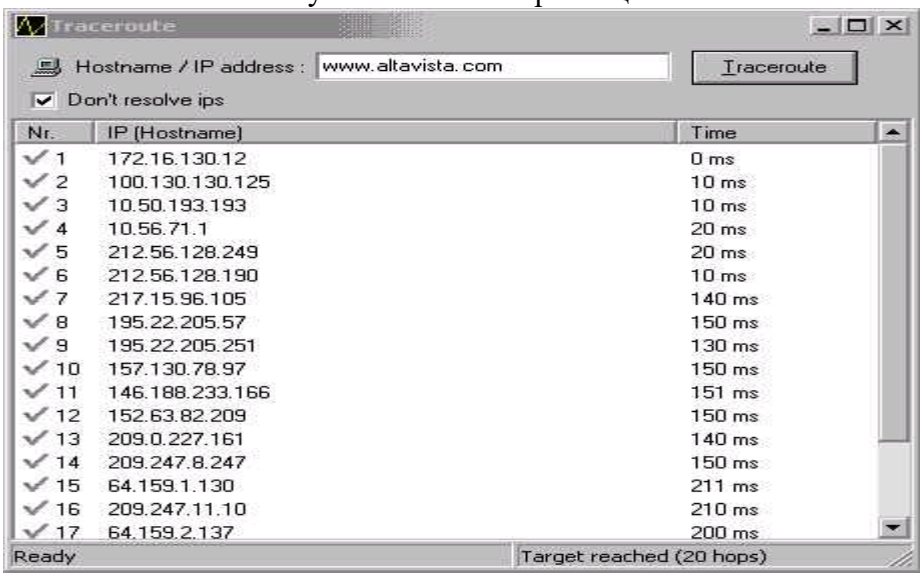


Рис. 10 Вікно виконання traceroute.

1.7 Команди контекстного меню

SNMPwalk

Виконання вказаної утиліти можливе, коли на комп'ютері, який сканується, встановлено SNMP. Це надає можливість скануючому комп'ютеру надати запит службі SNMP, та отримати відповідну інформацію,таку, як, наприклад, перелік відкритих портів, присутні служби, і так далі. Уведіть команду **SNMPwalk** із контекстного меню (рис. 11).

SNMP допоможе користувачам дізнатися багато про вашу систему. За винятком випадків, коли це обслуговування потрібне, рекомендується вказану службу закрити назавжди.

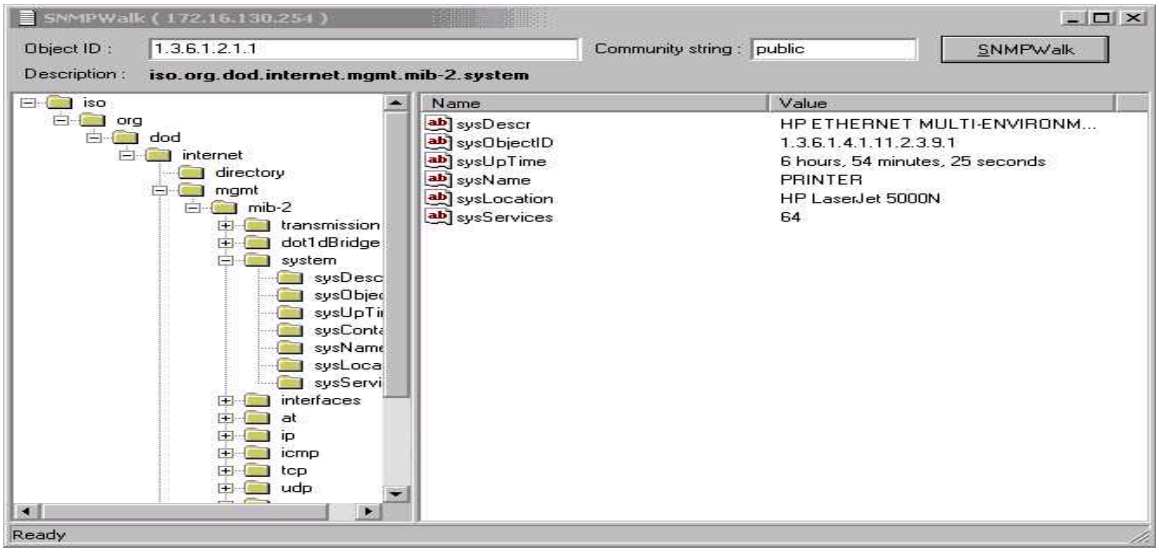


Рис. 11. Вікно програми SNMPwalk.

Збирання інформації.

Уведіть команду **Gather Information** із контекстного меню.

Дозволяє провести сканування одного вибраного комп'ютера зі списку.

Copy to clip board

Цей налагоджувальний елемент просто копіюватиме інформацію в буфер обміну.

Resolve Address

Якщо команда **Gather Information** не вибрана, щоб узнати доменне ім'я комп'ютера, можна вибираючи цей налагоджувальний елемент.

Crack Password (Win9x)

Уразливість у Windows 95, 98 і ME Netbios дозволяє користувачам легко визначити паролі на мережеві ресурси. Windows NT і 2000 не уразливі до цих нападів, і цей налагоджувальний елемент не працюватиме для них.

Для більш конкретної інформації про цю проблему зверніться за адресою:

http://support.microsoft.com/support/kb/articles/Q273/9/91.ASP?LN=EN-US&SD=gn&FR=1

Dictionary Attack

Команда аналогічна попередній з тою різницею, що для збільшення швидкості визначення паролю використовується словник Вікно утиліти вказано на рис. 12.

Рис. 15 Вікно Dictionary Attack

Send Message

Цей налагоджувальний елемент дозволяє скануючому комп'ютеру посилати Netbios повідомлення з підробленою Ip адресою відправника.

Shutdown

Дозволяє дистанційно вимкнути комп'ютер, який сканується в тому випадку, якщо в користувача, який сканує, маються відповідні права.

Expand All

Вибір цього налагоджувального елементу відкриє дерево комп'ютерів у лівій панелі рис. 3.

Saving Results

Щоб зберегти результати, виберіть Файл із меню і виберіть Результати (html) Збереження, або натисніть Control+S. Файл буде автоматично названий згідно вашому скануванню.

На збереженні файлу html, Internet Explorer або Netscape повинен запуститися на виконання і відобразити результуючий файл html.

List of Alerts

Список попереджень і їх опису.

Introduction

Цей розділ складає список усіх налагоджувальних елементів меню сканера LANguard і короткого опису кожної функції

1.8. Зміст команд головного меню

File Menu

- New scan - Дозволяє вам вибирати новий діапазон для сканування.
- Favorites – Обране. Налагодження, які використовуються з попередніх скануванb.
- Save Results (HTML) - Це збереже результати до файлу html після сканування

Results Comparison - Дозволяє вам порівнювати сканування, щоб відзначити нові можливі проблеми захисту, будь-які мережеві зміни, і т.п.

- Exit - Залишає програму

Edit

- Add computer - Дозволяє вам уручну додавати комп'ютер, щоб зібрати інформацію.
- Remove Computer - Дозволяє вам уручну видаляти комп'ютер із списку
- Find Computer - Дозволяє вам знаходити комп'ютер.
- Sort Computers – сортувати комп'ютери

VIEW

Debug Window – Показувати або ні праву панель Рис. 3.

Portscan.txt - Цей текстовий файл містить список портів, які будуть скануватися

Passwords.txt - Цей текстовий файл містить список мережевих паролів, які будуть підставлятися зі словника

Rpc.txt - Цей текстовий файл містить список відомих послуг Rpc

Object_Ids.txt - список ідентифікаторів об'єктів для запитів SNMP, для ідентифікації Операційної Системи.

Scan

Gather information - Дозволяє вам збирати інформацію щодо вибраного комп'ютера

Gather information from all - Дозволяє вам збирати інформацію щодо всіх комп'ютерів

Alerts - Конфігурація попереджень. Дозволяє вам додавати нові попередження, видалити існуючі, і конкретизувати, які попередження використовувати в скануванні

Options – налагодження конфігурації сканера LANguard..

Tools

DNS lookup - Дозволяє вам визначити доменне ім'я комп'ютера за його адресою IP.

Traceroute - Надає вам шлях між сканером і цільовою машиною

SNMP audit – Робить підбір за словником рядків сімейства SNMP

2. Хід роботи

1. Запустіть програму LANguard Network Scanner на виконання та познайомтеся з командами головного меню.
2. Налагодьте параметри програми для сканування внутрішньої мережі.
3. Проведіть сканування внутрішньої мережі.
4. Проведіть аналіз результатів сканування для даних, які можуть бути критичними (у зошиті для лабораторних робіт скласти таблицю з коментаріями).
5. Проведіть аналіз результатів сканування для даних, які можуть бути некритичними (у зошиті для лабораторних робіт скласти таблицю з коментаріями)
6. Проведіть повторне налагодження параметрів програми для сканування внутрішньої мережі (параметри повинні відрізнятися від попереднього налагодження).
7. Проведіть повторне сканування внутрішньої мережі.
8. Проведіть порівняння результатів сканування за перший та другий рази.
9. В зошиті для лабораторних робіт складіть табличку з даними, які відрізняються при первинному та повторному скануваннях. Поясніть, чому є відмінності в результатах сканувань.
10. Проведіть роботу з утилітами програми згідно п. 6 теорії.
11. Використайте в роботі команди контекстного меню програми.
12. Результати сканування мережі зберегти на сервері у своєму каталозі.
13. Зробити висновок про захищеність мережі зсередини.

3 Контрольні питання

14. Чому набуває важливості захист комп'ютерних мереж зсередини?
15. Перелік можливих точок входу хакера в локальну мережу.
16. Призначення програми LANguard Network Scanner.
17. Порядок сканування мережі.
18. Аналіз результатів сканування.
19. Критичні та некритичні параметри сканування їх призначення.
20. Налагодження параметрів програми.
21. Порівняння результатів сканування.

22. Додаткові утиліти програми, їх призначення.
23. Команди контекстного меню програми.
24. Команди головного меню програми.

Лабораторна робота 22 Сканування мереж

З м і с т

1. Теорія

1.1 Опис програми

Програма «10-страйк: Сканування Мережі» (Network Skanner) - зручна безкоштовна програма, яка допоможе вам одержати деяку інформацію про будь-яку локальну мережу. Вона просканує мережу, знайде всі доступні мережеві пристрої й одержить від них максимально доступний обсяг інформації. Програма може бути використана без попередньої установки на комп'ютер, тобто ви з легкістю можете записати її з флешки в будь-якій версії Windows, починаючи з Win2k. Крім одержання інформації програма дозволить виконувати вам деякі дії для керування комп'ютерами в мережі: пінгувати, трасувати маршрут, перезапускати, виключати й включати їх, управляти службами й реєстром на віддалених комп'ютерах. Крім усього, "Сканування Мережі" уміє взаємодіяти з мережевими пристроями за протоколом SNMP і одержувати будь-яку інформацію через нього. Програма є відмінним засобом для починаючого системного адміністратора або просто допитливого користувача.

1.1.1 **Основне призначення програми:**

Програма сканує локальну мережу, автоматично одержує перелік доступних хостів, формує список хостів, дозволяє виконувати наступні операції з ними:

Одержувати інформацію: IP-, Mac-Адреси, Dns-Ім'я, виробник адаптера, поточний користувач, домен, сервер, тип ОС, дата й час, час роботи, список локальних дисків, загальні ресурси, список активних підключень, облікові записи, групи, параметри реєстру, служби й пристрої, відкриті Tcp-Порти, запущені процеси, журнали подій, установлені програми, Snmp-Інформація.

- Пінгувати за протоколом ICMP
- Трасувати маршрут до віддаленого хоста
- Включати й виключати комп'ютери по мережі
- Відкривати в Провіднику (як у Мережнім оточенні)
- Порт на комутаторі
- Переглядати статистику використання локального вхідного й вихідного трафіка
- Управляти локальними папками загального доступу

- Управляти службами на віддаленому комп'ютері: зупиняти, запускати, відключати і т.д.
- Змінювати, додавати й видаляти параметри в реєстрі віддаленого комп'ютера.

1.1.2 **Можливості програми:**

- Швидке, багатопотокове сканування локальної мережі за заданими діапазонами Ip-Адрес;
- Одночасне застосування декількох способів виявлення мережевих пристроїв: ICMP-Пінг, сканування списку Tcp-Портів, Arp-Пинг (перетворення IP- в Mac-Адресу);
- Інтелектуальний алгоритм розпізнавання типу мережевих пристроїв. Визначення мережевих і локальних принтерів, серверів, серверів БД, роутеров, комутаторів, хабов, Wifi-пристроїв і т.д.;
- Одержання додаткової інформації про пристрої через Netbios;
- Пошук пристроїв, що підтримують протокол SNMP (комутатори, принтери, відеокамери, роутери і т.д.);
- Пошук пристроїв, що підтримують протокол UpnP (медіаплеєри, роутери і т.д.);
- Збереження результатів сканування в Csv-Форматі (підтримується Microsoft Excel);
- Автоматичне формування списку хостів для подальшої роботи;
- Автоматичне збереження всіх змін списку, параметрів хостів і перевірок;

Програма повністю працездатна під ОС WINDOWS NT4/2000/XP/2003/Vista/2008/7/8.

У локальній мережі повинен бути дозволений протокол ICMP або сканування TCP-Портів. Для повного функціонування повинні бути дозволені протоколи SNMP, Netbios.

Для успішного виконання програми необхідно запускати її тільки із правами адміністратора.

При використанні методу сканування мережі TCP-Пінг слід ураховувати, що в ОС Windows XP і вище не допускається більш 10 одночасних Tcp-Підключень. Це може позначитися на продуктивності програми

1.2 Початок роботи із програмою

1. Запустіть програму. Якщо ви запустили програму перший раз, то побачите на екрані головне вікно програми **" 10-страйк: Сканування Мережі"** і вікно **Майстра сканування мережі (рис. 1).**

Дотримуючись вказівок **Майстра...** можна швидко й легко виявити хости в мережі і додати їх у список.

Майстер... пропонує 2 способу пошуку хостів у мережі:

Сканування діапазону Ip-Адрес.

Даний спосіб дозволяє виявити максимальну кількість пристроїв, має наступні переваги:

- висока швидкість сканування діапазону (при оптимальному (див. нижче) виборі параметрів сканування й налагодження мережі);
- дозволяє визначати різні види пристроїв: принтери (локальні й мережні), комутатори, хаби, сервера, сервера баз даних, роутери, Wifi крапки доступу і т.д.;
- застосовує відразу кілька ефективних способів пошуку пристроїв у мережі (ICMP-Пінг, сканування списку Tcp-Портів, Arp-Запити);
- дозволяє одержувати інформацію із пристроїв за SNMP;
- автоматично одержує багато іншої інформації про знайдені хостах (IP, Mac-Адреси, виробника мережевого адаптера, Dns-Ім'я, тип ОС, підключені принтери, описи);
- дозволяє сканувати відразу кілька діапазонів Ip-Адрес;

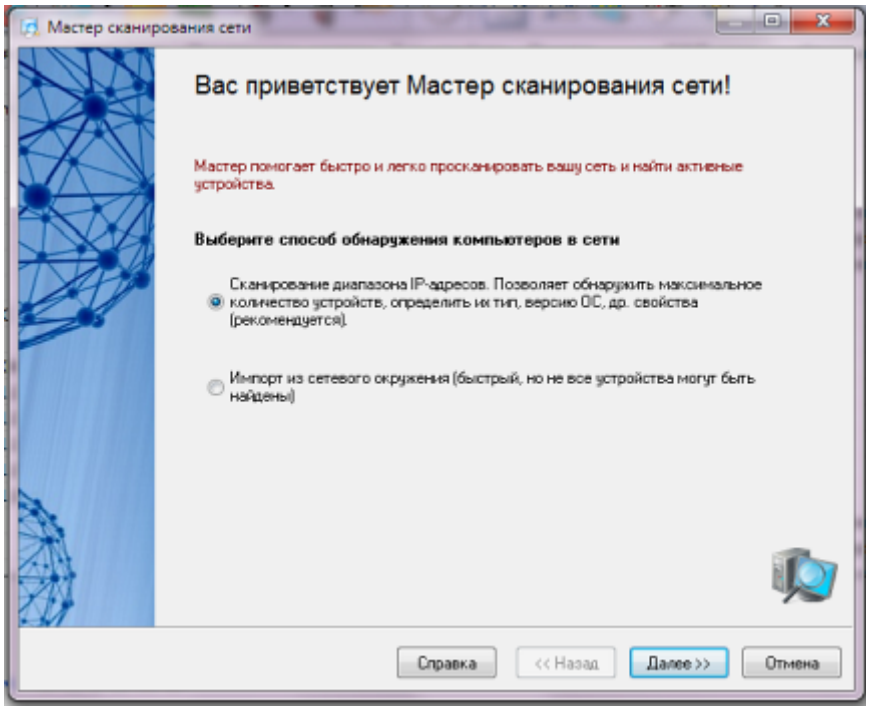


Рис. 1 Вікно майстра сканування мережі

Якщо у вас більша мережа, що комутирується, то рекомендується використовувати цей спосіб сканування.

Оптимальність вибору параметрів випливає з конфігурації вашої мережі, наявності й функціонування необхідних протоколів. Зокрема, у невеликий 100 Мбіт локальної мережі для виявлення хостів досить буде 2-х пакетів пінга, і 100-500 мс секунд відгуку. У випадку сканування Tcp-Портів треба зрозуміти, що чим більше ви вкажете портів у списку, тем довше буде відбуватися процедура **пошуку**. Оптимальним варіантом отут є завдання 2-3 загальнопоширених портів, за якими можна знайди Windows-Станції або сервера - це 139, 21 і 80й порти (Netbios, FTP, HTTP). Слід урахувати вбудоване обмеження (затримка) на одночасне сканування декількох Tcp-Портів в ОС Windows XP і вище.

У більшій мірі варто сказати про пошук **мережевих принтерів**. Дана процедура займає досить тривалий час, тому її не варто використовувати, якщо ви точно знаєте, що таких принтерів у вашій мережі немає. Інакше необхідно дочекатися закінчення цієї процедури, про що буде свідчити поява у вікні майстра індикатору ходу сканування мережі. Справа в тому, що пошук мережевих принтерів проводиться до запуску основної процедури сканування (яка виконується більшою кількістю паралельно працюючих потоків, на відміну від пошуку принтерів). Це відноситься й до можливості одержання додаткової інформації про хости через Netbios.

Якщо у вашій мережі заборонений протокол Netbios, то ніяка **додаткова інформація** не може бути отримана, і програма затратить досить багато часу на цю спробу (звідси відчуття, що програма "зависла").

Пошук пристроїв з SNMP здійснюється в багатопоточному режимі. Однак якщо ви вкажете досить велику кількість можливих community string, то це так само сповільнить процес сканування.

Виходячи із усього сказаного, випливає порада, що якщо ви вибрали параметри, і програма повільно сканує й взагалі "зависла" - слід відключити деякі параметри (у першу

чергу пошук мережевих принтерів, потім одержання додаткової інформації через Netbios) і спробувати просканувати знову.

Імпорт із мережевого оточення.

Даний спосіб працює трохи швидше, але не всі мережеві пристрої можуть бути знайдені (тільки комп'ютери й деякі сервера).

Якщо **Майстер...** виявив не всі хости, ви можете добавити їх в список вручну.

2. Використовуйте контекстне, головне меню й панель інструментів для доступу до функцій програми. Усі функції програми доступні через контекстне меню, панель інструментів, головне меню, і будуть описані далі.

1.3 Створення списку хостів мережі

Створення списку хостів мережі здійснюється за допомогою Майстра сканування мережі. Список хостів створюється в кілька етапів:

1. Виклик Майстра сканування мережі.

Для цього потрібно вибрати пункт головного меню **Файл**, потім **Сканувати мережа**.

2. Вибір способу сканування мережі.

Для пошуку мережевих пристроїв **Майстер** використовує 2 способи сканування мережі (рис.1):

- **Сканування діапазону Ip-Адрес** Даний спосіб дозволяє виявити максимальну кількість пристроїв, має наступні переваги:
  - багатопоточність, що забезпечує високу швидкість сканування діапазону;
  - дозволяє визначати різні види пристроїв: принтери (локальні й мережні), комутатори, хаби, сервера, сервера баз даних, роутери, Wifi крапки доступу і т.д.;
  - застосовує відразу кілька ефективних способів пошуку пристроїв у мережі (ICMP-Пінг, сканування списку TCP-Портів, Arp-Запити);
  - дозволяє одержувати інформацію із пристроїв за SNMP (комутатори, принтери, Wifi і т.д.);
  - дозволяє сканувати відразу кілька діапазонів Ip-Адрес;

Якщо у вас велика мережа, що комутується, то рекомендується використовувати цей спосіб сканування.

- **Імпорт із мережного оточення** Даний спосіб працює трохи швидше, але не всі пристрої можуть бути знайдені.

При імпорті з мережного оточення необхідно на наступних кроках Майстра просто слідувати його підказкам. Процес сканування діапазону адрес потребує детального опису.

3. Крок 1. Завдання діапазону Ip-Адрес (рис. 2).

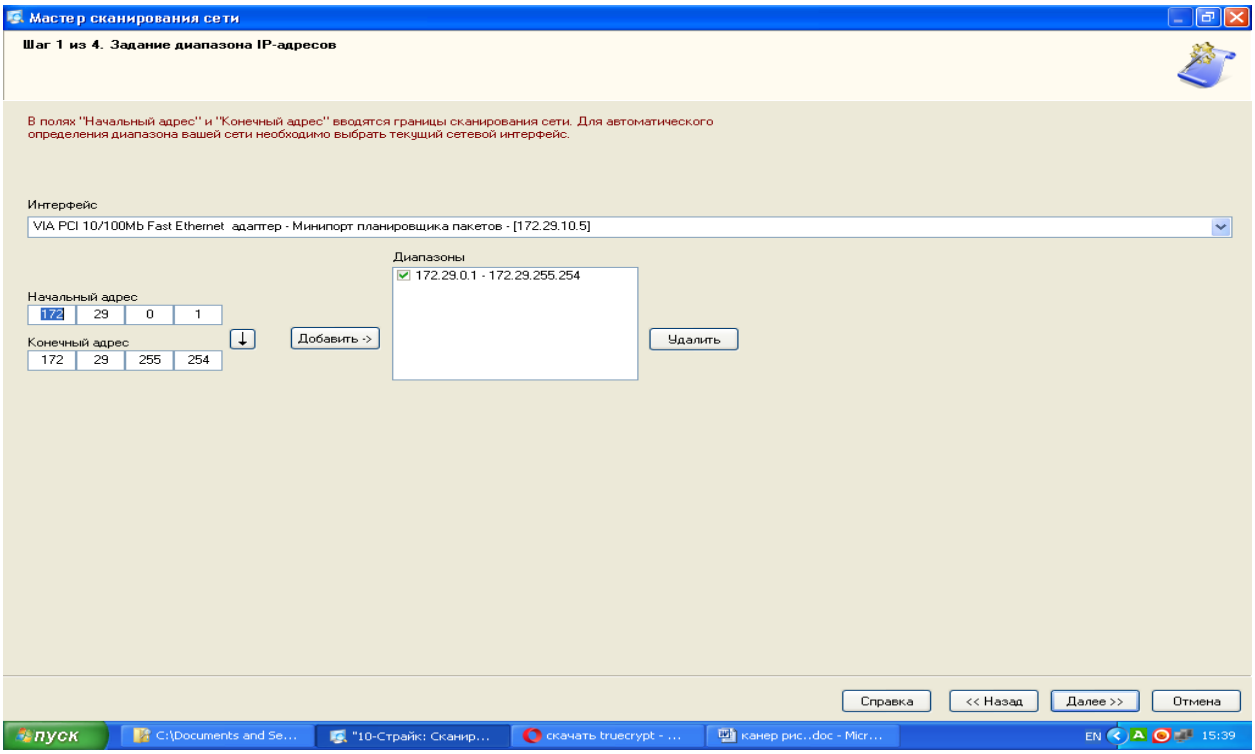


Рис. 2 Вікно задання діапазону **Ір-Адрес**

На першому кроці задаються діапазони сканування. Процедура виконується в кілька етапів:

1. У полях **Початкова адреса** й **Кінцева адреса** вводяться границі сканування мережі. Для автоматичного визначення діапазону можливих адрес вашої мережі необхідно вибрати поточний мережевий **Інтерфейс**.

2. Після заповнення полів адреси необхідно нажати кнопку **Додати** ->, після чого обраний діапазон занесеться в список скануємих діапазонів. **Вилучити** діапазон зі списку можна натисканням відповідної кнопки. Для того, щоб діапазони в списку були просканові, необхідно виділити їх галочкою.

3. Нажати кнопку **Далі** >>.

4. Крок 2. Завдання способу й параметрів сканування (рис. 3).

Майстер надає для вибору 3 способи пошуку пристроїв у мережі:

- **ICMP-Пінг**;

Параметр **Кількість пакетів** відповідає за число ICMP-Пакетів, що відправляються програмою за кожною скануємою адресою. У мережах з високим трафіком одного пакета може бути недостатньо для одержання відгуку від існуючого хоста. У цьому випадку рекомендується задавати не менш 3-4 пакетів.

- **сканування списку TCP-Портів**;

Для сканування TCP-Портів необхідно задати **список портів**, за якими пристрої можуть бути знайдені в мережі. Найпоширенішими відкритими портами в мережах Microsoft є 139 (Netbios), 21 (FTP), 80 (HTTP).

ВАЖЛИВО! При виборі методу сканування портів необхідно враховувати, що ваші дії в більшості випадків можуть розцінюватися брандмауерами як атака й спричинити відповідні наслідки.

Крім цього, ОС Windows XP і вище не дозволяють одночасного сканування групи Tcp-Портів і на рівні драйверів штучно гальмують процес .

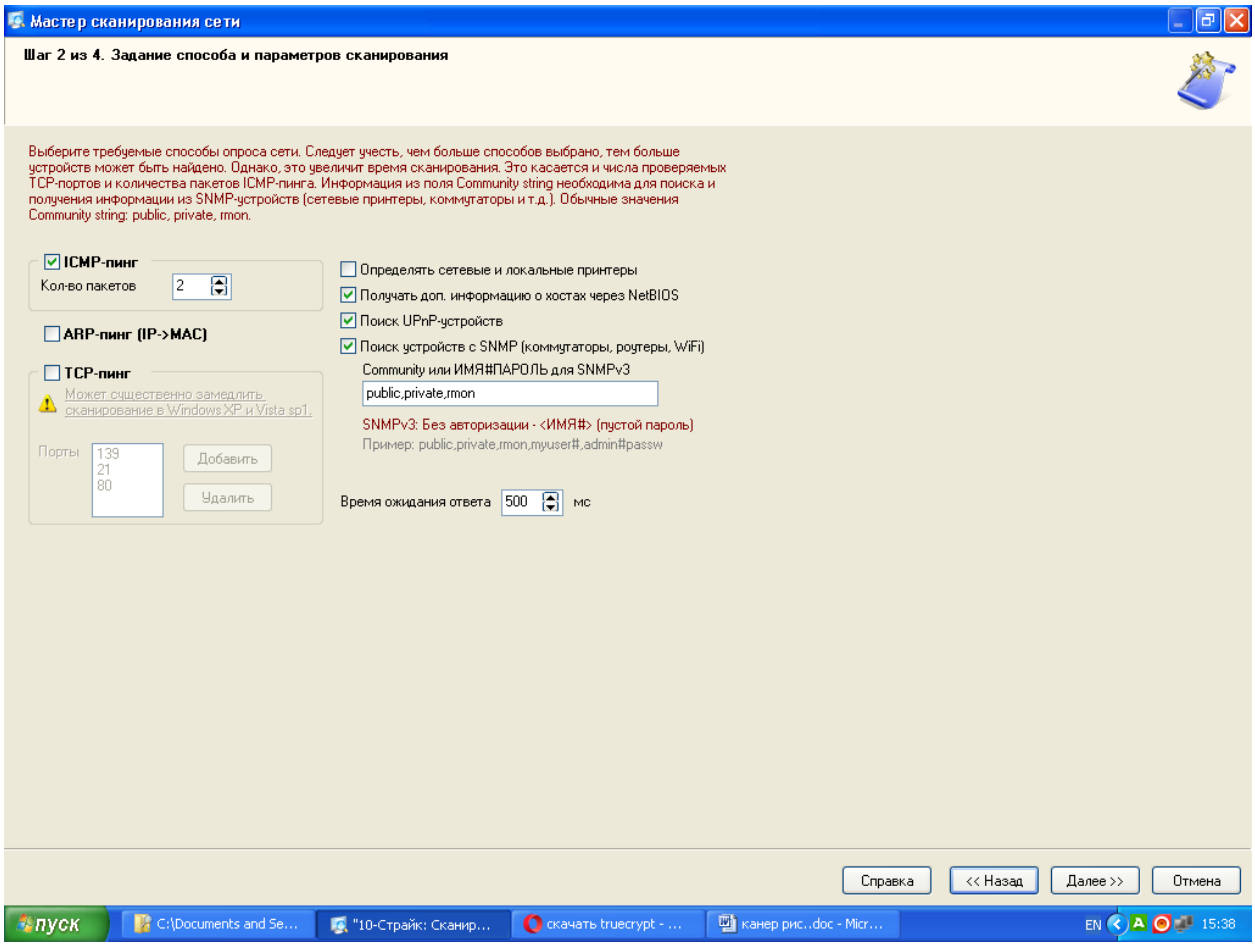


Рис. 3 Завдання способу й параметрів сканування

- **ARP-Пінг (IP->MAC)** .

ARP-Запити полягають у спробі визначення Mac-Адреси хоста за його Ip-Адресою. Якщо Mac-Адреса може бути отримана, Майстер поміщає даний хост у список результатів пошуку. Існує ймовірність, що програма може знайти неіснуючі хости. Справа в тому, що на комутаторі, в адресній таблиці можуть залишатися застарілі або зарезервовані записи. У цьому випадку, слід просто зняти з них галочки у вікні результатів.

Для всіх способів сканування необхідно задати **Час очікування відповіді** - час, у плині якого Майстер буде чекати відповідь від хоста, що сканується.

Якщо у вашій мережі є сервери друку або **мережеві принтери**, можна задати їхній пошук. Функція також може знайти локально-підключені до комп'ютерів принтери.

Майстер може автоматично знайти всі сервера, сервера БД у мережі, одержати іншу корисну інформацію про знайдені комп'ютери (тип ОС, коментар і т.д.). Для цього необхідно вибрати опцію **Одержувати дод. інформацію через Netbios**. Функція буде працювати тільки в тому випадку, якщо протокол Netbios дозволений політикою безпеки на вашім комп'ютері й комп'ютерах вашої мережі.

Якщо у вашій мережі є пристрої, на яких активний SNMP-Агент, то Майстер проінформує вас про це, відобразить опис цих пристроїв. Наявність активного SNMP-Агента допомагає Майстрові визначати більш широкий спектр типів пристроїв. Так, наприклад, по отриманій за **SNMP** інформації Майстер може ідентифікувати комутатори (switch), хаби, роутери, принтери, Wifi крапки доступу, радіороутери і т.д. При пошуку пристроїв з активним SNMP -Агентом, Майстер намагається підключитися до чергової адреси, використовуючи задані імена співтовариств (**Community**). Ці імена можуть бути

перераховані через кому в поле **Community strings**. Найпоширенішими іменами, що задаються за ***замовчуванням, співтовариств, є public***, private, rmon. Якщо ви впевнені, що на ваших пристроях задані інші імена, необхідно вказати їх у списку.

Після завдання всіх параметрів, Майстер переходить безпосередньо до сканування мережі. Для перехід до кроку сканування мережі потрібно нажати кнопку **Далі >>**.

5. Крок 3. Пошук і відбір комп'ютерів для приміщення в список.

Процес сканування стартує негайно. Спочатку здійснюється спроба виявлення мережевих і локальних принтерів. Ця процедура може забирати тривалий час, протягом якого програма може не відповідати на запити й буде недоступної кнопка **Зупинити**. Після цього проводиться пошук пристроїв за Netbios, що також може зайняти якийсь час. Після виконання двох підготовчих процедур, програма починає безпосередній перебір усіх Ip-Адрес заданих діапазонів. Про хід процесу сигналізує індикатор прогресу й напис у нижньому лівому куті Майстра - **"Сканування діапазону адрес..."**.

Хід процесу сканування можна зупинити, нажавши кнопку **Зупинити**.

Знайдені в процесі сканування хости поміщаються в список результатів. Існує можливість зміни типу знайденого пристрою прямо з вікна результатів. Для цього необхідно виділити необхідний запис (допускається множинний вибір) і викликати контекстне меню. У цьому меню необхідно вибрати встановлюваний тип пристрою.

Для того, що б помістити в список хостів не всі знайдені пристрої, пропонується відзначити бажані пристрої галочками. Кнопки **Відзначити всі**, **Виділені**, **Інвертувати** допомагають проводити множинний вибір пристроїв. Можна оперативно вивантажити всю отриману інформацію в CSV-**Файл**. При цьому, у звіт будуть поміщені й параметри сканування мережі. Для вивантаження інформації необхідно нажати кнопку **Звіт**.

Даний звіт може допомогти розроблювачам програми, якщо ви зіштовхнетеся із проблемами формування списку хостів мережі.

Після завершення процесу сканування потрібно перейти на завершальний крок, нажавши кнопку **Далі >>**.

6. Крок 4. Розміщення хостів у списку (рис. 4).

Перед поміщенням знайдених хостів у список можна задати додаткові параметри:

- Можна вказати, що **використовувати в якості імені (адреси) хоста** - Ip-Адресу пристрою або його DNS-Ім'я. Для мереж, з динамічним розподілом Ip-Адрес необхідно вибрати DNS -Ім'я, тому що цей атрибут у цьому випадку буде постійним. У мережах зі статичними Ip-Адресами можна вказати в якості імені Ip-Адреса пристрою.
- **Відкидати DNS -Суфікс в імені хоста** . У якості імені хоста Майстер може використовувати певні Dns-Імена пристроїв. Часто, такі імена мають суфікс, наприклад: *mary.dep1.orgname.com*. При виборі даного параметра ім'я хоста буде *mary*.

Для додавання тільки нових хостів, яких ще немає в списку, включіть відповідний параметр.

Після натискання кнопки **Готово** знайдені хости поміщаються в список (рис. 5).

1.4 Робота зі списком хостів

Додавання хоста

Для додавання нового хоста в список необхідно виконати наступні дії:

1. Вибрати пункт головного меню **Хости | Додати хост**;

3. У вікні, що з'явилося, увести необхідні параметри. Обов'язковим параметром є **Ім'я або адреса хоста**;

Опис параметрів хоста:

Ім'я або адреса хоста Ім'я комп'ютера в мережі або його Ip-Адреса. Значення даного поля є вхідним параметром для функцій програми.

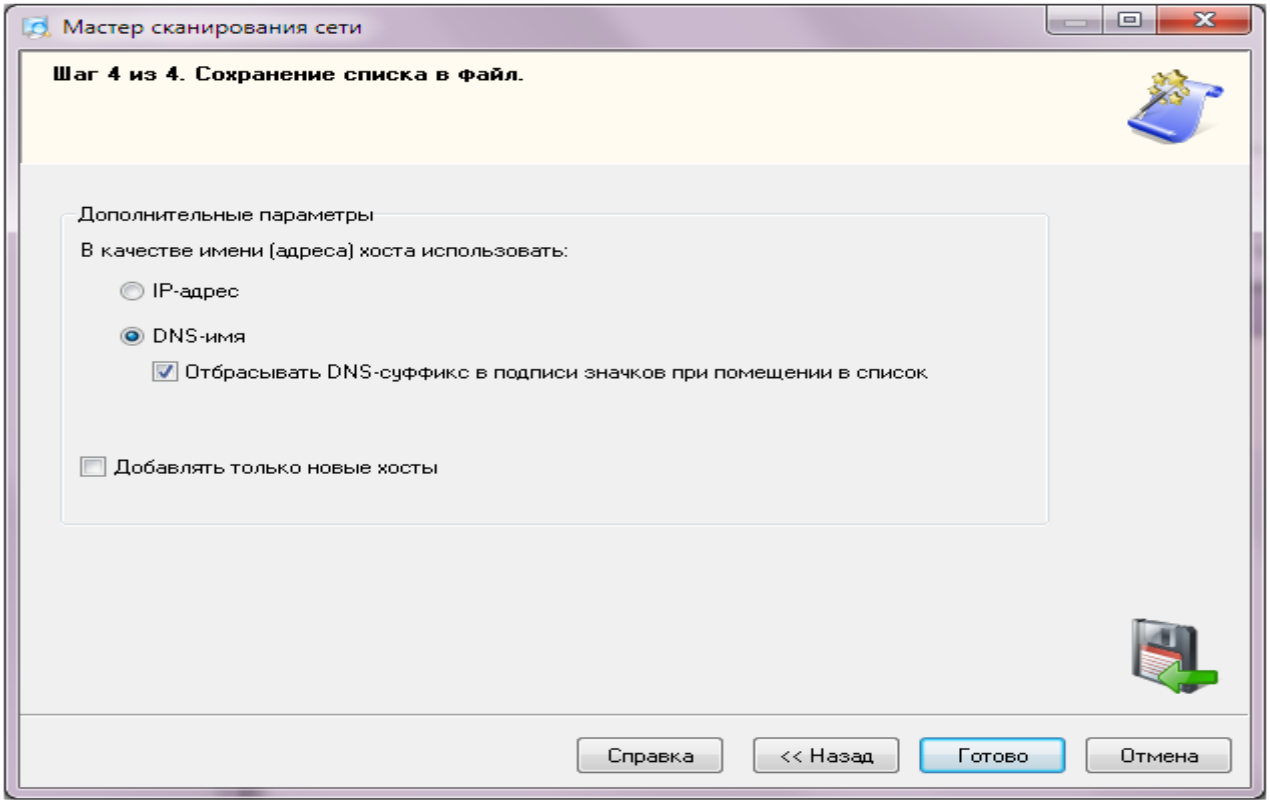


Рис. 4 Вікно налагодження програми

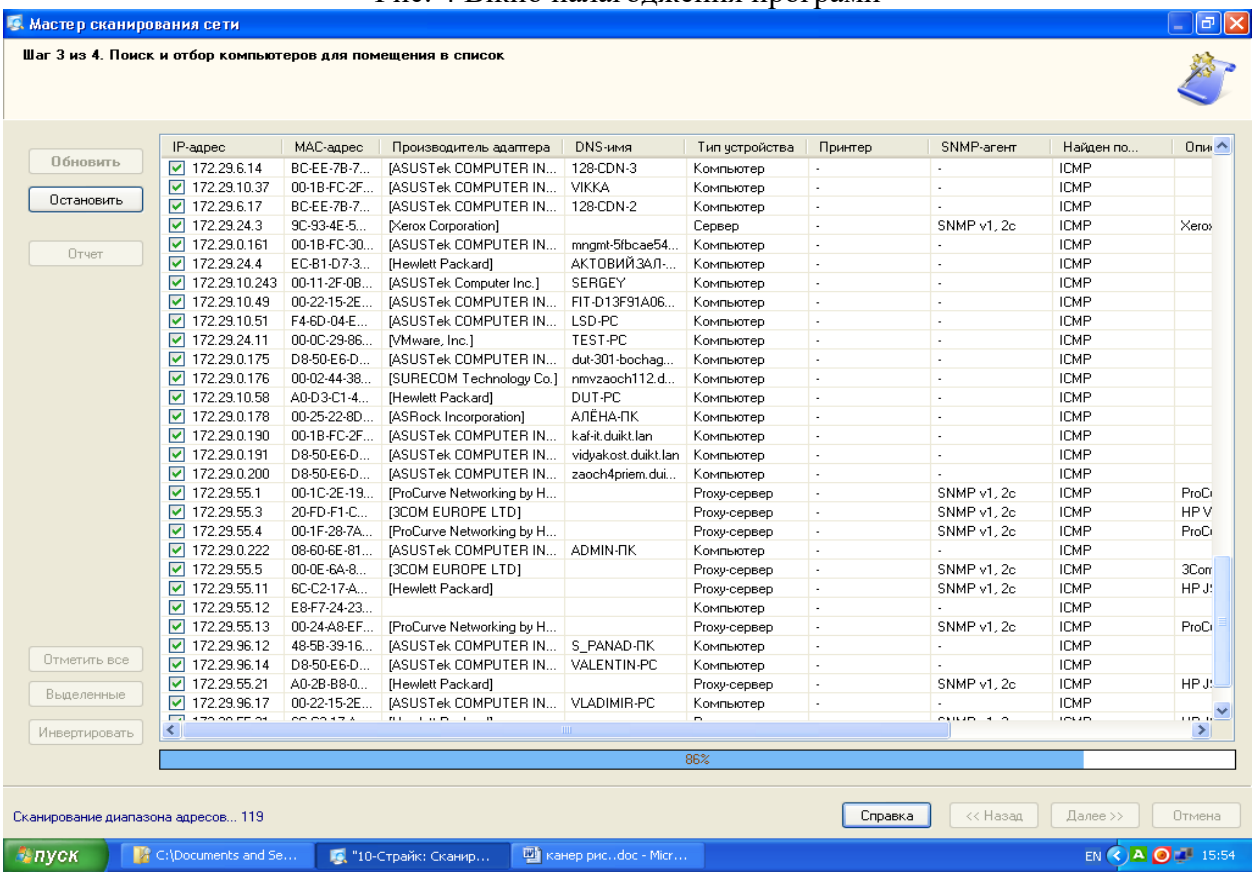


Рис. 5 Розміщення хостів у списку

Назва в списку За замовчуванням, у якості назви хоста в списку виступає його адреса або мережеве ім'я. Його можна змінити, задавши будь-яке бажане ім'я в цьому полі.

Тип Тип пристрою служить для візуального поділу хостів у списку. Кожний тип супроводжується умовним значком-піктограмою.

Мас-Адреса Для успішної роботи функції включення комп'ютера по мережі (Wake on LAN) необхідно для кожного хоста один раз задати Мас-Адресу мережевого адаптера (рис. 6). Мас-Адреса можна одержати автоматично у включених хостів, або ввести її вручну.

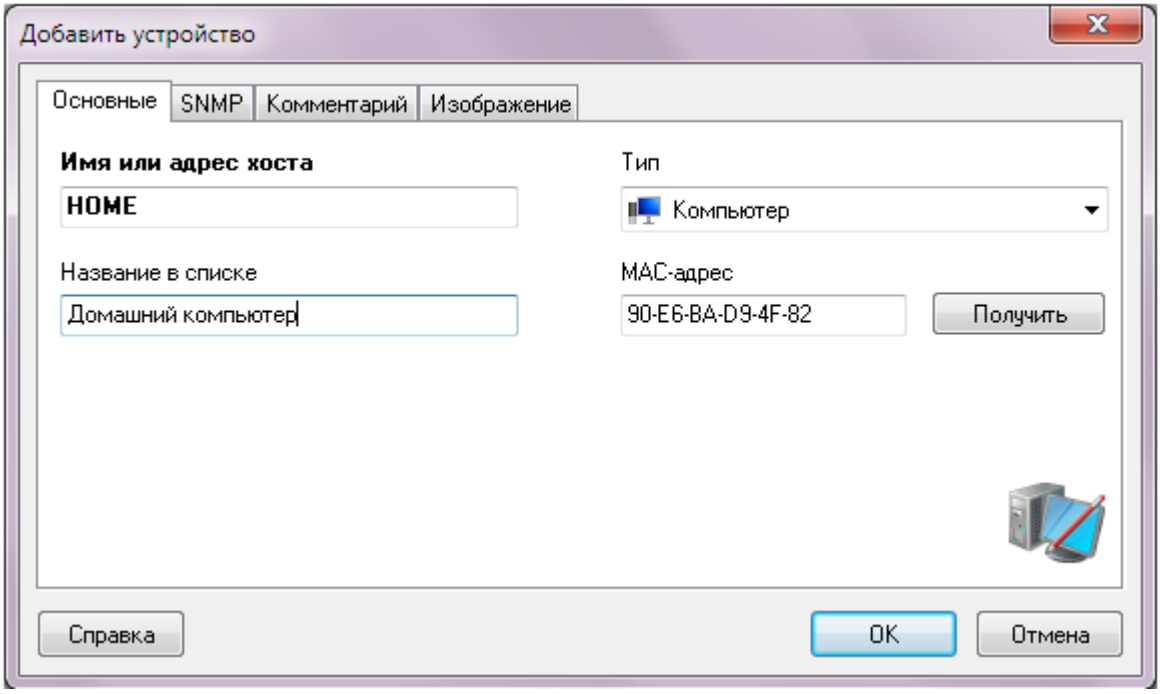


Рис. 6 Введення **Мас-Адреси**

SNMP **Для одержання SNMP-Інформації про хост необхідно знати його** Community**. Можна задати цей параметр, включивши галочку** Агент є (рис. 7)**. Уведене значення буде автоматично підставлятися там, де це необхідно.**

Коментар: Кожний хост можна супроводити користувацьким коментарем. У цьому полі можна зберігати інформацію про користувача комп'ютера, складові його системи, список ПЗ і т.д. Для зручності й швидкості введення коментаря передбачений механізм вибору атрибутів зі списку. Список атрибутів може бути доповнений (рис. 8).

Зображення **Кожному хосту можна прив'язати яке-небудь зображення, яке допоможе простіше й швидше ідентифікувати його (фото користувача, приміщення і т.д.). Включіть галочку** Файл зображення **(рис. 9) й виберіть його файл.**

Після завдання параметрів потрібно нажати кнопку **ОК**. Новий хост поміститься в список. Збереження нової інформації у файл відбувається автоматично.

Зміна параметрів хоста

Для зміни параметрів хоста необхідно виконати наступні дії:

1. Виділити в списку хост;

2. Викликати контекстне меню, вибрати пункт **Змінити хост**;

3. Змінити необхідні параметри у вікні, що з'явилося. Нажати кнопку **ОК** для збереження змін.

Зміни зберігаються у файлі й набувають чинності негайно.

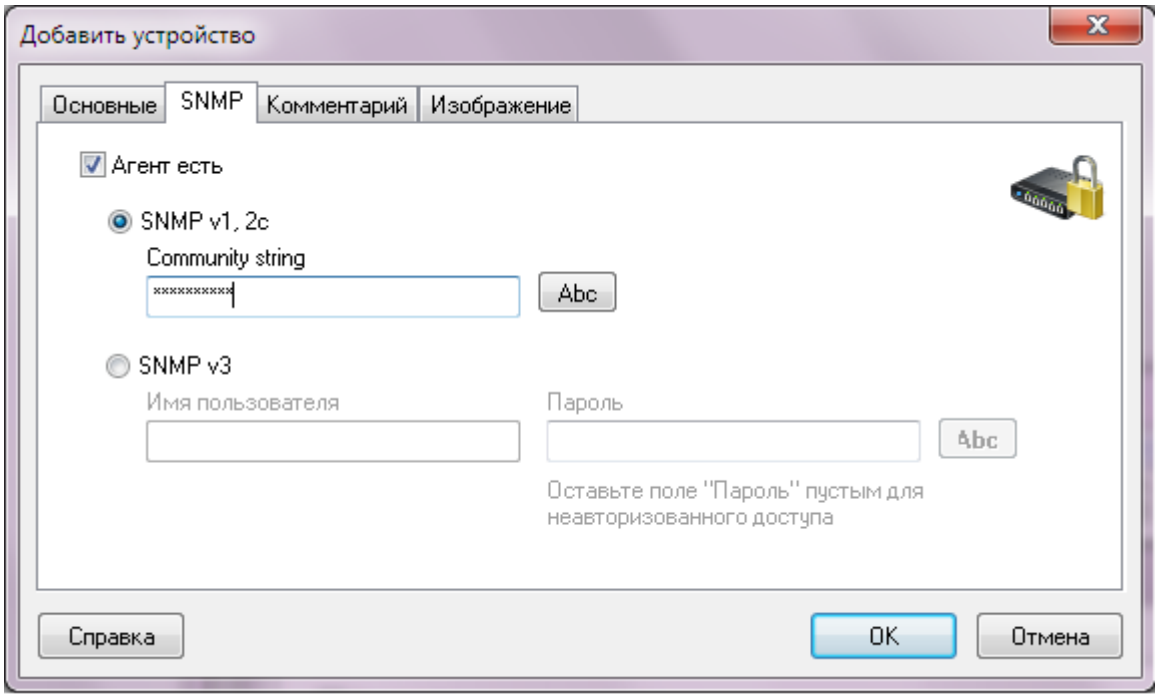


Рис. 7 Вікно **SNMP**

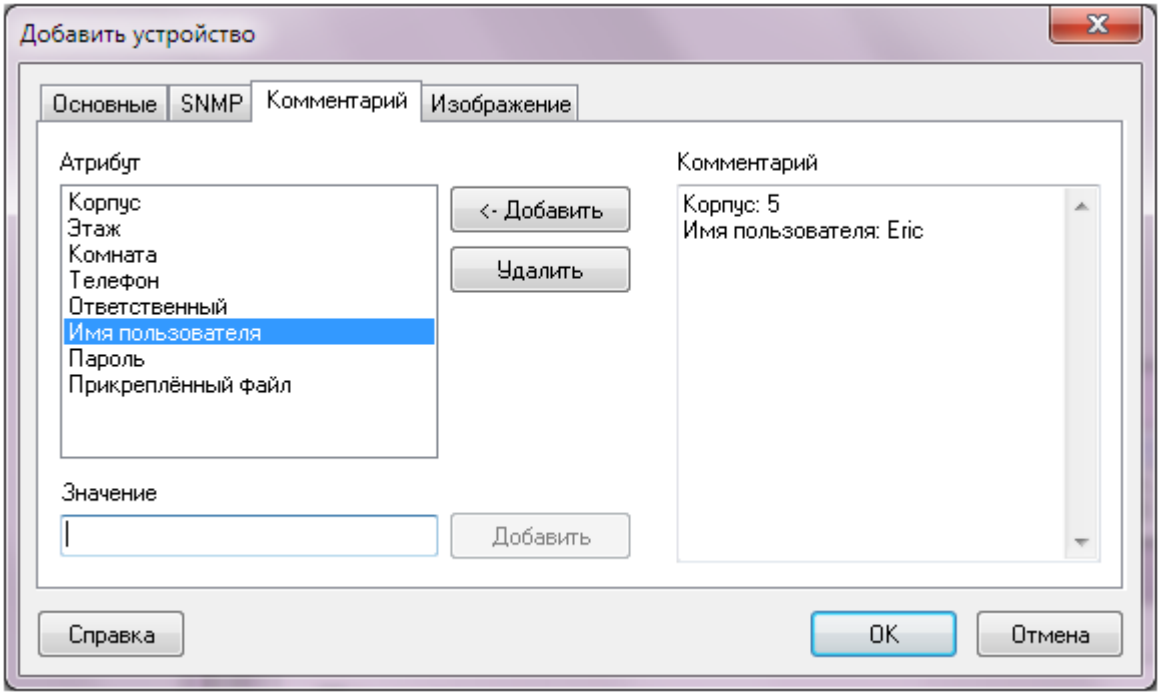


Рис. 8 Вікно коментарів

1.5 Видалення хоста

Для видалення хоста необхідно виконати наступні дії:

1. Виділити в списку хост;

2. Викликати контекстне меню, вибрати пункт **Вилучити хост**. Підтвердити дію, нажавши кнопку **Так** у запиті, що з'явився;

Обраний хост віддаляється зі списку й файлу.

1.5 Завершення роботи віддаленого комп'ютера

При відповідних правах у мережі ви можете завершити роботу віддаленого комп'ютера.

При цьому можливі наступні варіанти:

- Виключити комп'ютер, при цьому програми з незбереженими даними запросять підтвердження на вихід без збереження;
- Виключити комп'ютер, ігноруючи незбережені дані;
- Перезавантажити комп'ютер;
- Скасувати операцію завершення роботи, якщо час затримки перевищує 0 секунд. Після закінчення заданого часу скасування операції буде неможливе.

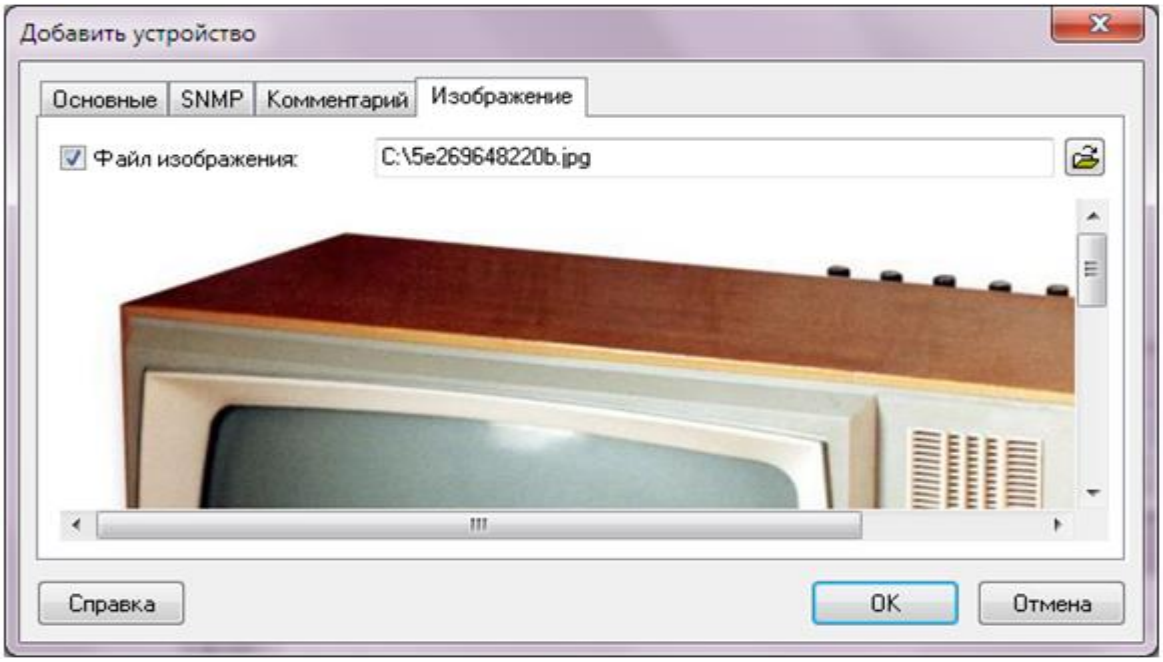


Рис. 9 Вікно відбору зображення

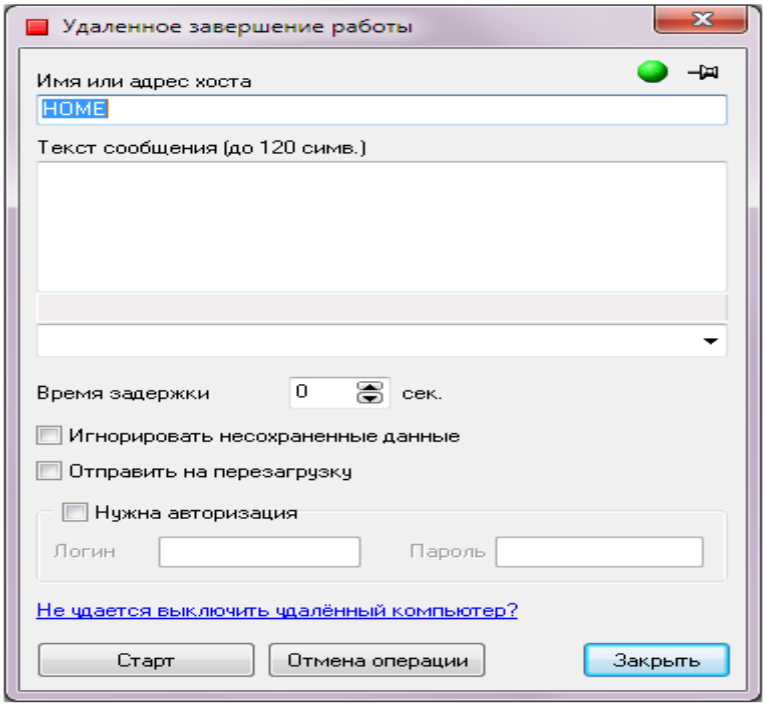


Рис. 10 Вікно управління віддаленим ПК

Можна завершити роботу відразу декількох комп'ютерів. Для цього необхідно перелічити в полі **Ім'я комп'ютера** імена комп'ютерів, що вимикаються, розділяючи їх символом ";". Після натискання кнопки **Старт** в, список будуть додаватися найменування й результати виконуваних операцій.

Якщо користувач, під яким працює програма, не має прав адміністратора на комп'ютері, що вимикається, то для успішного виконання вимикання або перезавантаження необхідно задати ім'я й пароль користувача з необхідними повноваженнями. Для завдання імені й пароля необхідно включити параметр **Потрібна авторизація** й заповнити поля **Логін** і **Пароль**.

Перед завершенням роботи на екран віддаленого комп'ютера буде виведене повідомлення, яка інформує про завершення роботи й залишок часу перед цим (рис. 11). Також, у це повідомлення можна додати будь-який текст (поле **Текст повідомлення**). У рядку стану буде відображатися повідомлення про залишок часу до виконання операції.

Якщо мережеві адаптери й BIOS'и ваших машин підтримують функцію **Wakeuponlan**, то ви можете за певних умов включати комп'ютери по мережі.

Для успішного виконання цієї функції повинні бути дотримано кілька умов:

- Мережевий адаптер повинен бути PCI2.2-compatible, або більш старий, але з кабелем, по якім з материнської плати подається живляча напруга в 5В;
- Режим Wakeonlan повинен підтримуватися й бути включений в Biose (Wakeon - Netcard);
- Комп'ютер попередньо повинен бути "правильно" виключений - це називається "Soft-Off", лампочки на клавіатурі й мережевій карті повинні горіти.

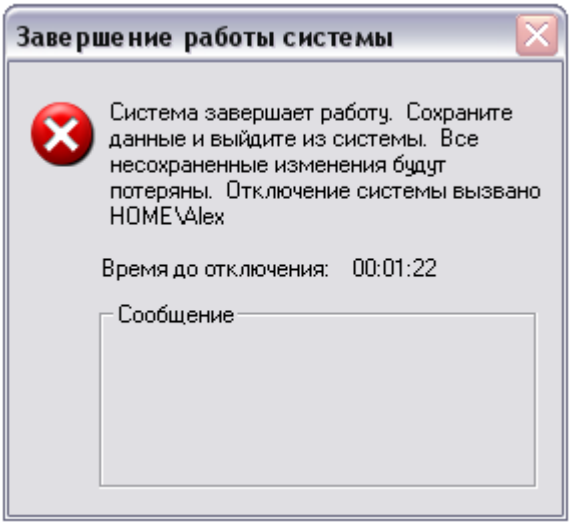


Рис. 11 Вікно попередження

1.6 Включення комп'ютерів за мережею

Для включення по мережі одного або декількох комп'ютерів необхідно виділити їх у списку й вибрати пункт контекстного меню **Включити/Виключити | Включити.** У вікні нажати кнопку **Старт**. Після цього всім комп'ютерам, у яких визначилася Mac-Адреса, буде відправлений сигнал на включення. Для відправлення цього сигналу необхідно, щоб ваш firewall пропускав вихідні UDP-Пакети.

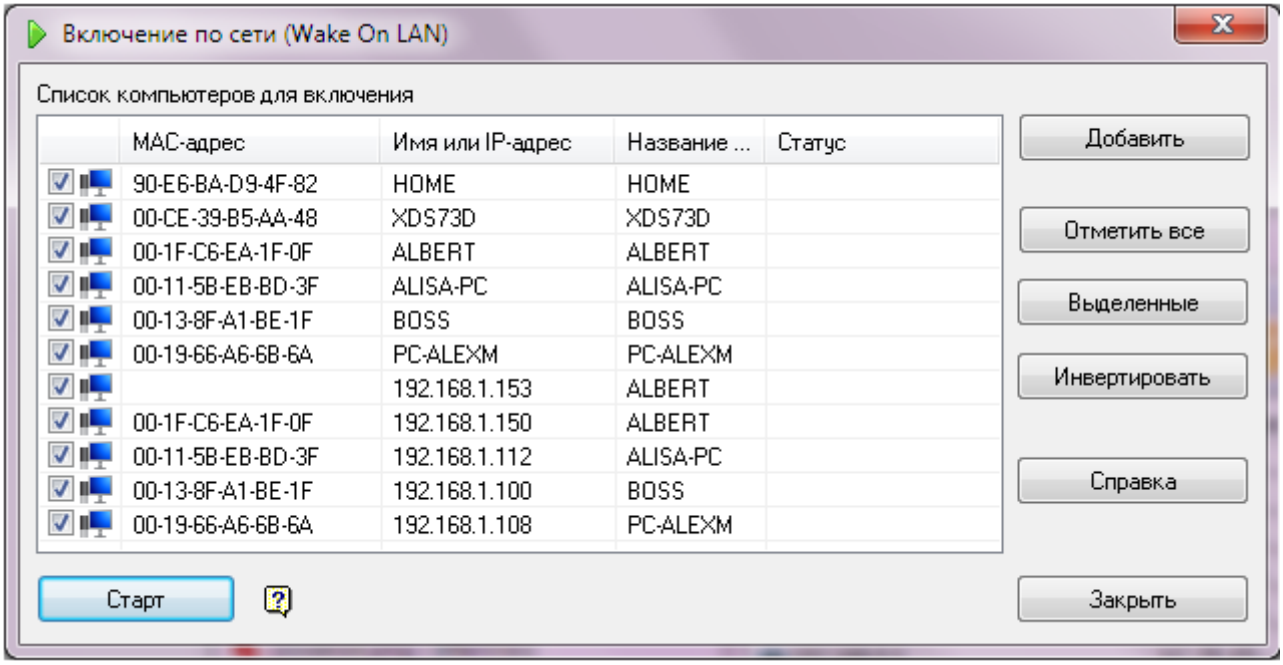


Рис. 12 Вікно включення ПК

Тому що для доставки пакета-сигналу на включення використовується протокол UDP, немає гарантії, що комп'ютер обов'язково одержить цей сигнал і ввімкнеться. Якщо таке відбулося, необхідно повторити процедуру включення ще раз.

1.7 Інформація про систему

У вікні **Інформація про систему** зібрані відомості про віддалену машину. Якщо користувач, під яким працює програма, не має прав адміністратора на віддаленому комп'ютері, то для успішного одержання інформації про журнал подій, списку процесів, установлених програм, керування службами й реєстром, необхідно задати ім'я й пароль користувача з необхідними повноваженнями. Для встановлення з'єднання з віддаленим комп'ютером від імені адміністратора необхідно нажати кнопку на панелі інструментів (рис. 13) із зеленою піктограмою або викликати пункт головного меню **Сервіс | Підключитися з логіном і паролем...**, у діалоговім вікні, що з'явилося, увести ім'я й пароль, нажати **кнопку** ОК. У випадку успішного підключення програма видасть відповідне повідомлення, або повідомлення про помилку. Після встановлення з'єднання всі запити по одержанню або зміні інформації на віддаленому комп'ютері будуть іти від цього користувача. По завершенню роботи з інформацією віддаленого комп'ютера необхідно розірвати з'єднання (з метою безпеки, тому що їм можуть скористатися інші програми), нажавши кнопку із червоною піктограмою, або викликавши пункт головного меню **Сервіс | Розірвати з'єднання.**

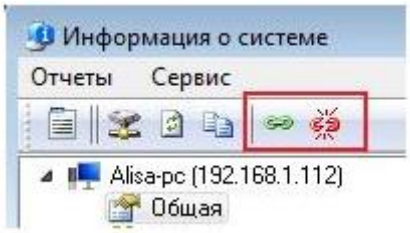


Рис. 13 Панель інструментів

Ви можете скопіювати отриману в розділах інформацію в буфер, а потім вставити в будь-який текстовий файл або аркуш Microsoft Excel. Для цього викличте контекстне меню списку властивостей і виберіть пункт **Копіювати в буфер**.

Загальна інформація

У цьому розділі відображається узагальнена інформація про віддалений комп'ютер: Ip-Адреси, Dns-Ім'я, Mac-Адреси адаптерів, їх виробники користувач, домен/робоча група, сервер, тип операційної системи установки, , дата й час, час роботи без перезавантаження, список дисків (рис.14).

Одержання деяких властивостей віддаленого комп'ютера займає якийсь час, тому можлива затримка (тривалість - від 0 до 20 сек., залежно від розташування комп'ютера в мережі і її швидкодії).

Частина властивостей може виявитися недоступною з ряду причин, пов'язаних з організацією мережі й правами користувача.

Якщо в системі встановлено кілька мережевих адаптерів (фізичних або віртуальних), то будуть знайдені всі їх IP і Mac-Адреси.

Для одержання додаткової інформації про домен натисніть ярлик біля імені домена.

Для одержання списку дисків віддаленого комп'ютера потрібні права адміністратора домена (роб.групи).

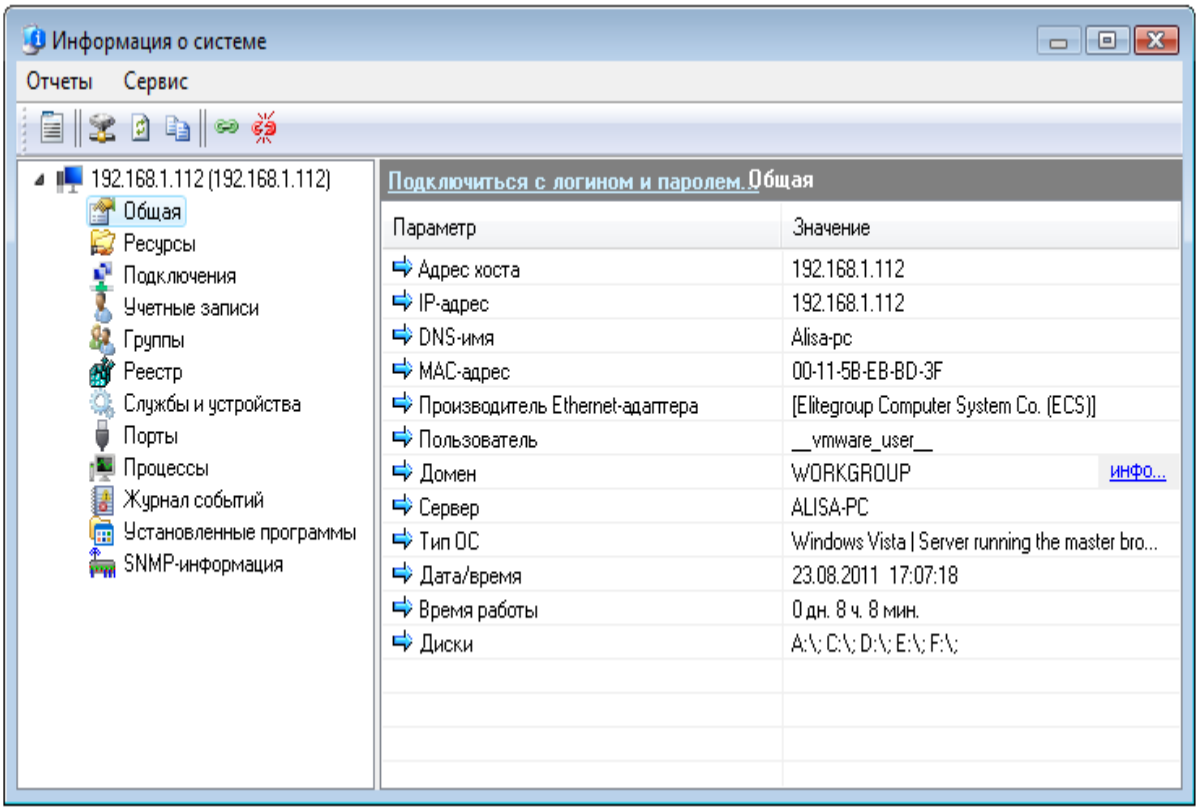


Рис. 14 Інформація про систему

Ресурси

У цьому розділі ви можете подивитися список відкритих ресурсів віддаленої машини (рис. 15). У списку можуть бути показані й так звані сховані ресурси (зі значком $). Зі списку ресурсів ви можете легко відкрити їх у Провіднику (подвійним кличем миші на рядку).

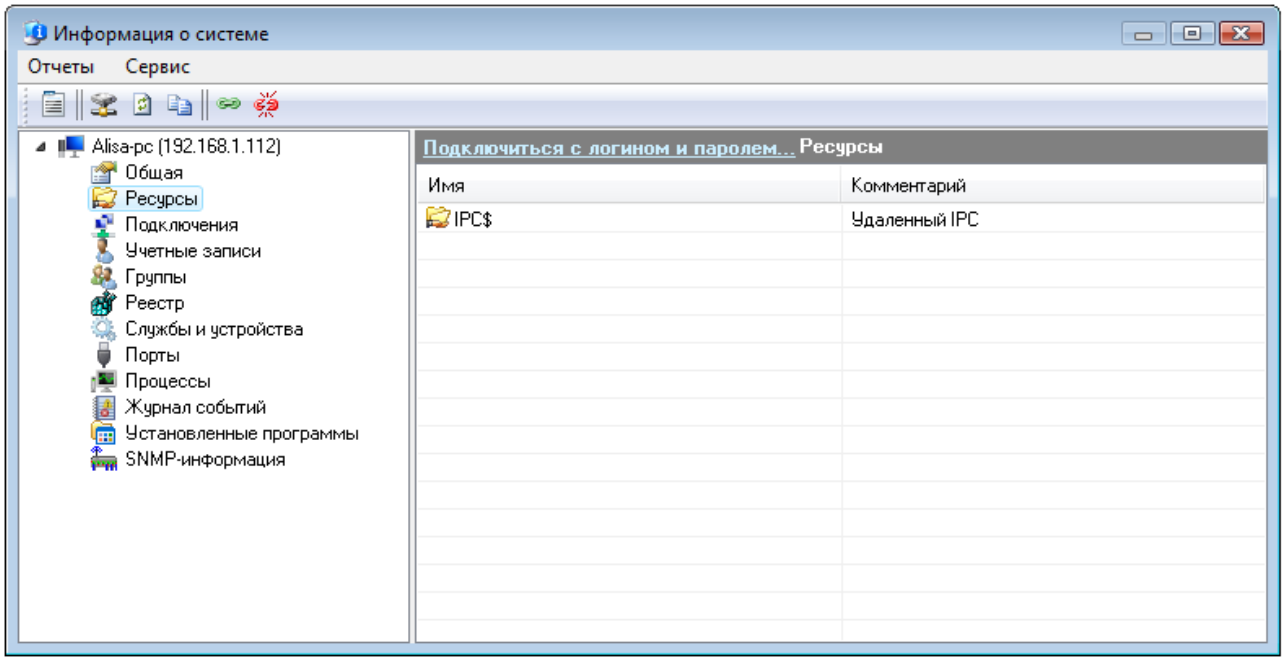


Рис.15 Список ресурсів віддаленого ПК

Для підключення мережевого диска виділіть ресурс у списку й виберіть пункт контекстного меню **Підключити мережевий диск...** Після підключення диска, автоматично відкривається вікно провідника.

Підключення

У цьому розділі ви можете одержати інформацію про поточні підключення до віддаленої машини, або відстежити, хто в цей момент використовує мережеві ресурси на будь-якій машині мережі (рис. 16).

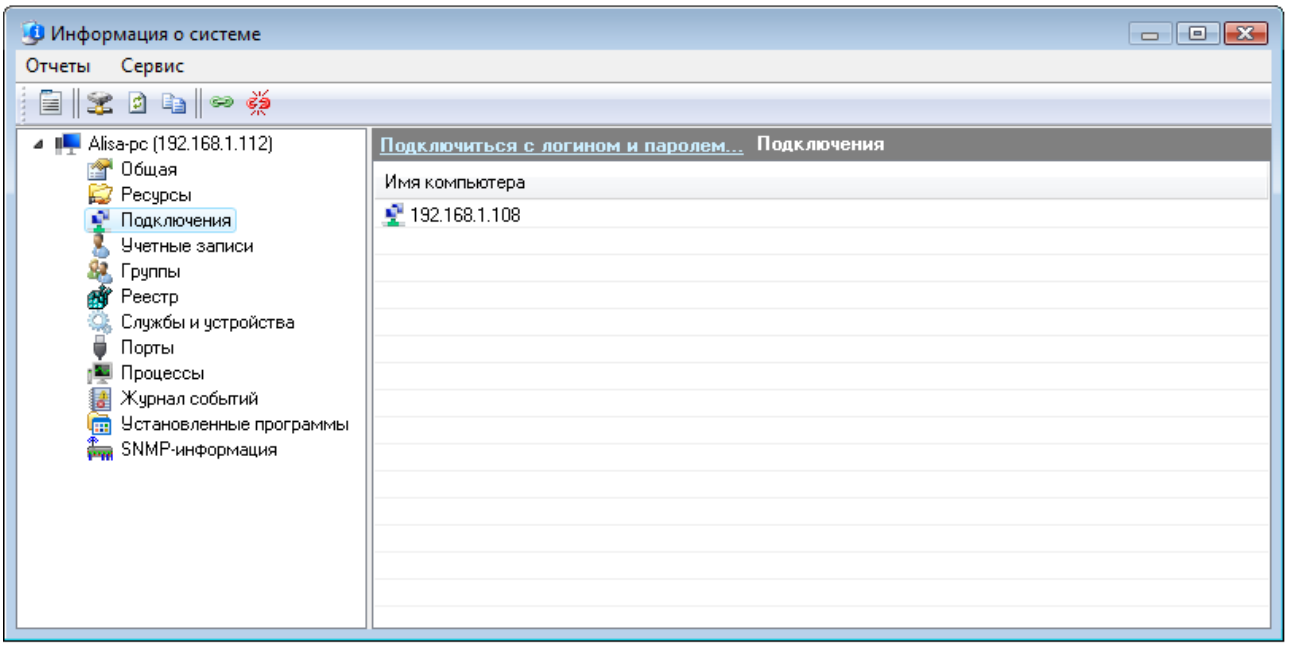


Рис. 16 Вікно підключення на віддаленому ПК

Облікові записи

У цьому розділі ви можете переглянути список облікових записів віддаленої машини (рис. 17) й вибрати тип відображуваних записів (фільтр).

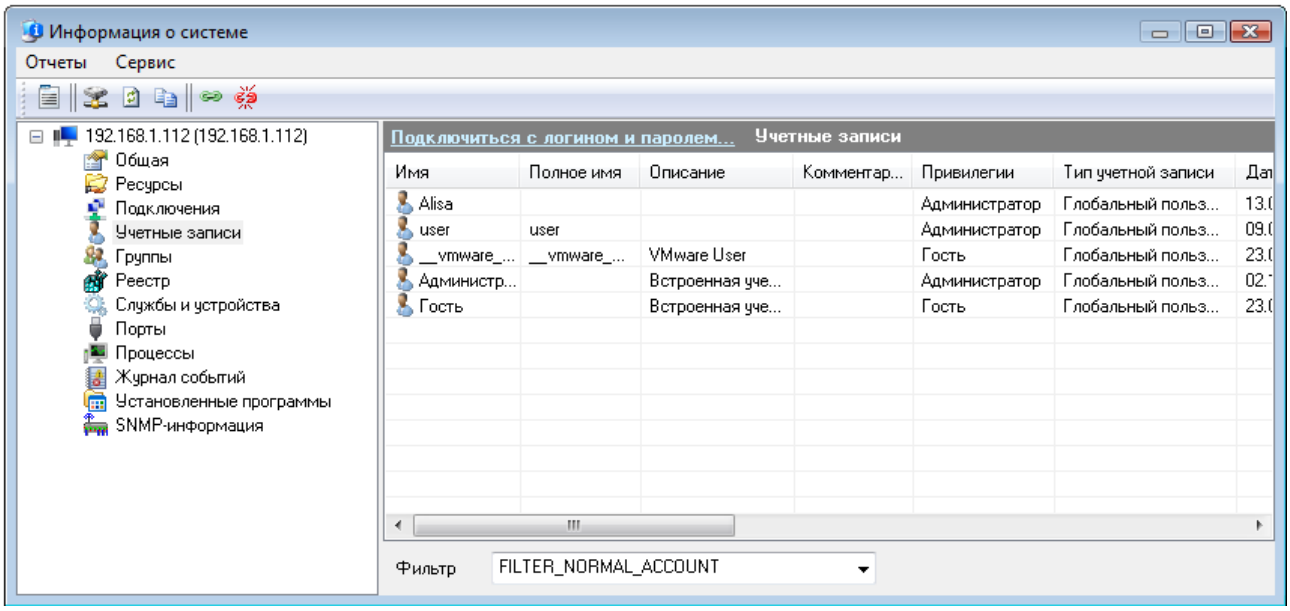


Рис. 17 Вікно облікових записів на віддаленому ПК

Групи

Список локальних і глобальних груп користувачів віддаленої машини (рис. 18).

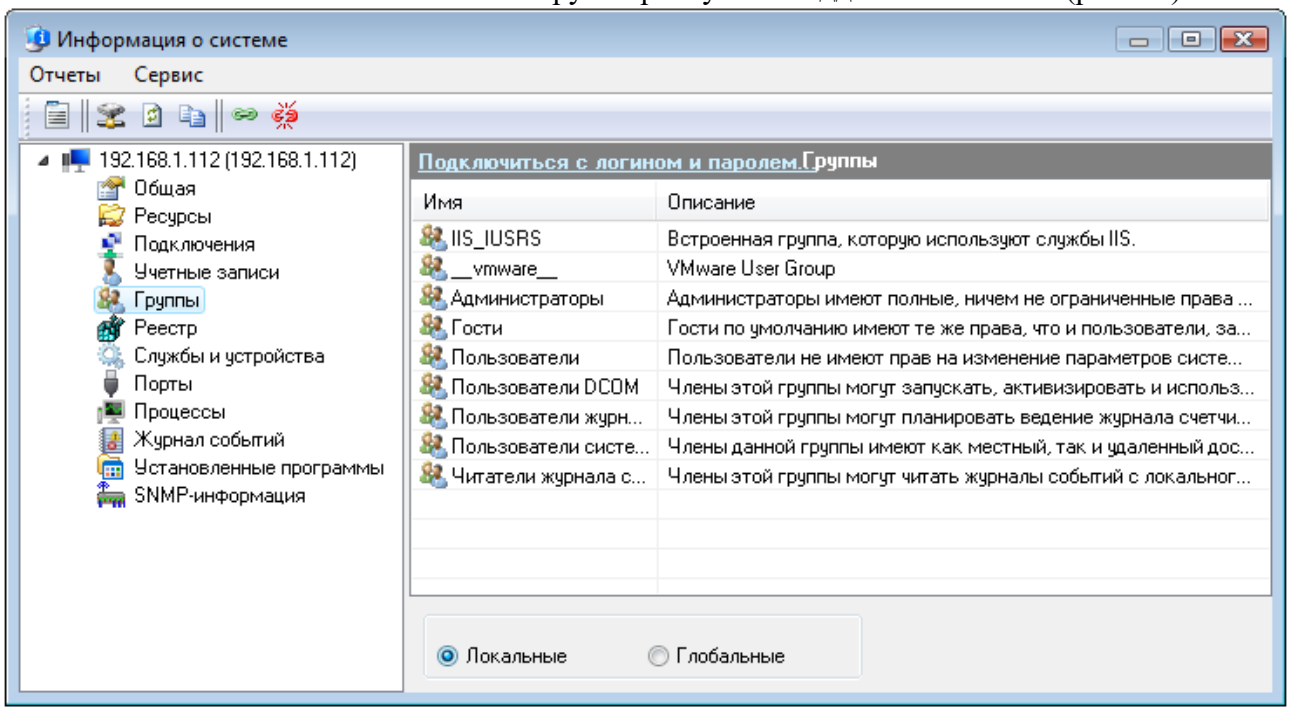


Рис. 18 Список груп користувачів на віддаленому ПК

Реєстр

У цьому розділі ви можете переглядати реєстр на віддаленій машині (рис. 19).

Одержання інформації про зміст реєстру виконується динамічно, через що можлива деяка затримка при розкритті вузлів. Не всі відображувані дерева реєстру можуть бути розкриті, як і не всі розділи можуть бути доступні. Це визначається налагодженням політики безпеки на віддаленій машині.

Через контекстне меню дерева ключів доступне копіювання їх імен у буфер.

По подвійному кличу на виділеному рядку параметра з'являється вікно з полями, у яких відображаються параметр і значення, які також можна скопіювати в буфер.

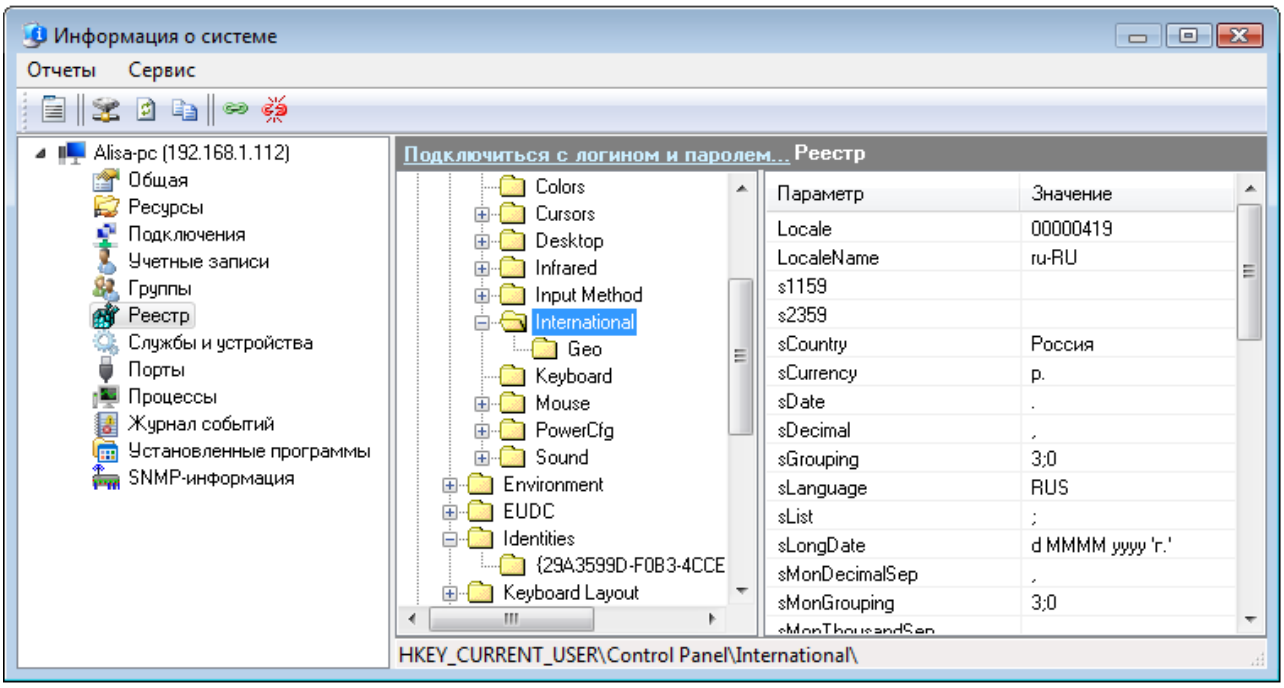


Рис. 19 Реєстр на віддаленому ПК

Через контекстне меню списку параметрів доступна зміна, додавання, видалення параметрів і їх значень. Однак операції зі зміни реєстру віддаленого комп'ютера вимагають повноважень адміністратора..

Служби й пристрої

Програма дозволяє одержати список усіх служб і пристроїв віддаленого комп'ютера (рис. 20). Можна відображати тільки ті служби, тип яких відповідає обраному значенню поля **Тип**. Також можна відображати/не відображати активні/не активні служби (список **Стан**).

При наявності повноважень адміністратора на віддаленому комп'ютері доступне керування службами: пуск, останов, перезапуск. Для керування виділеної в списку службою необхідно вибрати відповідний пункт контекстного меню.

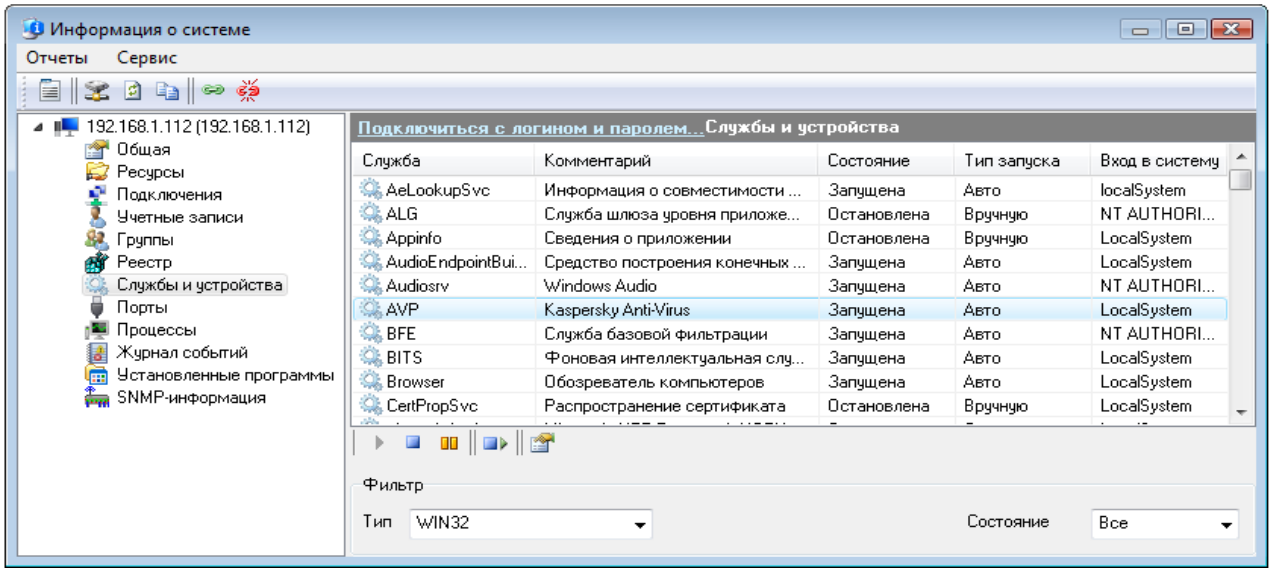


Рис. 20 Служби та пристрої на віддаленому ПК

Порти

За допомогою сканера портів можна одержати інформацію про відкриті порти вашої й віддаленої машини (рис. 21). Функція визначає як TCP, так і UDP порти. Можна вказати інтервал сканування й затримку - час, протягом якого програма буде чекати відповіді від віддаленого комп'ютера.

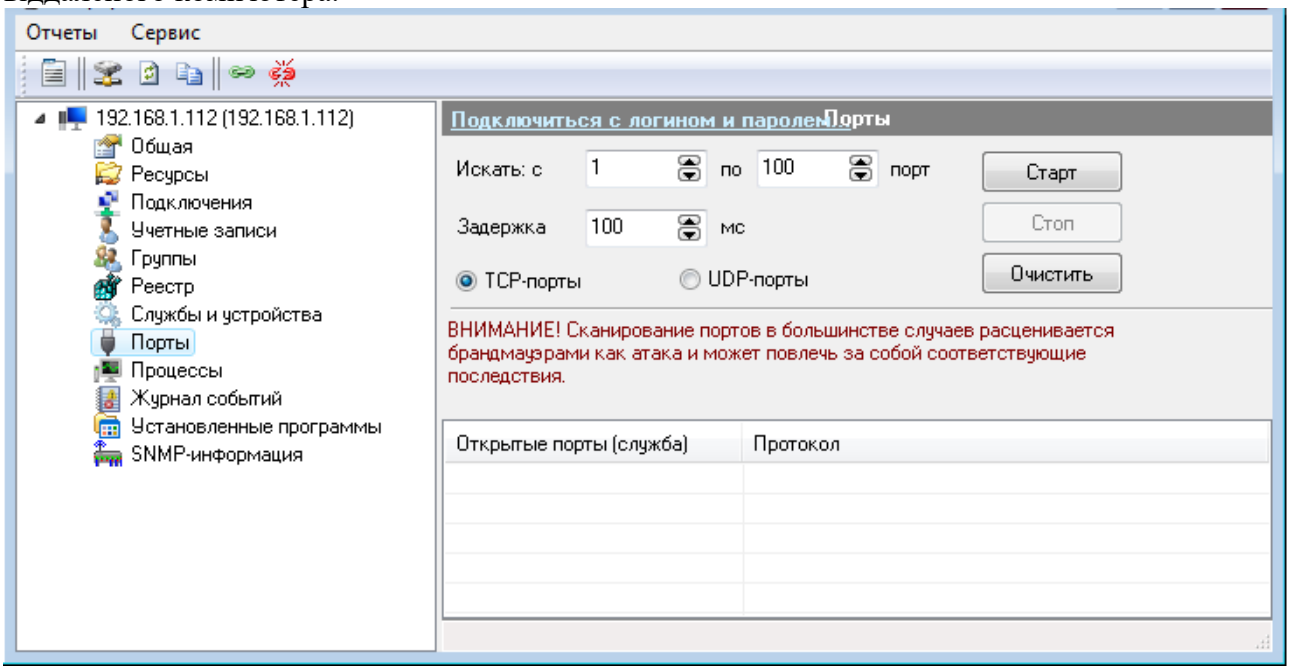


Рис.21 Порти на віддаленому ПК

ВАЖЛИВО!: Сканування портів у більшості випадків розцінюється брандмауерами віддалених хостів як атака, що може викликати відповідні наслідки.

Процеси

У цьому розділі (рис. 22) ви можете подивитися список активних процесів на віддаленій машині.

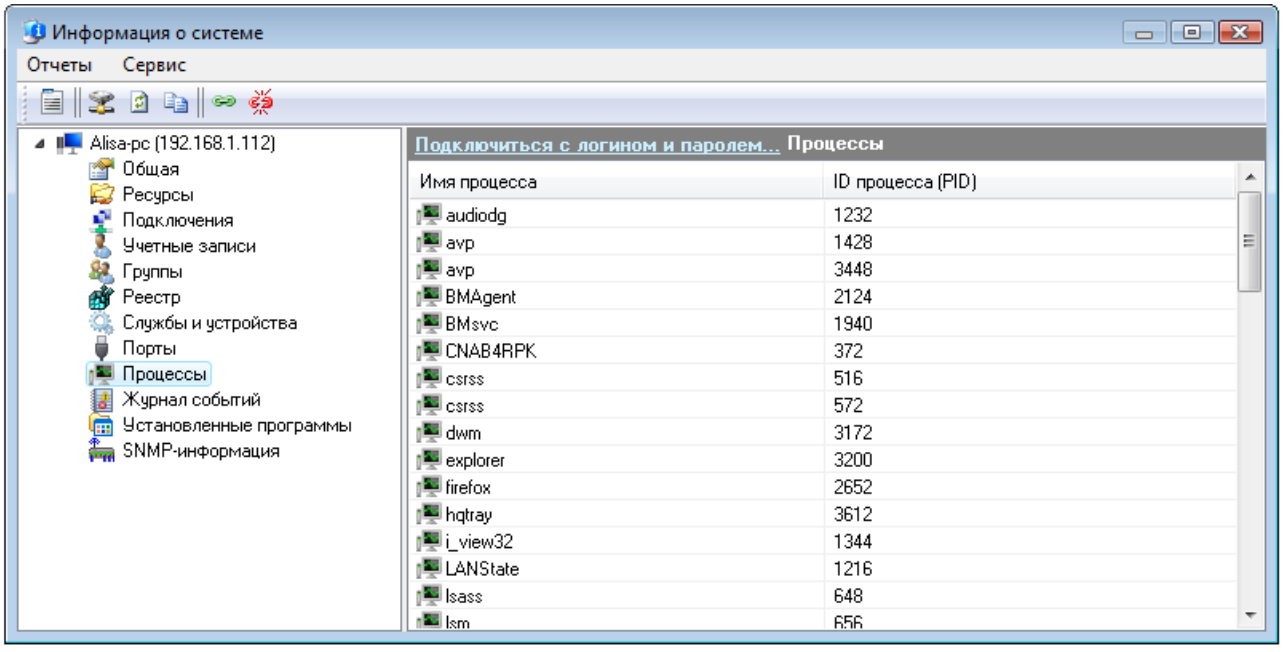


Рис. 22 Процеси на віддаленому ПК

Журнал подій

Програма дозволяє читати журнали подій (рис. 23) з віддалених машин. Доступні журнали системних, прикладних подій і, при певних правах у домені (роб. групі), подій служб безпеки. При цьому доступно докладний опис події (помилки, повідомлення, попередження). Для перегляду події необхідно подвійним клацанням на виділеному записі журналу відкрити вікно **Подія** (рис. 24)**.** Кнопки навігації (продубльовані "гарячими клавішами" Left, Right Arrow) дозволяють швидко переходити до наступного або попередньому запису журналу.

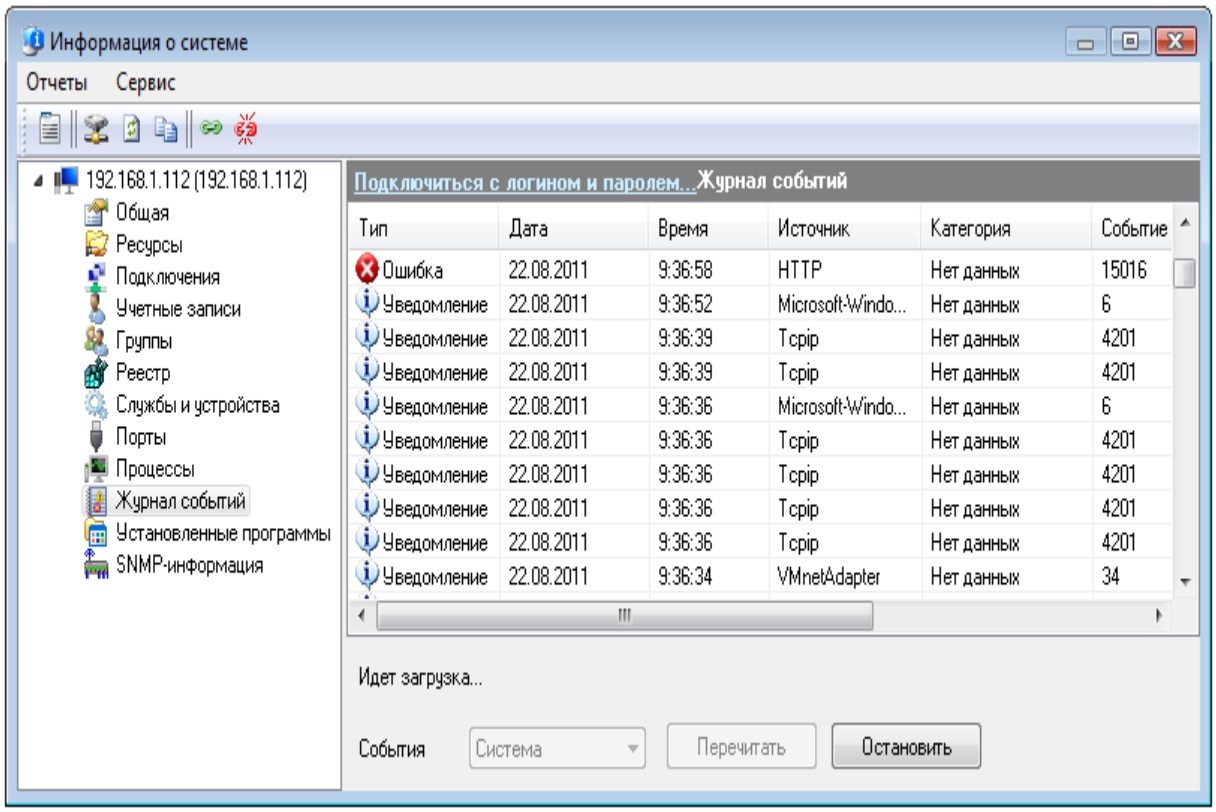


Рис. 23 Журнали на віддаленому ПК

Установлені програми

У цьому розділі ви можете одержати список установлених на віддаленому комп'ютері програм. Для успішної роботи функції необхідно мати:

- Наявність прав адміністратора на віддаленому комп'ютері;
- Запущену на віддаленому комп'ютері службу ***"Вилучене керування реєстром"***.

SNMP- Інформація

Програма може одержувати масу корисної інформації з комутаторів, роутеров і інших мережевих пристроїв, що підтримують SNMP-Протокол. Кожний комп'ютер при наявності активного SNMP-Агента може віддавати програмі інформацію із протоколу SNMP. В операційній системі Windows 2000/XP/2003/Vista SNMP-Агент реалізований у вигляді служби **"Служба SNMP"**.

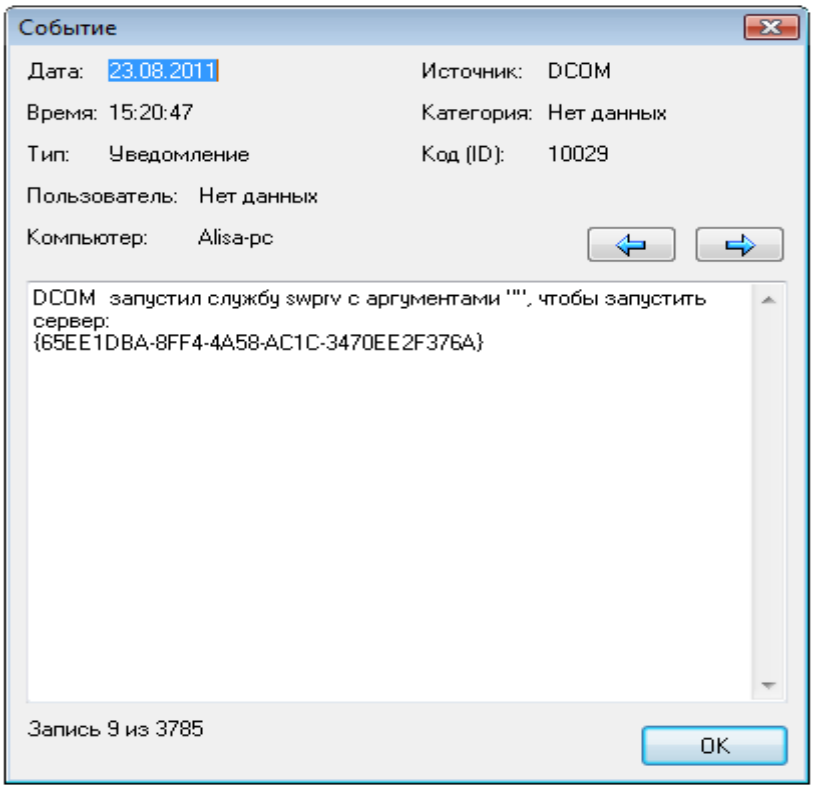


Рис. 24 Подія на віддаленому ПК

1.8 Установка підтримки SNMP на ПК з Windows Налаштування властивостей безпеки SNMP

Увага! Уважно вивчіть проблеми безпеки перед установкою служби SNMP на комп'ютер. Змініть community за замовчуванням, налагодьте обмеження в брандмауерові.

Часто в деяких мережевих пристроях (таких, як роутери, комутатори, мережеві принтери і т.д.) SNMP- Агент присутній, але не запущений. Для його запуску звичайно виконують наступні дії: звертаються до налагодження пристрою через Web-Інтерфейс, шукають параметр типу **"SNMP Agent (Disable/Enable)"** і встановлюють перемикач у позицію **Enable**, при цьому попутно звернувши увагу на параметр Community.

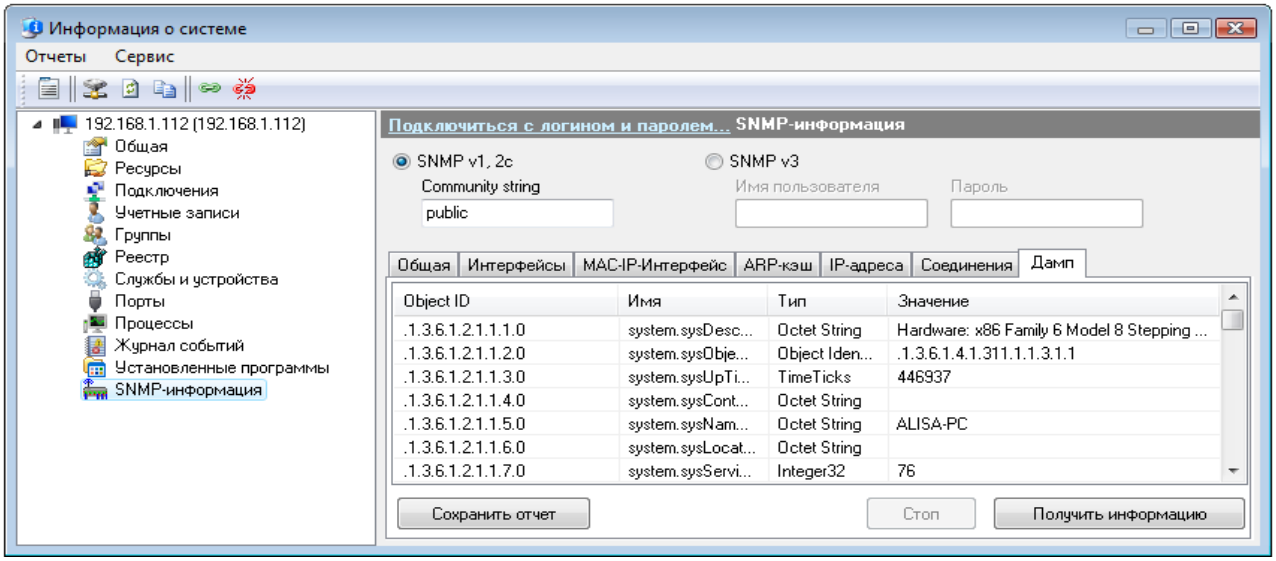


Рис. 24 SNMP-інформація на віддаленому ПК

Community (співтовариство) - це свого роду пароль доступу до інформації в пристрої. Даний пароль необхідно вказувати в поле SNMP Read Community string (рис. 24). Для одержання інформації необхідно вибрати, вкладку й нажати кнопку **Одержати інформацію**. На всіх вкладках, крім **Загальна,** є кнопка **Зберегти звіт**, що дозволяє вивантажити отриману інформацію в CSV-Файл.

На вкладці **Інтерфейси** можна одержати інформацію про існуючі у пристрої мережеві інтерфейси з докладною інформацією про кожний з них. Крім цього, доступна мережева статистика по вхідних і вихідних пакетах, що дозволяє відслідковувати мережевий трафік на віддалених пристроях.

На вкладці Mac-Ip-**Інтерфейс** можна одержати інформацію про таблицю з'єднань.

На вкладці **З'єднання** можна одержати інформацію про поточні TCP і UDP з'єднання хоста. Приводиться інформація про стан з'єднання, номер віддаленого/локального порту, віддаленої/локальної Ip-Адреси.

На вкладці **ДАМП** можна одержати всю доступну по SNMP-Протоколу інформацію від віддаленого пристрою. Одержання інформації може забрати тривалий час (залежить від пристрою), протягом якого не можна буде одержати інформацію з інших вкладок.

Дані можуть бути збережені в CSV-Звіт. Для зручного перегляду інформації можна подвійним клацанням на будь-якому записі відкрити вікно **Детальний перегляд** (рис. 25). Можна переходити до наступного / попереднього запису, натискаючи кнопку **Слід. >>/<< Перед.**

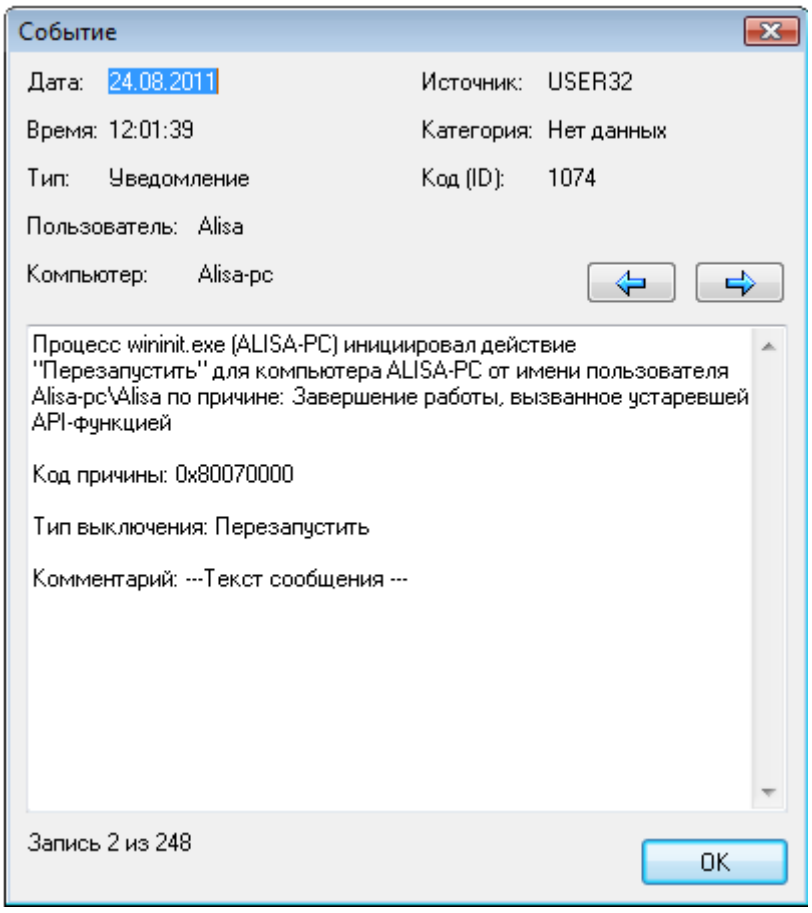


Рис. 25 Подія на віддаленому ПК

Інформація про домен

У вікні **Інформація про домен** зібрані відомості про домен або робочу групу. Доступна наступна інформація:

- Ім'я контролера домена;
- DNS-Ім'я контролера домена;
- Список довірених доменов;
- Користувачі, робочі станції, групи.

Одержання інформації може забрати тривалий час. Необхідно дочекатися закінчення роботи функції.

1.9 Робота з папками

У вікні відображаються папки вашого комп'ютера, до яких у даний момент призначений загальний доступ. (рис. 26)

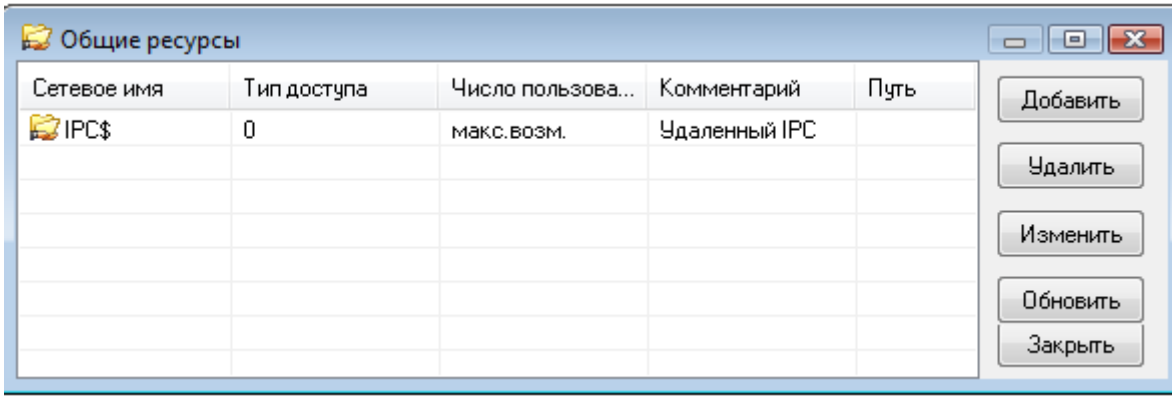


Рис. 26 Вікно папок

Ви можете:

- Змінити тип доступу до папок, вибравши в контекстному меню пункт **Змінити** й замінивши відповідні значення полів у вікні **Доступ** (рис. 27)**;**
- Закрити доступ, нажавши кнопку **Вилучити**;
- Відкрити доступ до нової папки, нажавши кнопку **Додати** й вибравши в дереві каталогів необхідну папку.

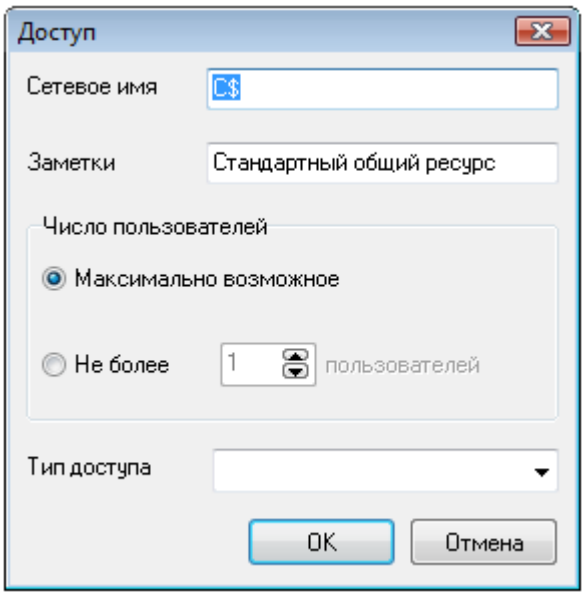


Рис. 27 Вікно доступу

1.10 Пінг

Функція **Пінг** подібна команди Winows - ping, але більш зручна (рис. 28). Можливе завдання параметрів:

- Розмір пакета даних;
- Число запитів;
- Час очікування.

Результати пінга, як і повідомлення про помилки, помістяться у вікно **Результат.**

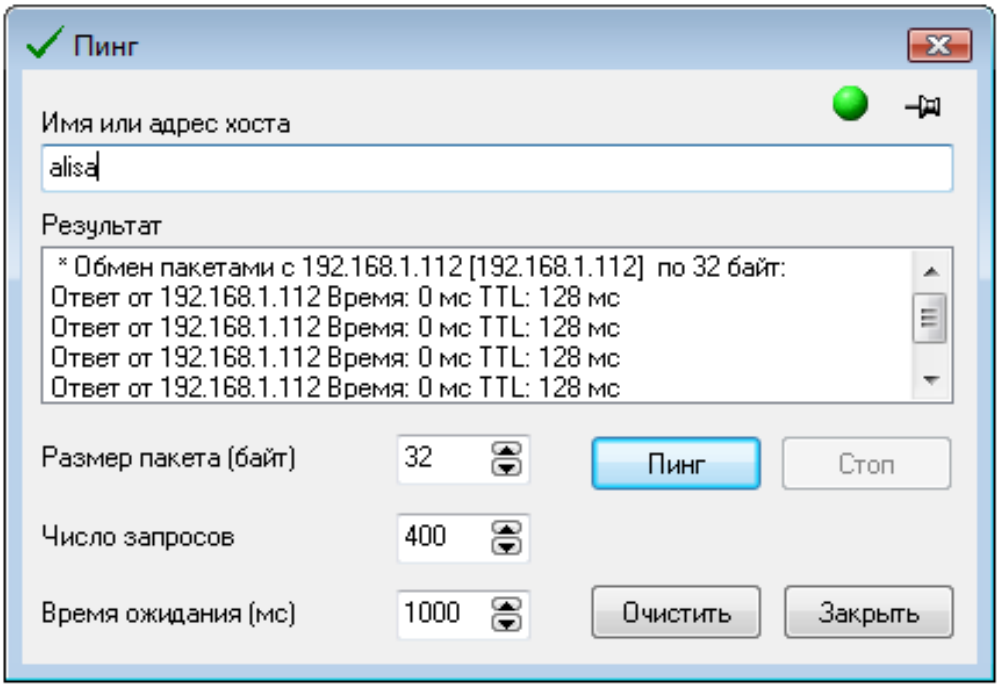


Рис. 28 Вікно пінг

Індикатор у верхньому правому куті повідомляє про готовність (зелений) або зайнятості (червоний).

Процес пінга можна зупинити натисканням кнопки **Стоп**.

1.11 Трасування маршруту

Функція **Трасувати маршрут** подібна команди Winows ***tracert***, але більш зручна (рис. 29). Можливе завдання параметрів:

- Число переходів**;**
- Час очікування**.**

Результати трасування помістяться у вікно **Результат**.

Індикатор у верхньому правому куті повідомляє про готовність (зелений) або зайнятості (червоний).

Процес трасування можна зупинити натисканням кнопки **Стоп**

1.12 Мережевий трафік

У цьому вікні ви можете бачити статистику вхідного й вихідного локального трафіка (рис. 30), а також найменування й Mac-Адреса інтерфейсу, через який він проходить (рис. 31).

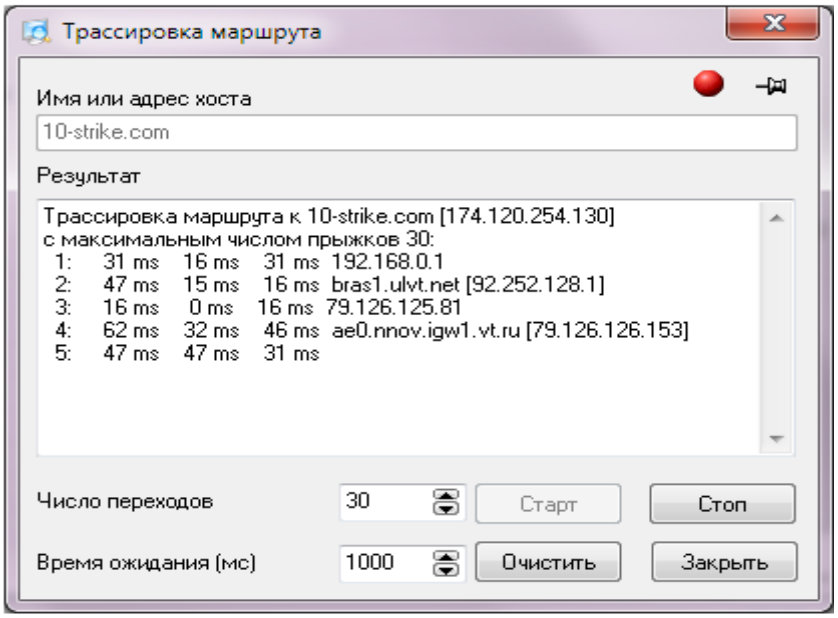


Рис. 29 Вікно трасування

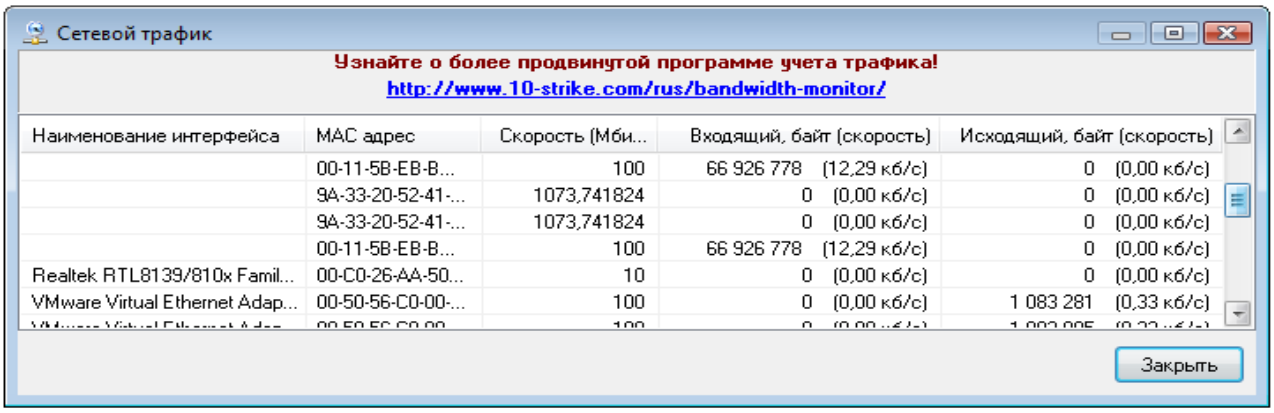


Рис. 30 Вікно мережевого трафіку

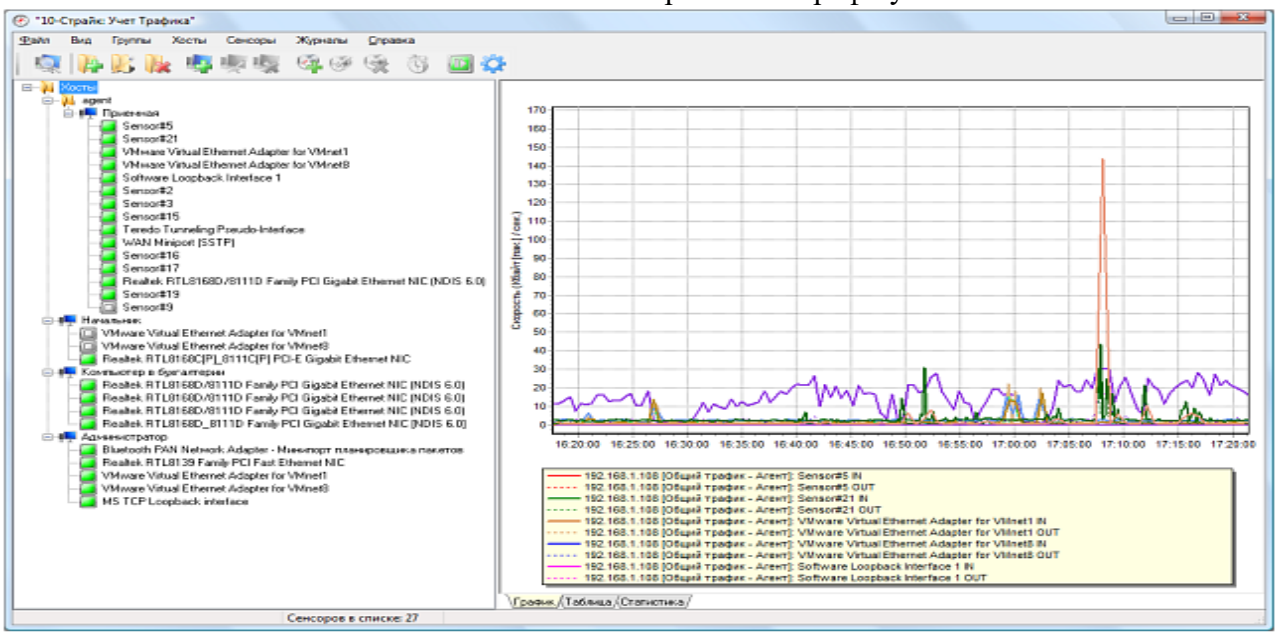


Рис. 31 Вікно графічного відображення мережевого трафіку

2. Хід роботи

Виконати роботи згідно п 1. Звіт представити в вигляді рисунків та пояснювального тексту. Сканування мережі провести трьома способами.

3.Контрольні питання

1. Призначення програми.
2. Можливості програми.
3. Як створити список хостів мережі?
4. Робота зі списком хостів.
5. Як завершити роботу віддаленого комп'ютера?
6. Як включити комп'ютери за мережею?
7. Як отримати інформацію про систему.
8. Установка підтримки SNMP на ПК з Windows Налаштування властивостей безпеки SNMP .
9. Робота з папками.
10. Як провести пінг мережі?
11. Як трасувати маршрут до віддаленого хоста?
12. Як отримати мережевий трафік?

РОЗДІЛ 5
Захист інформації відновленням даних на дисках, які попередньо видалені , або видалені при форматуванні
Лабораторна робота 23
Тестування дисків та відновлення даних на дисках, які попередньо видалені , або видалені при форматуванні.

Мета роботи – засвоїти принципи, технологію тестування дисків та відновлення даних на них, із використанням програми Easy Recovery Professional.

ПЛАН

1. Теорія

1.1. 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, яку має на панелі програми головні компоненти (див. рис. 1).

1.1.1. Компонента Disk Diagnostics Contents (Зміст Діагностики Диска)

Забезпечує Вас коштовною системою діагностичних інструментів (рис. 2). Інструменти, включені в цю категорію розроблені (призначені), для того, щоб швидко визначити, чи має ваша система проблеми з апаратними засобами ЕОМ або на-диску проблеми файлової структури. Усі інструменти в цій категорії роблять детальне повідомлення про систему.
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 Вам перевіряти фізичний стан вашого диска. Ви маєте здатність вибрати для одночасного дослідження одразу декілька дисків. Наступні випробовування, доступні в DriveTests інструменті (рис. 3):
У процесі вибору можливе встановлення:

Рис. 1. Вікно запуску програми.

Рис. 2. Вікно інструментів Діагностики Диска.

- Швидкого Діагностичного Іспиту
- Повного Діагностичного Іспиту

Якщо ваш 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 Вам із джемпером, для дисків ATA/IDE.

Ви маєте вибір (опцію), щоб керувати одним випробовуванням одночасно на кожнім відібраному диску швидко визначати, чи має ваш нагромаджувач на твердих дисках, серйозні фізичні проблеми, вибирайте 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. 4. Швидкий Діагностичний Іспит визначить, з 90-процентною впевненістю, у 90 секунд, чи має ваш твердий диск фізичну проблему. Повний Діагностичний іспит перевірить повний нагромаджувач на твердих дисках, що має фізичні проблеми типу нечитабельних секторів. Якщо Ви невпевнені щодо фізичної стабільності вашого твердого диска, виберіть -- Повний Діагностичний іспит. шикарний(сильний) – іспит для самоконтролю, аналізу і Reporting Технологія. шикарна(сильна) допомога іспитів запобігає втраті даних, пророкуючи можливі відмови диска, використовуючи спеціальні алгоритми, убудовані в програмувальне устаткування вашого нагромаджувача на твердих дисках. Самі нові IDE і SCSI накопичувачі на твердих дисках підтримують шикарну (сильну) технологію.

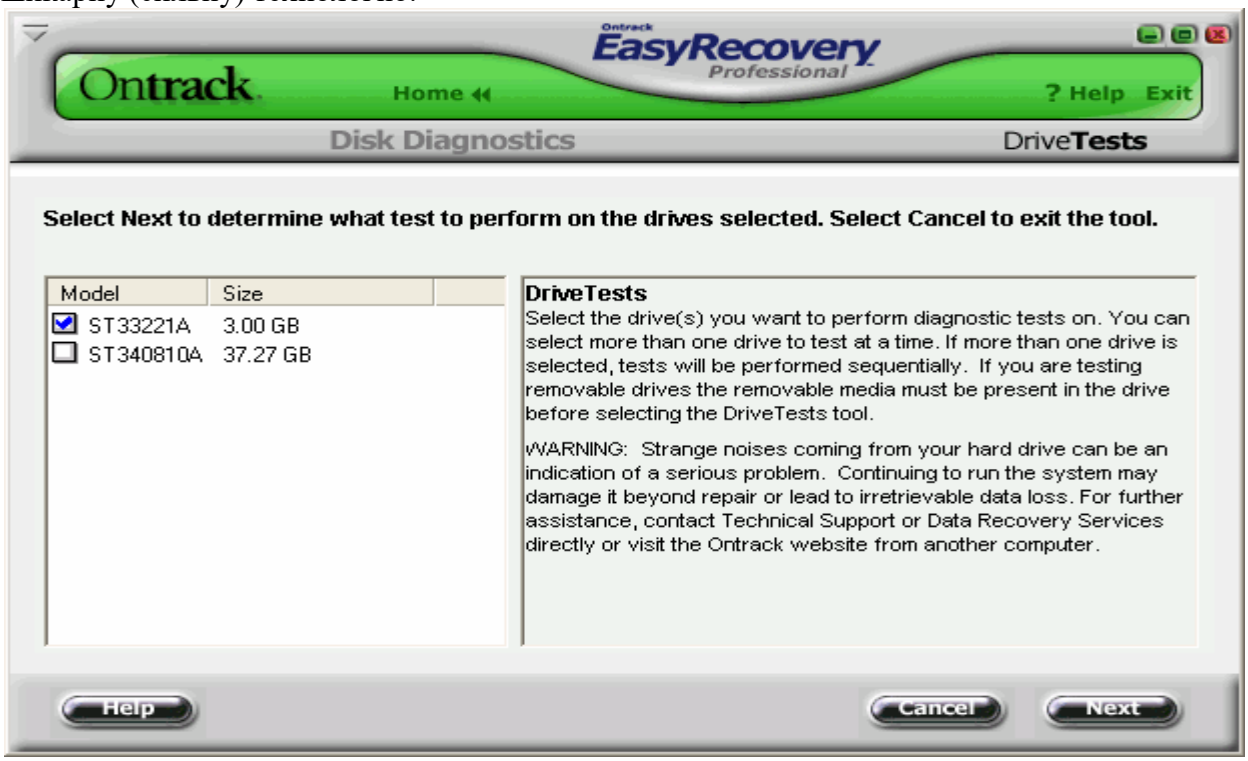


Рис. 3. Вікно майстра вибору дисків та режимів дослідження дисків.

1.1.2. Компонента SMARTTests

Включає три, окремі діагностичні іспити:

- · шикарний (сильний) іспит -- виконає швидку перевірку статусу нагромаджувача на твердих дисках, за кілька секунд.
- · короткий шикарний (сильний) 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 з вашим диском

- · розширений шикарний (сильний) іспит – проведе всебічну перевірку твердого диска. Цей іспит також убудований у програмне устаткування нагромаджувачів на твердих дисках і розроблений (призначений), щоб знайти незначні внутрішні проблеми або непогодженості з вашим диском.

Для перевірки дисків необхідно:

1. Вибрати диск, на якому Ви бажаєте виконати шикарний (сильний) іспит . Іспитові результати будуть показані, коли іспити повні. Ви можете вибрати більше ніж один диск одночасно. Якщо більше чим один диск відібраний, іспити будуть виконані послідовно.
2. Вибрати тип шикарного (сильного) іспиту на відібраних дисках.

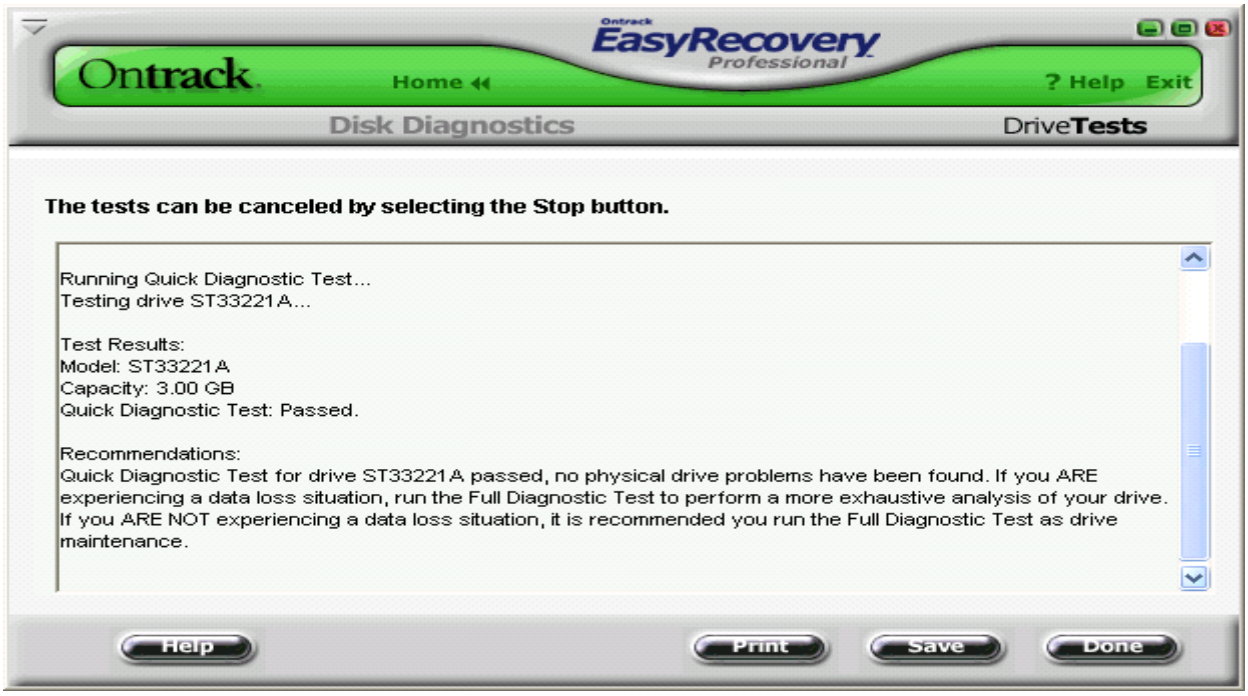


Рис. 4. Вікно результатів дослідження диска.

1.1.3. Компонента PartitionTests

У деяких випадках, у той час як ваш диск не може мати ніяких фізичних проблем, він може мати на диску проблеми файлової структури. PartitionTests інструмент розроблений (призначений), щоб аналізувати на диску структуру файлової системи. Перевірки файлової системи перевіряють цілісність даних розділів NTFS і FAT. Час іспитів зміниться дуже в залежності від розміру розділу числа файлів у розділі.

Для перевірки диска виберіть розділ, який буде перевірятися (рис. 5). Про будь-які знайдені помилки файлової структури будуть повідомлення на екрані.

1.1.4. Компонента DataAdvisor (Радник Даних)

Це діагностичний інструмент щоб оцінити стан вашої комп'ютерної системи. Радник Даних швидко оцінює “здоров'я” вашого диска, структуру файлової системи, і комп'ютерної пам'яті, пізнаючи проблеми, які могли заподіяти втрату даних. Цей усебічний діагностичний інструмент може використовуватися, щоб і діагностувати поточні проблеми і як частина правильної програми обслуговування, щоб ідентифікувати потенційні проблеми, що могли вести до втрати даних. Якщо потенційні проблеми ідентифіковані, Ви будете мати час і зробити виправлення, щоб уникнути майбутньої втрати.

При виборі DataAdvisor , програма дозволить проводити:

- · Швидкий Функціональний Іспит - читає й прагне на твердому диску перевіряти катастрофічні фізичні проблеми.
- · шикарна (сильна) Перевірка - повідомляє Вам 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.

1.1.5. Компонента Ontrack JumperViewer

Це графічний, діалоговий аплет Яви для того, щоб швидко знайти розміщення джемпера для IDE/ATA нагромаджувачів на твердих дисках. Цей оглядач на основі Інтернету дозволяє Вам одержувати доступ до самої поточної бази даних призначень джемпера нагромаджувача на твердих дисках. База даних включає останні версії головних виготовлювачів дисків.

Для більшої кількості допомоги на Ontrack JumperViewer відвідують наступний зв'язок: http://www.ontrack.com/jumperviewer/jumperviewerhelp.asp

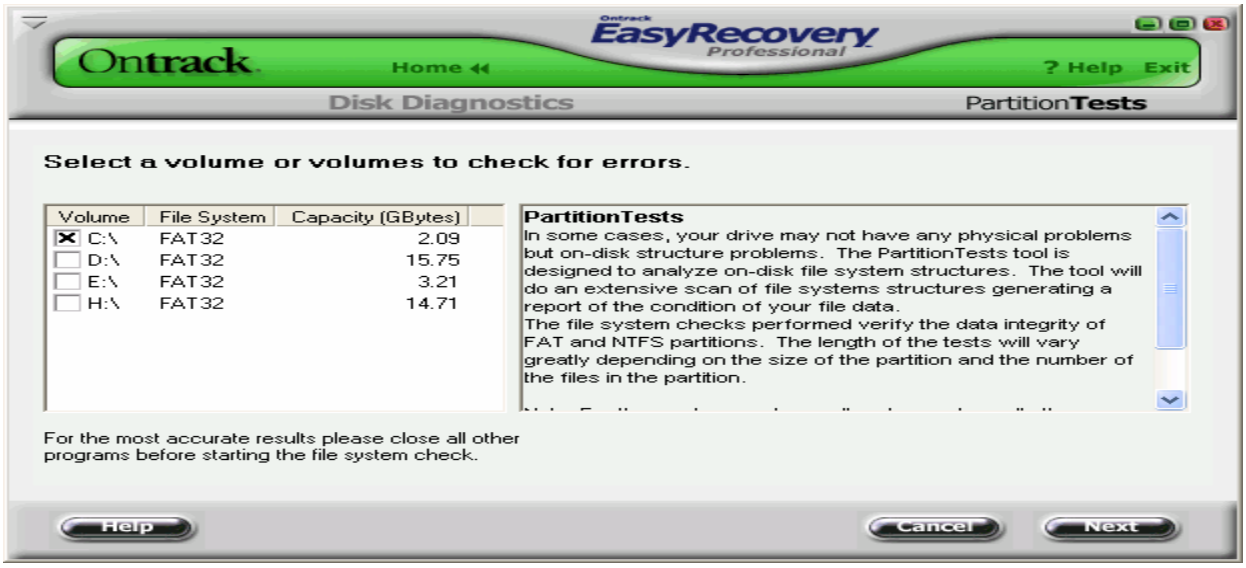


Рис. 5. Вікно майстра діагностики.

1.1.6. Компонента SizeManager

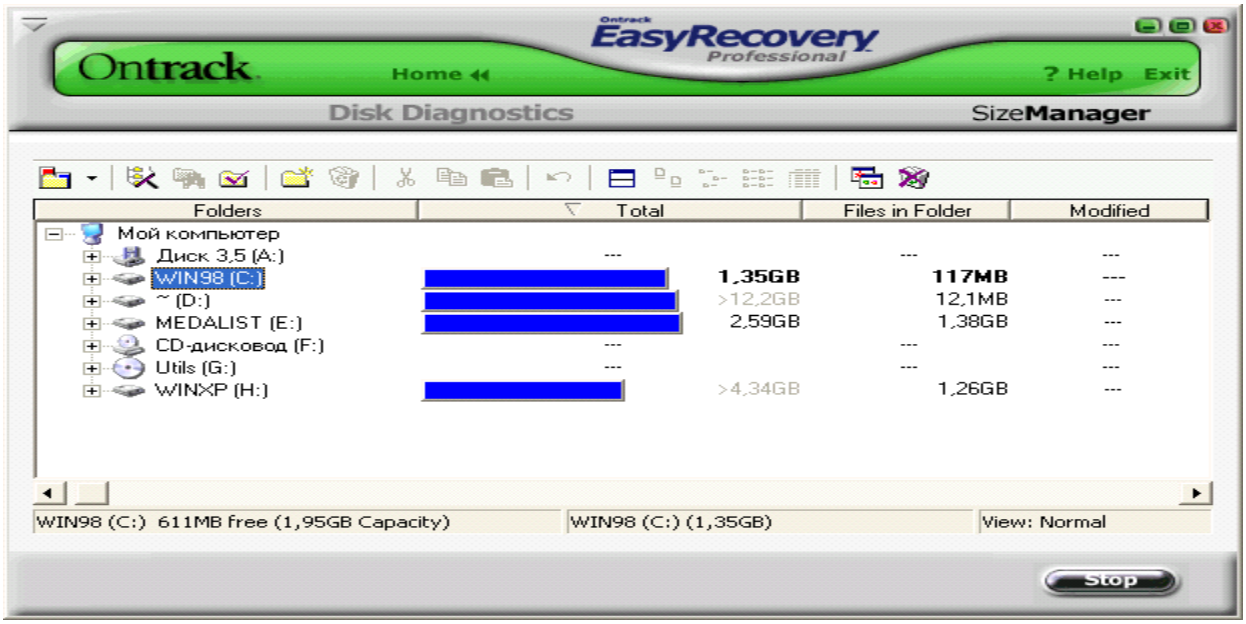
Показує степінь використання диска на вашій комп'ютерній системі. SizeManager надає миттєве графічне представлення того, де і як використовується місце на вашому комп'ютері (рис. 6), полегшує визначення місцезнаходження негабаритних каталогів і файлів. SizeManager допомагає Вам визначати, які файли захаращують місце на вашій системі.

1.2 Категорія Data Recovery (Відновлення Даних)

Включає інструменти відновлення (рис. 7), файлів та каталогів. Інструменти Відновлення Даних повернуть файли FAT і розділів NTFS. Усі інструменти є що не руйнують і тільки читають . Інструменти розроблені (призначені), щоб повернути і копіювати ваші дані до іншого призначеного типу змінного диска, іншого нагромаджувача на твердих дисках, гнучкої дискети, або диску мережі.

Кожен інструмент – це майстер, який веде користувача через три простих кроки та дозволяє:

1. Оцінити - інструмент ідентифікує всі пристрої і/або розділи на системі і показує графічне представлення того, що було знайдено
2. Відтворити - інструмент досліджує структури файлу, що залишаються на 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)



Малий. 6. Вікно SizeManager

Рис. 7. Вікно відновлення файлів, каталогів.

FormatRecovery (Відновлення Формату)

RawRecovery (Попереднє Відновлення)
ResumeRecovery (Відновлення Резюме)
EmergencyDiskette (Надзвичайна Дискета)

1.2.1. 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

1.2.2. Компонента AdvancedRecovery

Для самого важкого відновлення призначена компонента , AdvancedRecovery інструмент (рис. 8), який забезпечує Вас просунутими варіантами відновлення, включаючи, проблеми повернення файлів та каталогів при помилковому вилученні з розділу вірусних нападів, і інших помилок та пошкоджень файлової системи. Інструмент забезпечує детальне графічне представлення дисків, зв'язаних із вашою системою, включаючи розділи, зв'язані з кожним пристроєм.

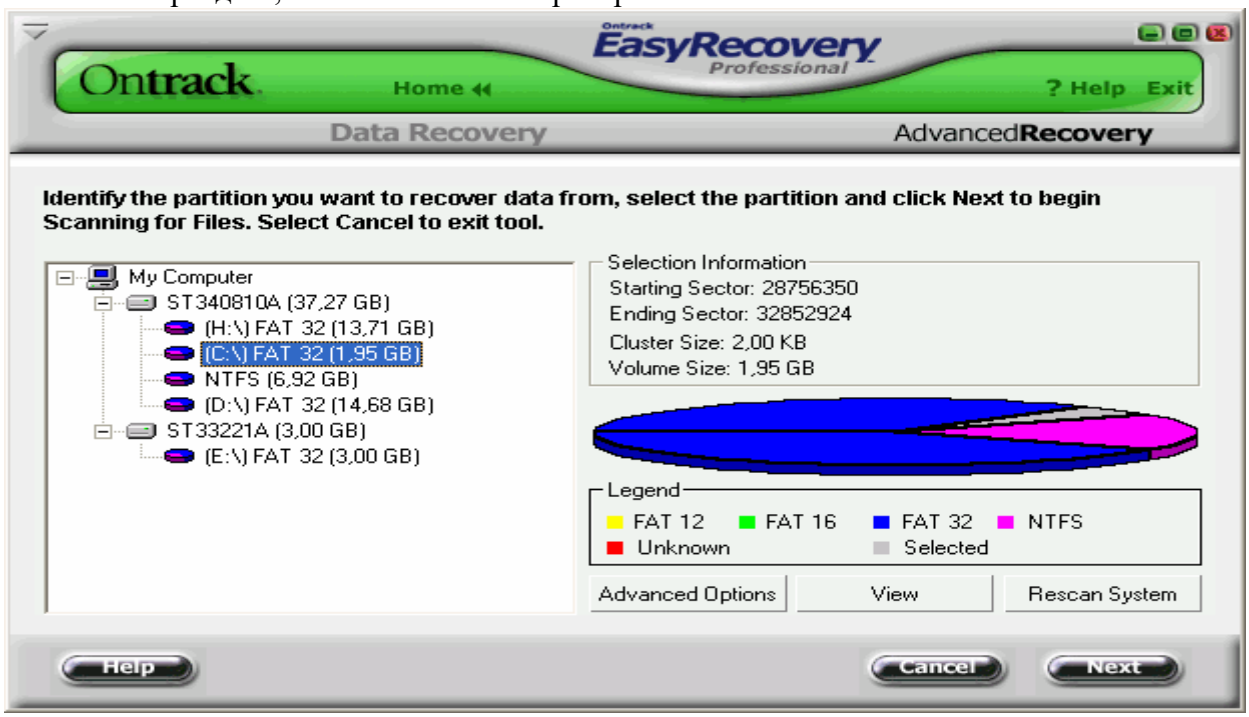


Рис. 8. Вікно майстра AdvancedRecovery

Список видалених файлів представлений на рис. 9. Вікно вибору диска, куди будуть записані відновлені файли, представлене на рис. 10. Вікно результатів відновлення файлів представлене на рис. 11.

1.2.3. Компонента DeletedRecovery.

Помилкове видалення файлів - один із самих загальних (звичайних) сценаріїв відновлення даних. DeletedRecovery інструмент дасть Вам швидкий доступ до вилучених файлів, і має різні варіанти щоб переглянути розділ. Ви можете виконати швидкий перегляд, або повний перегляд для вилучених файлів. Ви також маєте можливість встановлення Фільтру для Файлів (рис. 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. 13).

Як правило, якщо Ви видалили один або два файли і не скопіювали ніяких даних до розділу, то Ви маєте дуже гарний шанс на відновлення вилучених файлів. У цій ситуації, інформація файлу може звичайно бути знайдена, використовуючи швидкий вибір перегляду. Якщо Ви видалили повний довідник з декількома довідниками й файлами, Ви будете ймовірно повинні виконати повний перегляд. Імовірність відновлення файлу цілком неушкодженим зменшується, коли файл фрагментовано.

1.2.4. Компонента FormatRecovery

Інша загальна (звичайна) ситуація відновлення даних настає при випадковому форматуванні розділу. FormatRecovery інструмент дозволить Вам повертати 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, на розділі , який відформатовано, усе ще присутні і можуть бути повернуті (відновлені), із використанням даного інструменту.

Перший екран на FormatRecovery інструменті покаже список розділів знайденого на дисках, знайдених у вашій системі. Щоб починати форматоване відновлення, виберіть розділ, а потім файли, які Ви будете відновлювати (рис. 13).

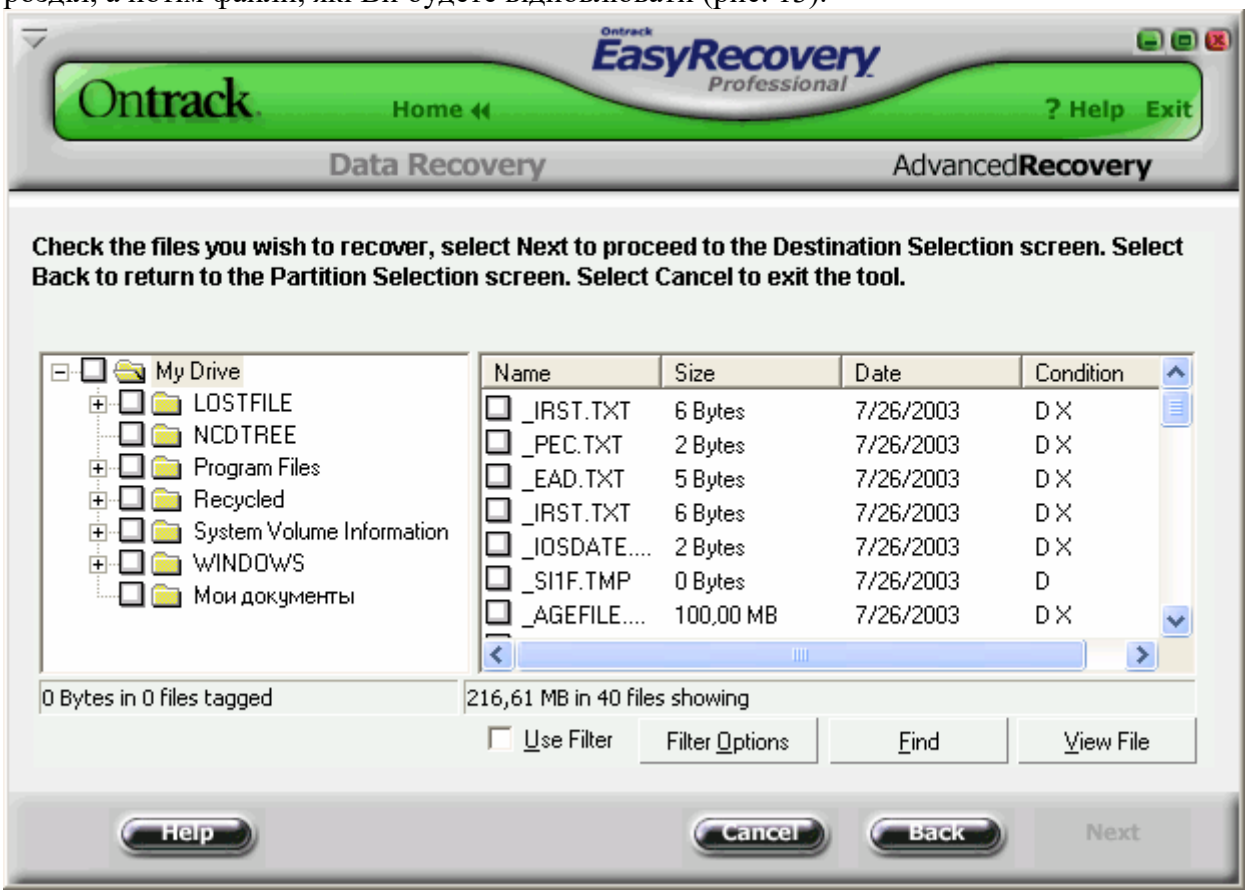


Рис. 9. Вікно зі списком видалених файлів.

Цей інструмент допоможе Вам повертати файли від розділів з ушкодженими файловими системами. Він буде читати всі сектори на диску послідовно (сектор за сектором), щоб визначити підписи удару головкою (заголовка) файлу. Якщо Ви недавно керували диском defragmenter , ваші можливості відновлення дуже поліпшені.

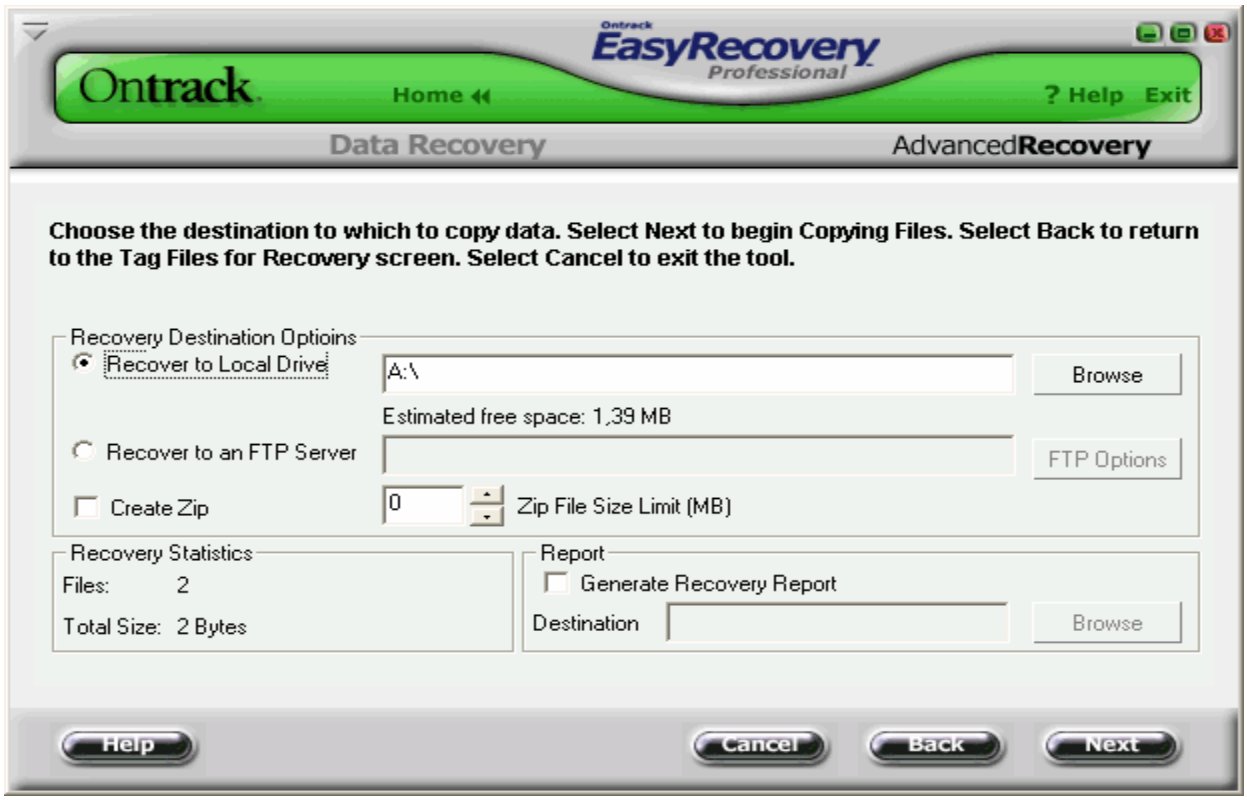


Рис. 10. Вікно вибору диска, куди будуть записані відновлені файли.

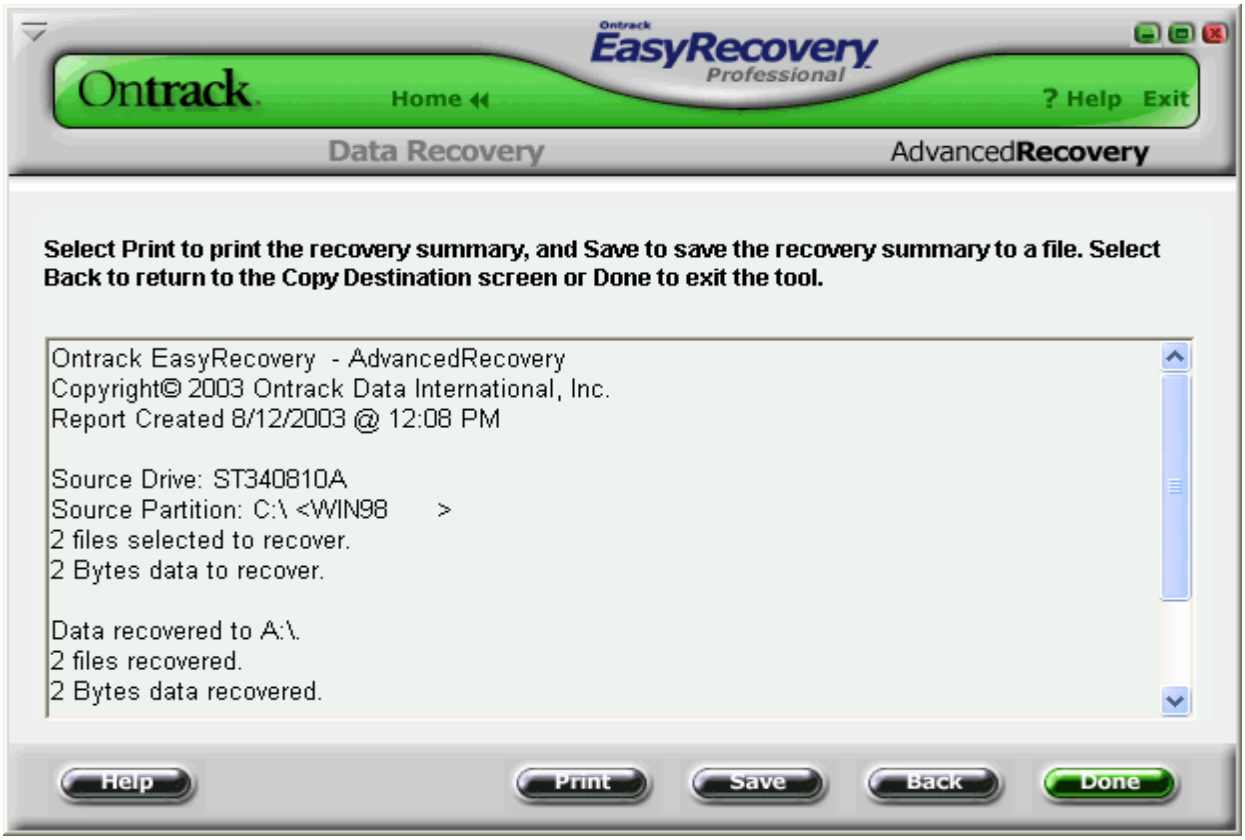


Рис. 11. Вікно результатів (резюме) відновлення файлів.

Рис. 12. Вікно встановлення фільтру

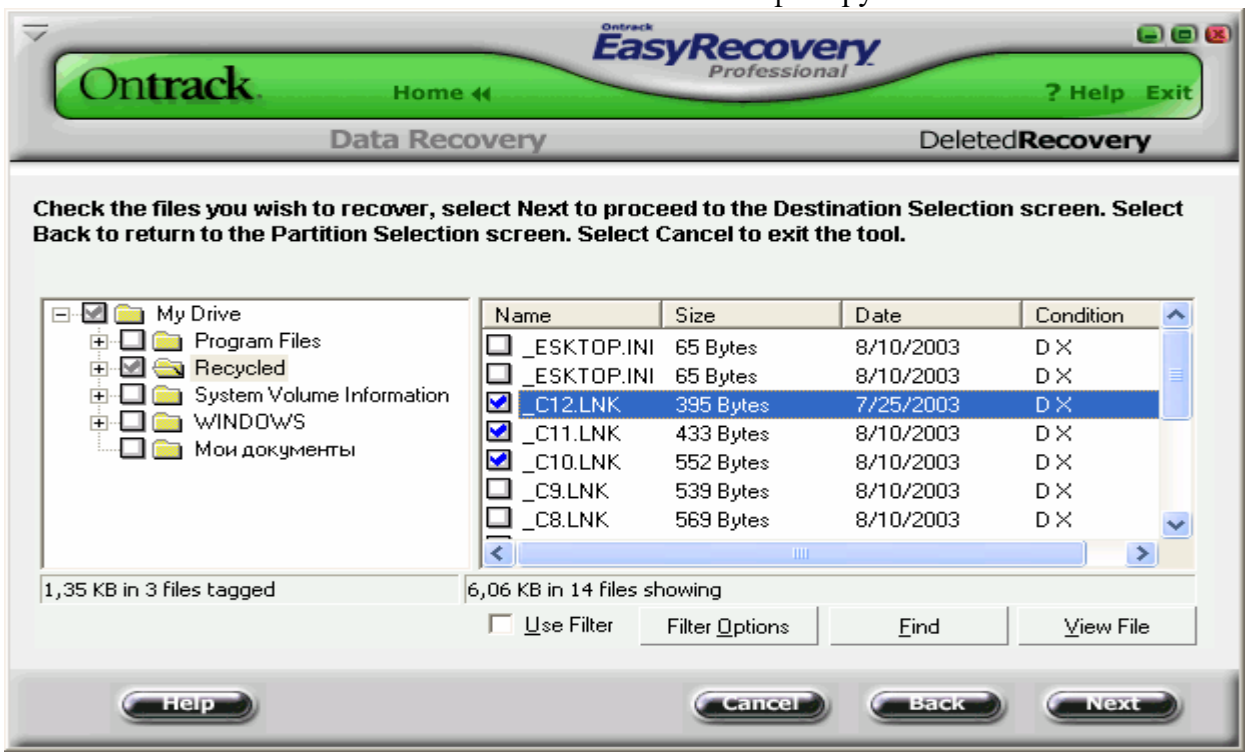


Рис. 13. Вікно перегляду видалених файлів.

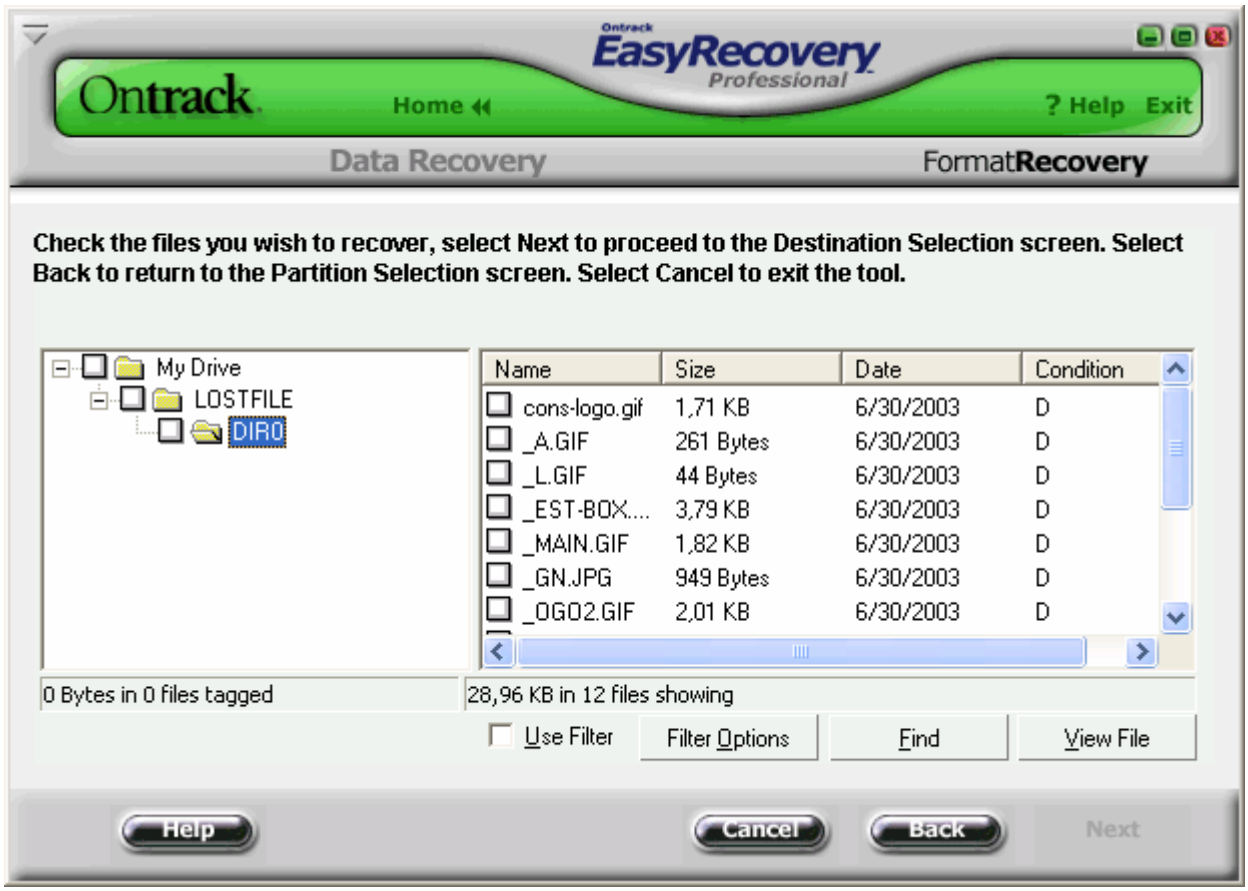


Рис. 13. Вікно зі списком видалених каталогів та файлів після форматування дискети.

2. Хід роботи

1. Проведіть тестування диска «С» на вашому комп'ютері в режимі Швидкого Діагностичного Іспиту.
2. Проведіть тестування диска «С» на вашому комп'ютері в режимі Повного Діагностичного Іспиту
3. Проведіть тестування диска «С» на вашому комп'ютері в режимі ШИКАРНИЙ (СИЛЬНИЙ) іспит.
4. Проведіть тестування оперативної пам'яті вашого комп'ютера.
5. Відновити два файли на диску “С”, за допомогою компоненти AdvancedRecovery, та записати їх на диск “А”.
6. Відновити два файли на диску “А”, за допомогою компоненти FormatRecovery, та записати їх на диск “С” .
7. Відновити два файли на диску “А”, за допомогою компоненти DeletedRecovery, та записати їх на диск “С” .

3. 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 ШИКАРНИЙ (СИЛЬНИЙ) іспит.
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.

Лабораторна робота 24
Видалення даних за допомогою програми Disk Wiper.

Мета роботи – засвоїти принципи, технологію роботи з остаточного видалення даних.

ПЛАН

1. Теорія
1.1 Введення
1.2 Версія Windows Disk Wiper
2. Хід роботи
3. Контрольні питання

1. ТЕОРІЯ

1.1 Введення

Реальне видалення файлів на накопичувачах на жорстких дисках 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.

1.2 Версія Windows Disk Wiper

Версія Windows Disk Wiper має розвинений інтерфейс і більше функціональних можливостей в порівнянні з версією для DOS. Інтерфейс вікон майстра дає Вам більше можливостей (рис. 1).

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. 1). Після введення команди з'явиться вікно (рис. 2). 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. 3).

При виборі команди **Format** із під меню **Partition** з'явиться вікно рис. 4.

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. 5).

Після форматування диску необхідно перезавантажити комп'ютер.

Розділ може бути видалений, якщо ввести команду **Delete** із під меню **Partition** (рис. 6).

При введенні команди Wipe partition із під меню Partition буде проведено повне очищення диску від всіх 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. 7)

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**.

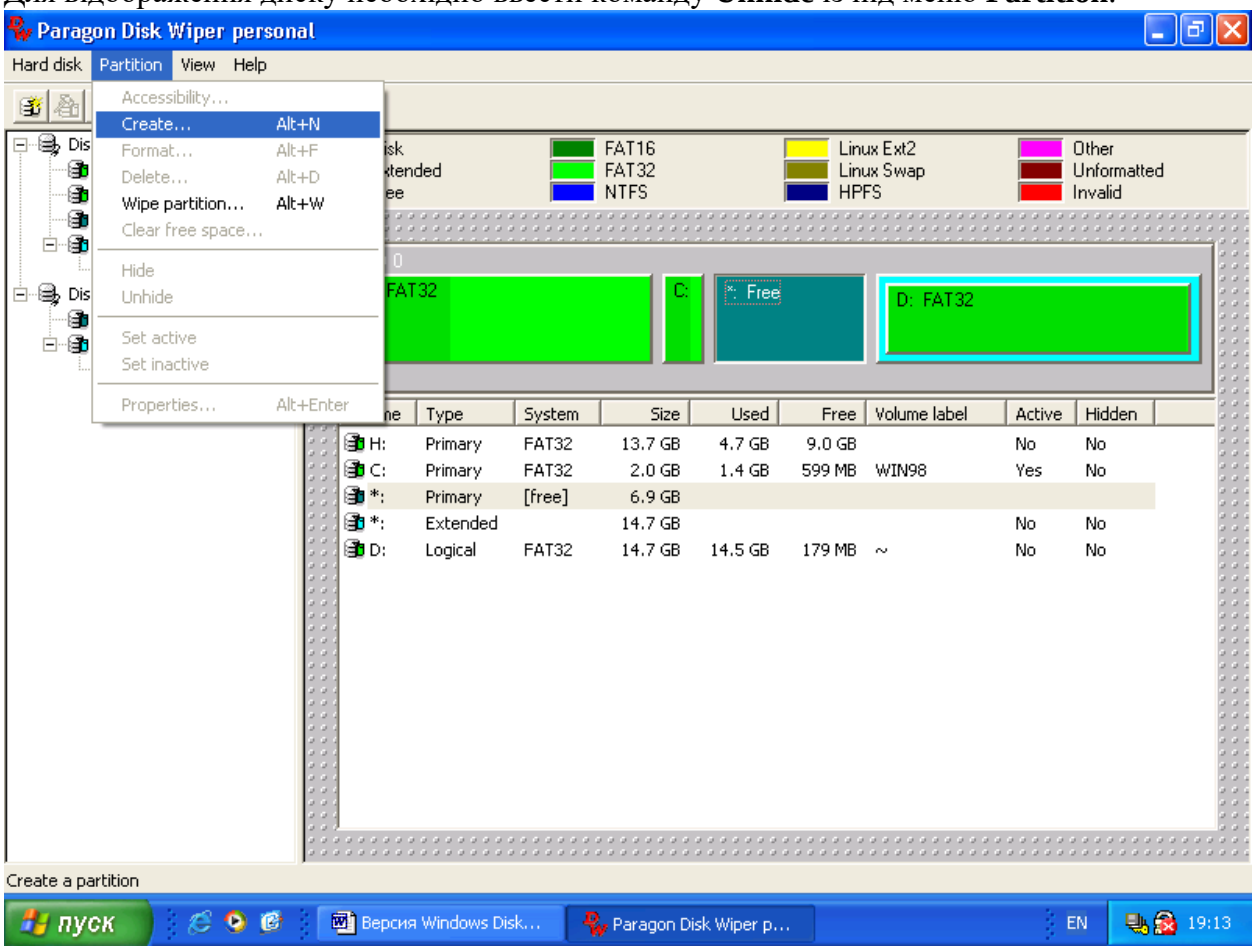


Рис. 1. Вікно майстра програми.

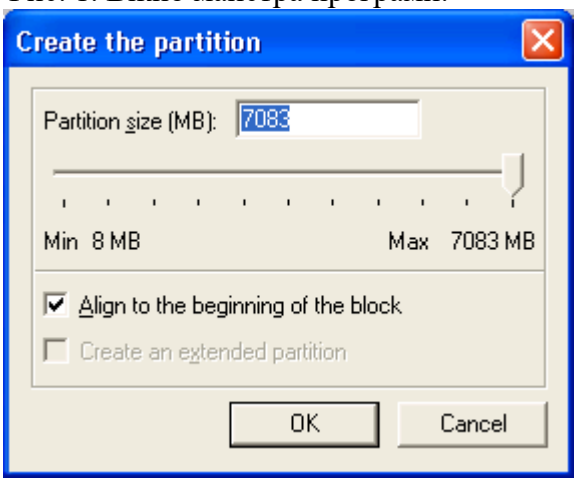


Рис. 2. Вікно вибору параметрів диска, який буде створено.

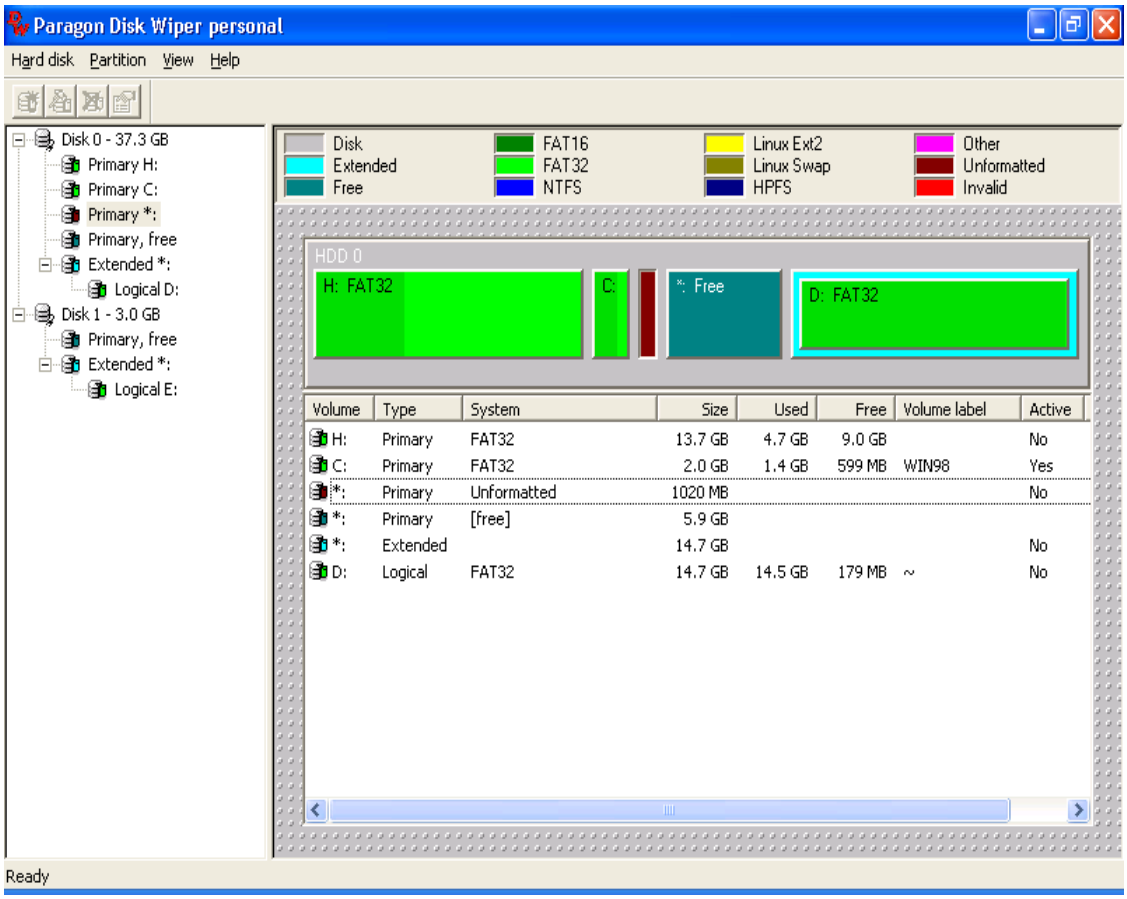


Рис. 3. Вікно з створеним неформатованим розділом.

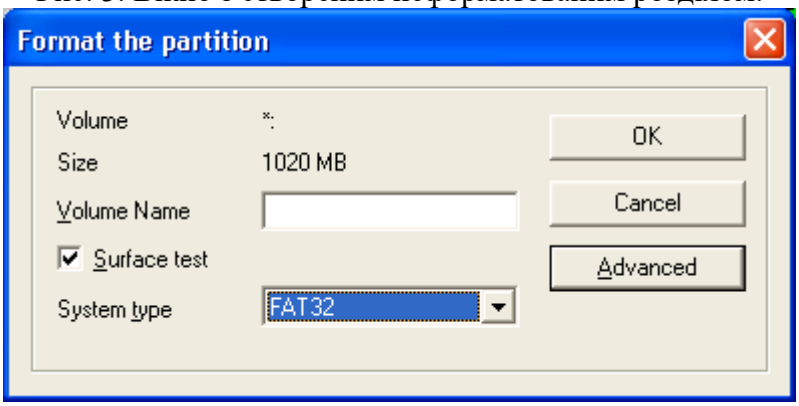


Рис 4. Вікно вибору параметрів форматування.

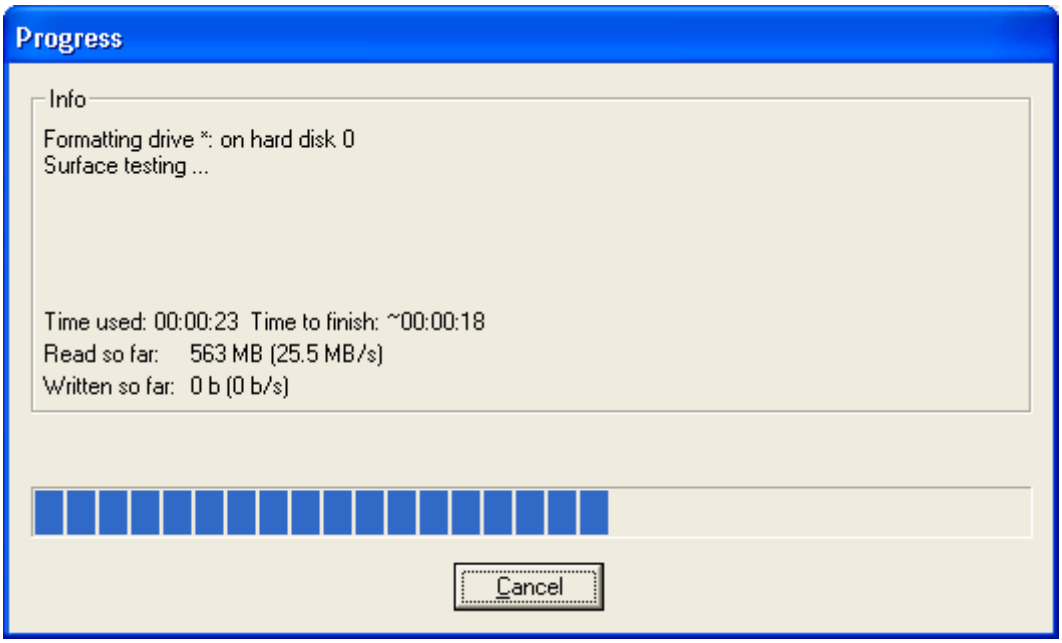


Рис. 5 Форматування диску.

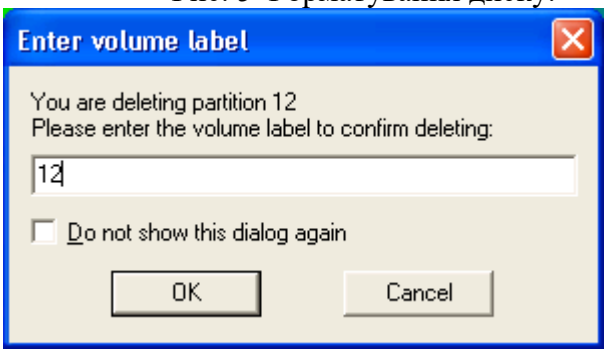


Рис. 6. Вікно видалення розділу.

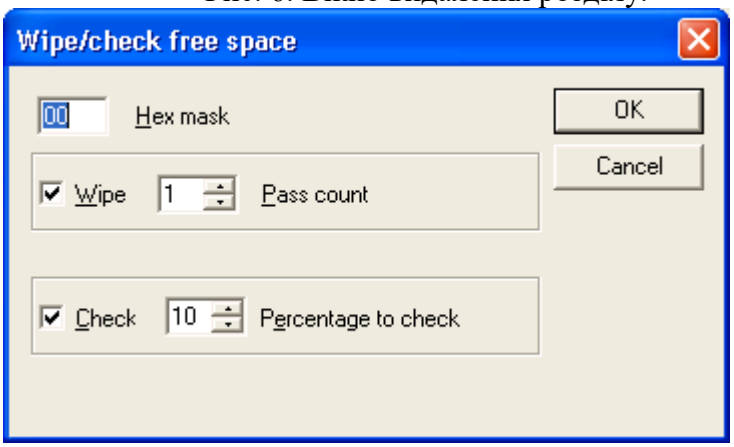


Рис. 7. Вибір параметрів очищення вільного простору на диску

2. Хід роботи

1. Створіть логічний диск „D”на своєму комп'ютері за допомогою програми Windows Disk Wiper розміром 1024 Мб (мітка диска 12).
2. Проведіть форматування створеного логічного диску (прийняти FAT32).

3. Перезавантажте комп'ютер та впевніться, що створений диск має правильне позначення.
4. Проведіть копіювання на створений диск 20 довільних файлів та каталогів.
5. Проведіть видалення 5 файлів з провідника Windows на створеному диску.
6. Проведіть очистку вільного простору на вказаному диску.
7. Проведіть повну очистку диску.
8. Проведіть приховування диску „D” (перевірте з провідника Windows, що диск не видно).
9. Відобразьте диск.
10. Проведіть видалення диску „D”.

3. Контрольні питання

1. Призначення програми Disk Wiper.
2. Особливості програми Windows Disk Wiper.
3. Як створити новий логічний диск за допомогою програми Windows Disk Wiper?
4. Як провести форматування створеного диску?
5. Як перевірити правильність позначення створеного диску?
6. Послідовність очистки вільного простору на диску.
7. Послідовність повної очистки диску.
8. Послідовність видалення логічного диску.
9. Як проводиться приховування диску та його відображення?

Лабораторна робота 25
Видалення програмного забезпечення за допомогою програми Revo Uninstaller

Мета роботи – Засвоїти принципи й елементи технології видалення програмного забезпечення за допомогою програми Revo Uninstaller. Ознайомитись з можливостями програми очистки реєстру та залишків програм, які не видаляються особистим деінсталятором програми.

План

1. Теорія
1.1 Режими роботи програми
1.2 Видалення програми
2. Хід роботи
3. Контрольні питання

1. Теорія

Вступ

В більшості випадків не представляється можливим видалення всіх компонентів програм, які видаляються та очистки реєстру від їхніх елементів. Це приводить до того, що вказані компоненти займають додаткове місце на логічних дисках, як правило, системному, а також знижується швидкість роботи комп'ютера внаслідок недостатнього місця на диску та наявності зайвих записів в реєстрі Windows.

Програма Revo Uninstaller дозволяє виконати вказані дії. Встановлення програми

відбувається внаслідок подвійного клацання по піктограмі . Далі слід слідувати за майстром встановлення програми та відбирати потрібні параметри.

1.1 Режими роботи програми

При запуску програми відкривається вікно (рис. 1).

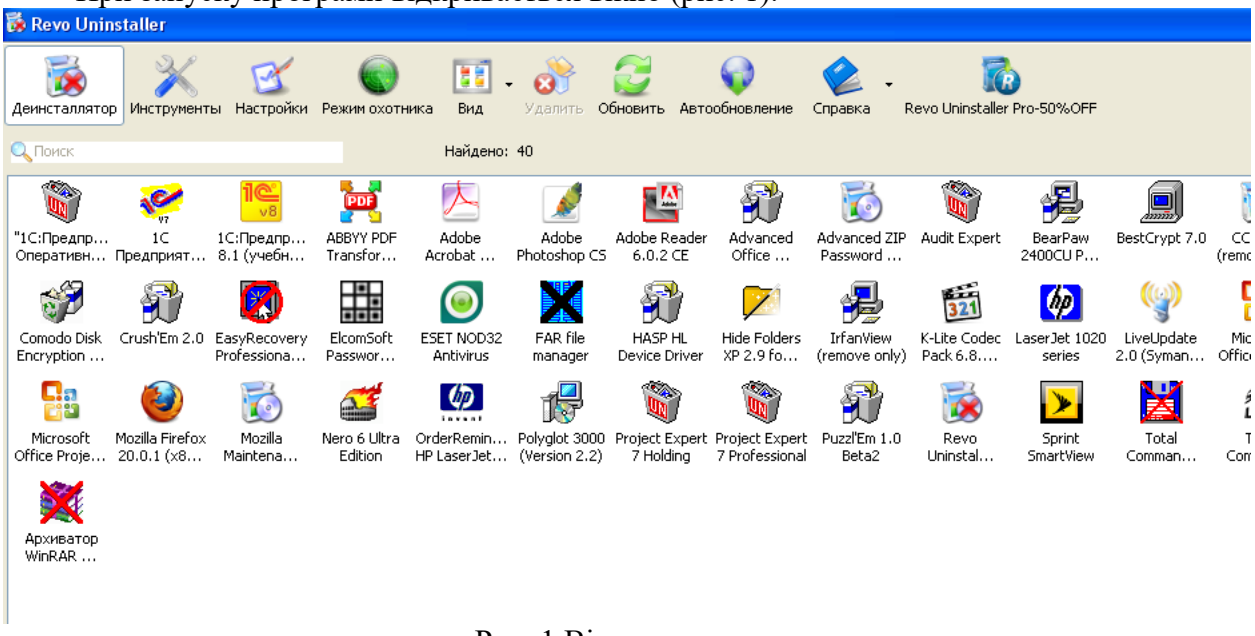
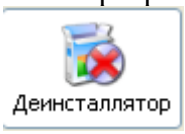
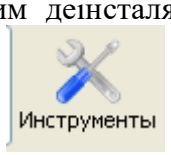
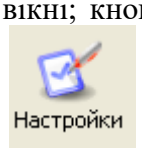


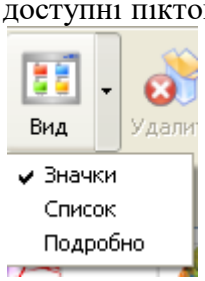
Рис. 1 Вікно програми

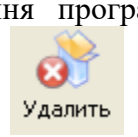
Програма може працювати в декількох режимах, якщо включена кнопка 

Деинсталятор, то це режим деінсталяції програмного забезпечення, яке представлено в основному вікні; кнопка 

дозволяє оптимізувати інструменти програми (рис. 2); кнопка 

дозволяє налагодити параметри програми (рис.3), кнопка 

переводить автоматично її в режим, коли на робочому столі доступні піктограма та контекстне меню (рис. 4), кнопка 

дозволяє відібрати параметри представлення програмного забезпечення у вікні програми; кнопка 

дозволяє почати процес видалення програми (вона активна, якщо виділена

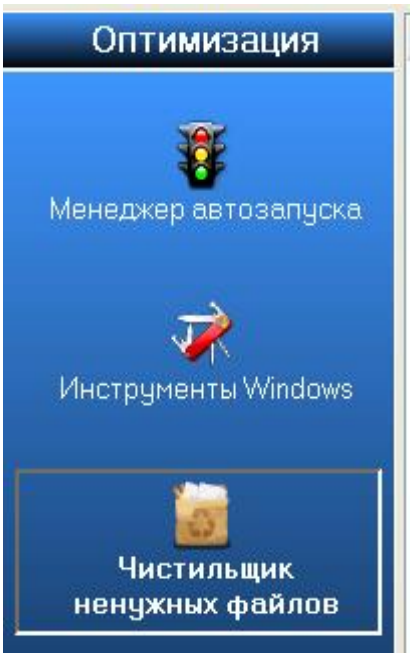
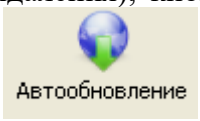
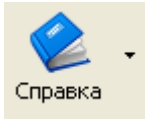


Рис. 2 Режим оптимізації інструментів

програма для видалення); кнопка 

дозволяє обновити список програмного забезпечення; кнопка 

дозволяє обновити версію програми через Інтернет; кнопка 

надає довідку за програмою.

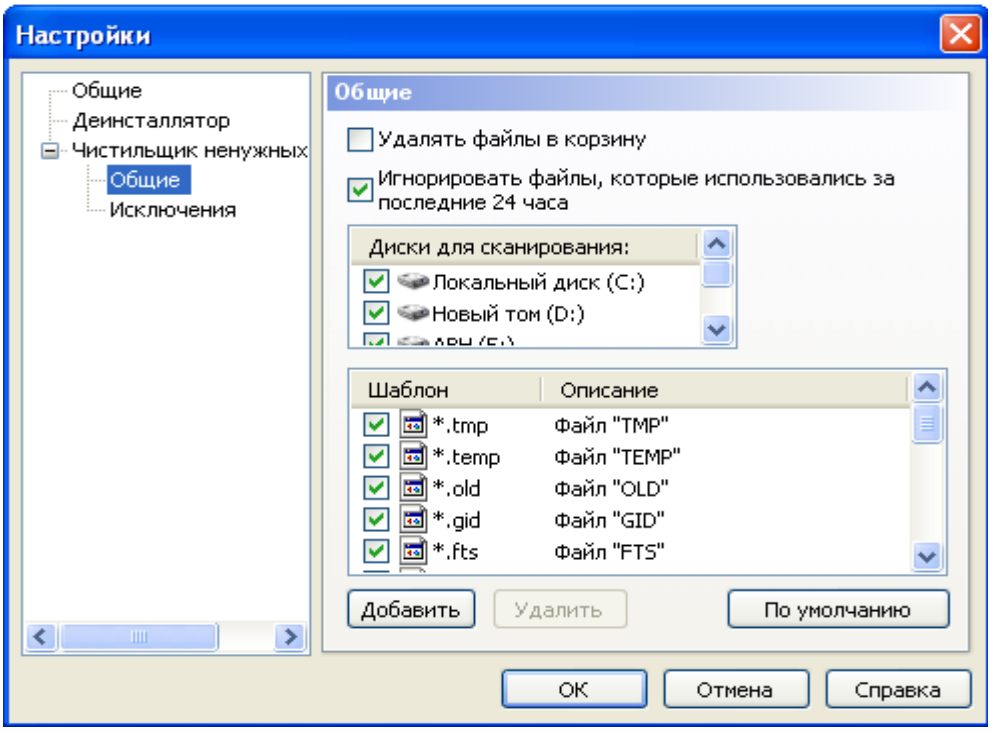


Рис. 3 Режим налагодження параметрів програми

.

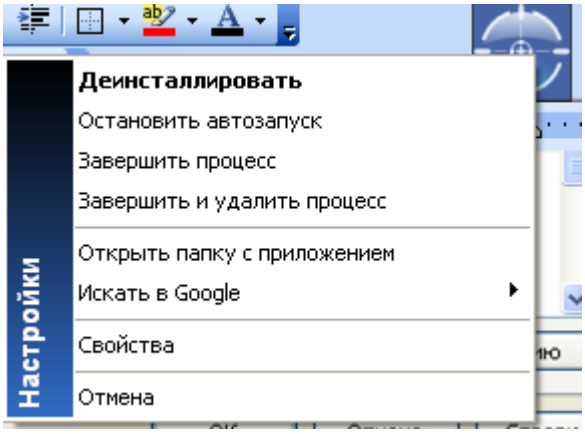


Рис. 4 Режим мисливця

1.2 Видалення програми

Процес видалення програми відбувається за допомогою майстра. Після введення команди видалити з'являється вікно з запитом підтвердження на видалення (рис. 5). Якщо ввести команду **Нет**, то видалення програми не відбудеться, і навпаки якщо ввести команду **Да**, відкриється вікно майстра (рис. 6) в якому необхідно відібрати режим деінсталяції та ввести команду **Далее**. Почнеться процес деінсталяції (рис.7) буде підключено на цьому кроці роботи майстра внутрішній деінсталятор програми (рис. 8).

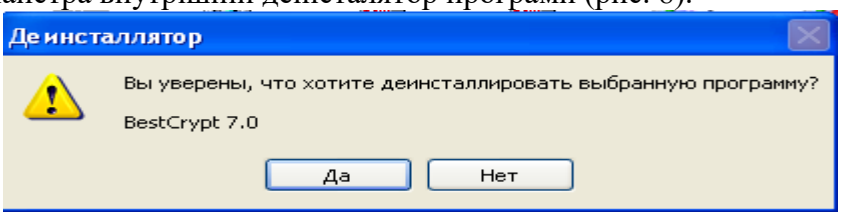


Рис. 5 Вікно підтвердження видалення програми.

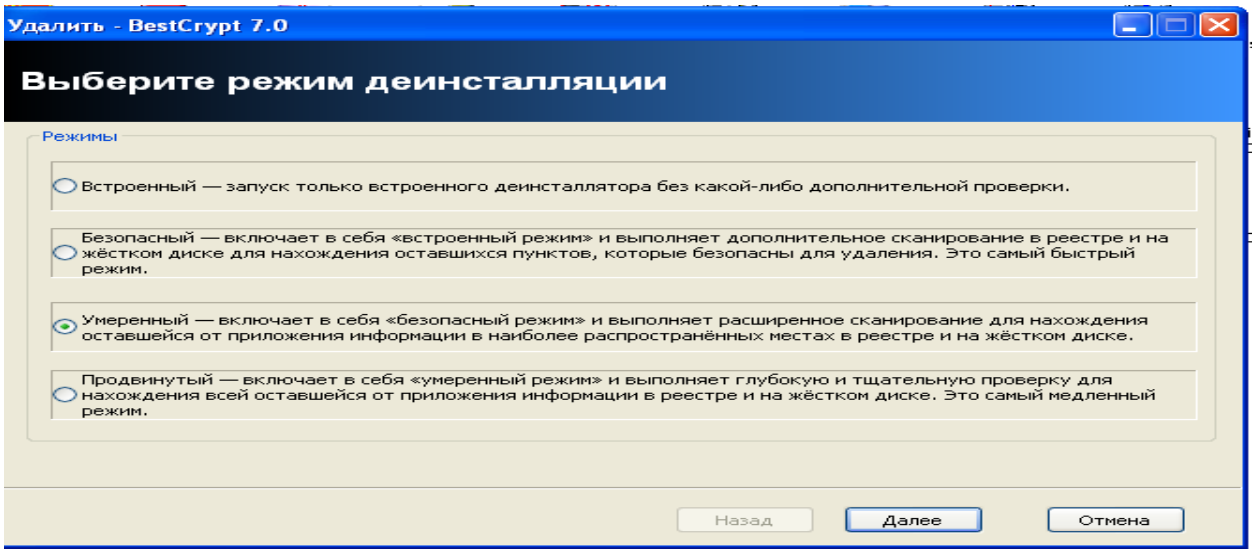


Рис. 6 Вікно майстра видалення програм.

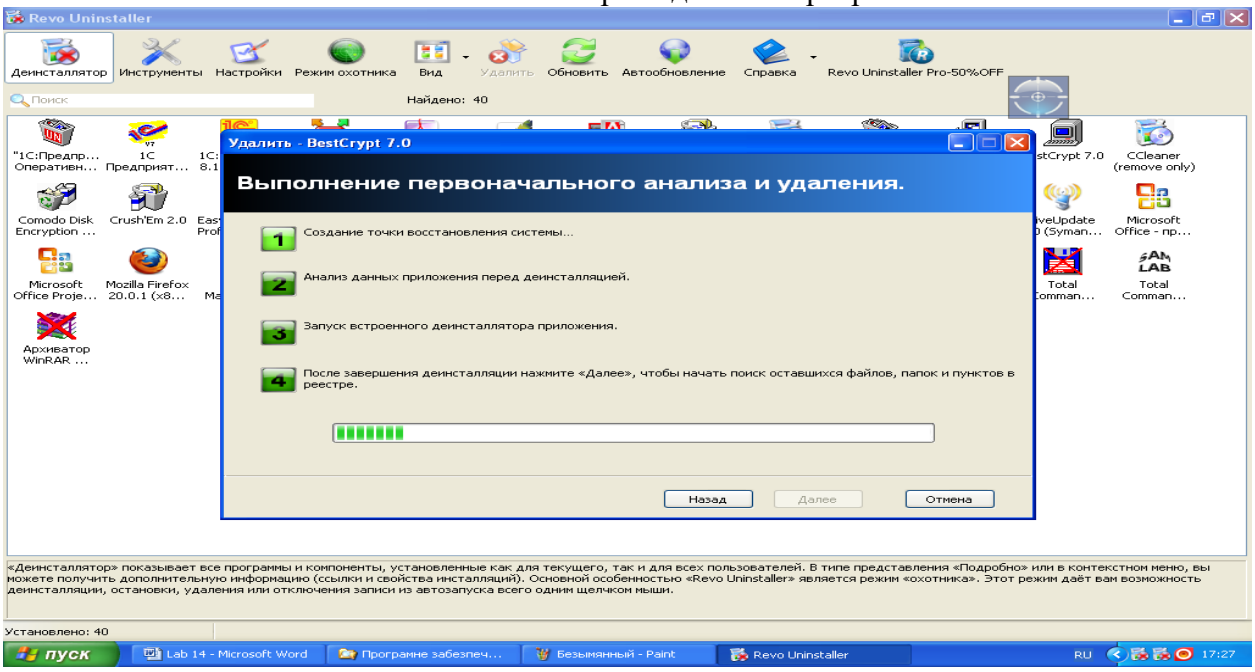


Рис. 7 Процес деінсталяції

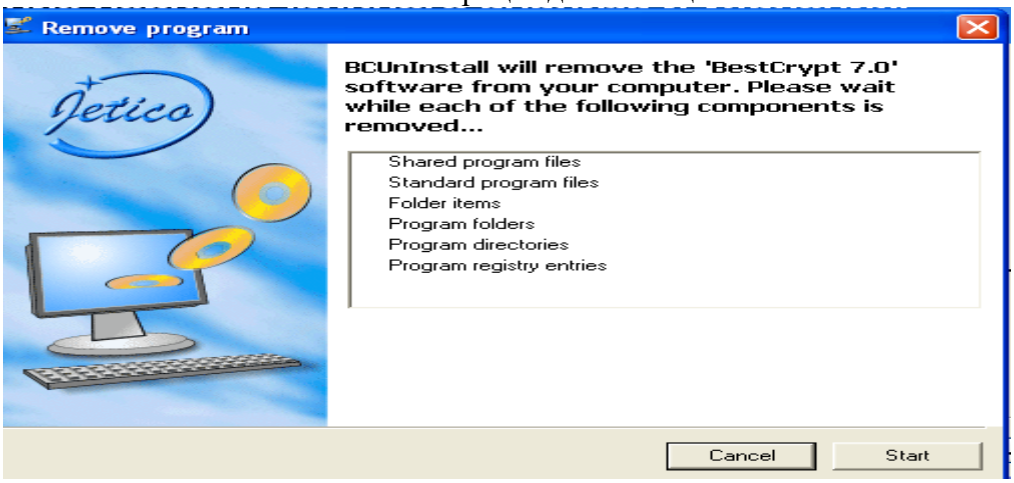


Рис. 8 Стартове вікно внутрішнього деінсталятора програми.

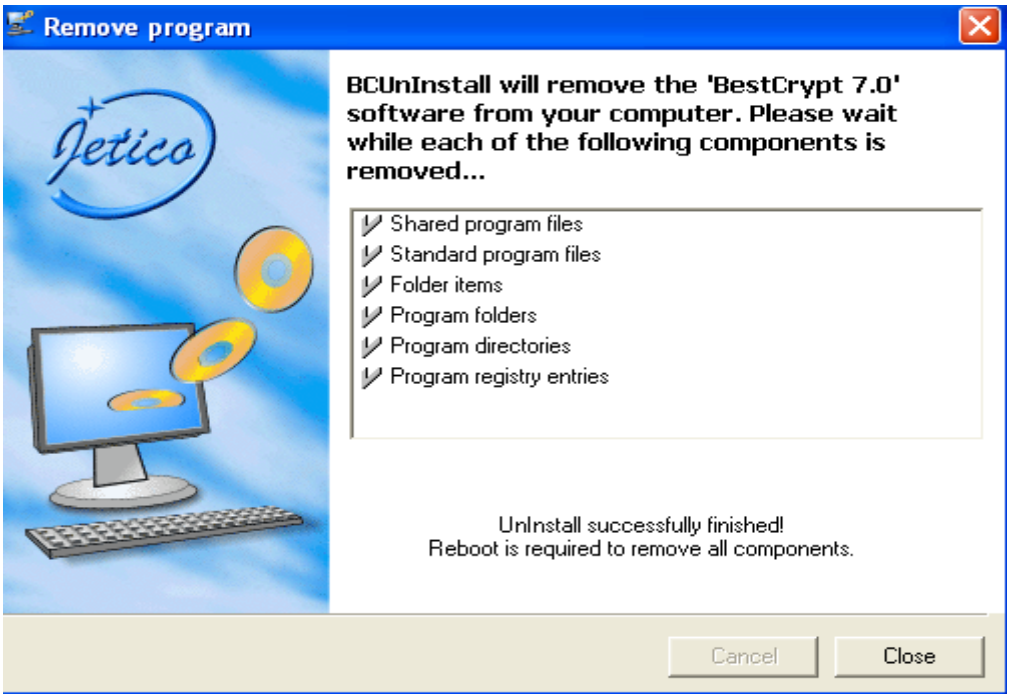


Рис. 8 Завершення роботи внутрішнього деінсталятора.

Якщо після завершення роботи внутрішнього деінсталятора буде запропоновано перезавантажити комп'ютер, відмовтеся від вказаної пропозиції, введіть команду **Далее**. Почнеться процес пошуку елементів програми (рис. 9), які не були видалені внутрішнім деінсталятором. Після введення команди Далее відкриється вікно зі знайденими даними в реєстрі Windows (рис. 10).

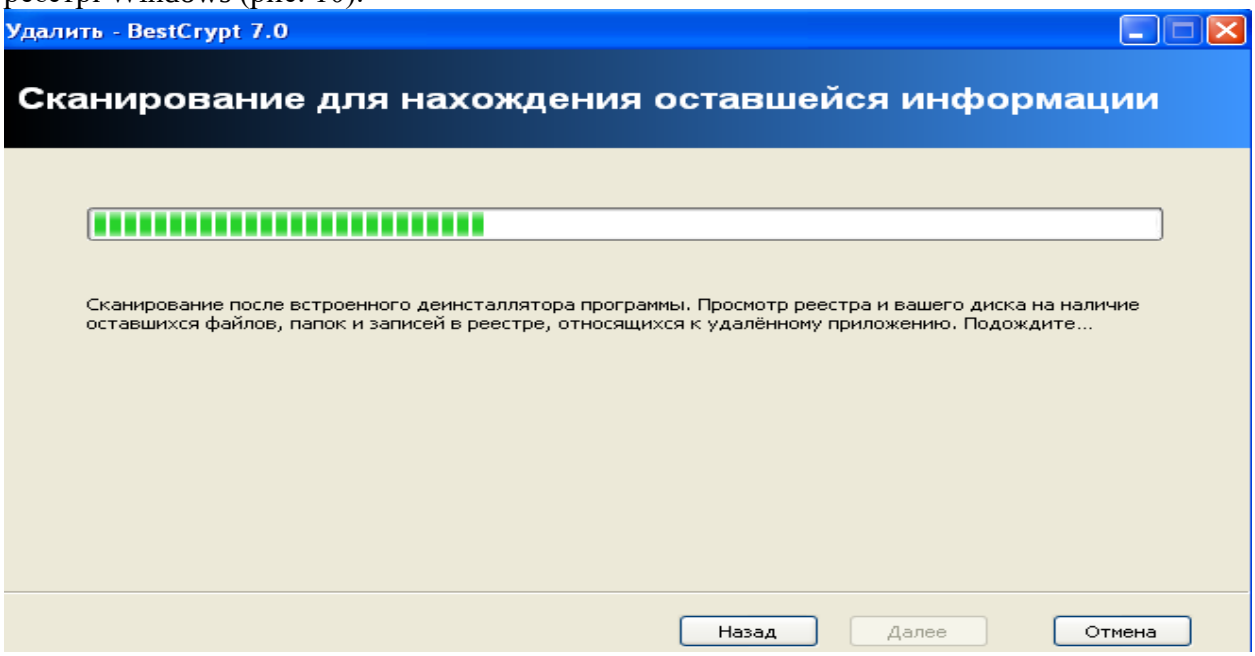


Рис. 9 Процес пошуку елементів програми

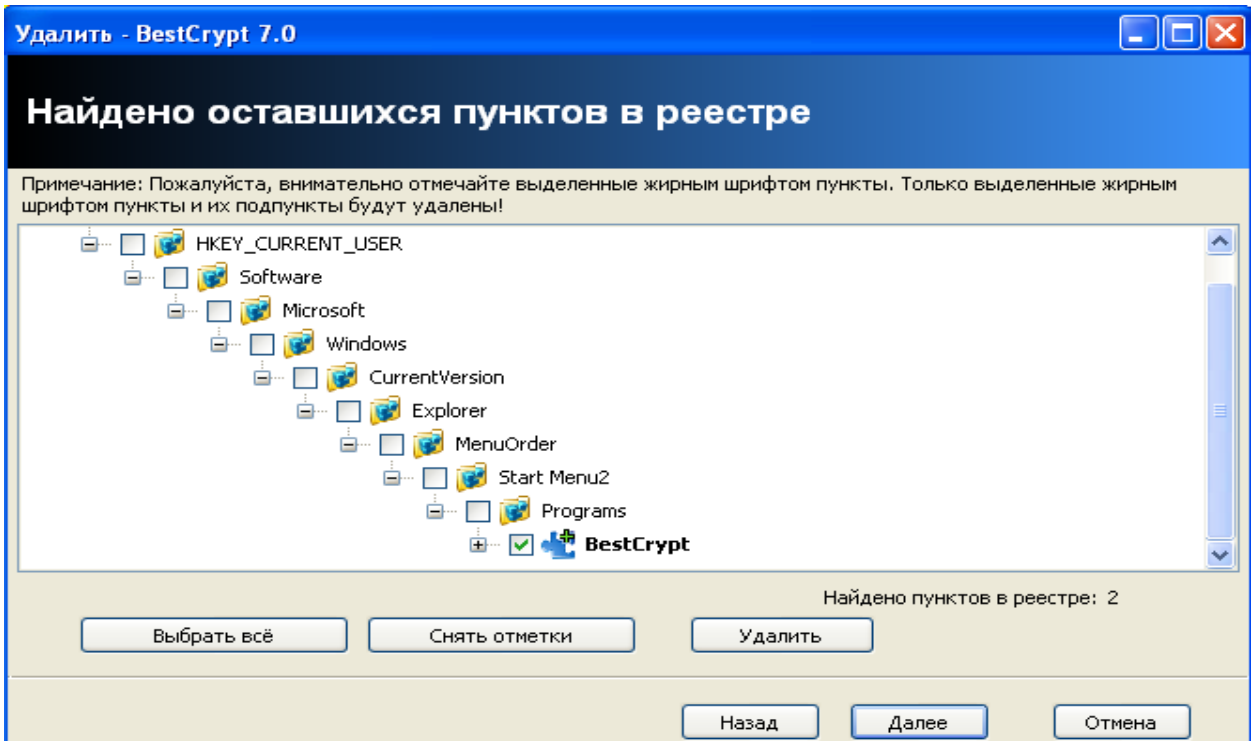


Рис. 10 Елементи програми в реєстрі

Встановіть прапорці біля елементів, які необхідно видалити (проконсультуйтеся обов'язково з викладачем) та введіть команду **Удалить**. Після видалення, введіть команду **Далее** та слідуйте за майстром.

2. Хід роботи

1. Ознайомтеся з програмою її режимами роботи та налагодженням.
2. Проведіть видалення програми за вказівкою викладача (самостійно не вибирати програму для видалення).
3. Обов'язково показати викладачу елементи реєстру, які відмічені для подальшого видалення (тут можливе видалення, яке приведе до подальшої непрацездатності операційної системи).

3. Контрольні питання

1. Які режими роботи програми Ви знаєте?
2. Як налагодити параметри програми?
3. Як перейти в режим мисливця та які команди доступні в цьому випадку?
4. Чи потрібно окремо включати внутрішній деінсталятор програми?
5. До чого може привести неграмотне видалення даних з реєстру операційної системи?
6. Яка послідовність видалення програми?

Лабораторна робота 26. Програма роботи з дисками та томами Acronis Disk Director

Зміст

1. Теорія

1.1. Основні можливості програми

В Acronis Disk Director передбачена безліч функцій, включаючи наступні.

- Створення базових і динамічних томів

Зручний майстер створення томів удосконалений і тепер підтримує створення динамічних томів. Тепер крім базових томів в Acronis Disk Director легко створювати динамічні томи, що дозволяє:

- збільшувати розмір тому понад ємність одного диска, використовуючи складові тому;
- зменшувати час доступу до файлів за допомогою того, що чередується том;
- забезпечувати перешкодостійкість за допомогою дзеркального тому.

- Додавання, видалення й поділ дзеркальних томів

Базовий або простий тому можна зробити перешкодостійкість усього однією дією — шляхом додавання дзеркала. Якщо потрібно додатковий незайнятий простір на диску, де перебуває одне із дзеркал, вилучіть дзеркало. Розділіть дзеркальний том, щоб одержати два незалежні прості томи з ідентичним вихідним умістом.

- Копіювання або переміщення тому одного типу як тому іншого типу

При копіюванні або переміщенні тому змініть його тип. Наприклад, уміст дзеркального тому можна копіювати в складовій тому.

Перетворення основних томів у логічні й навпаки

Перетворіть основний том в логічний для створення п'ятого тому на диску, де в цей момент уже є чотири основні томи.

Перетворення базових дисків у динамічні й навпаки

Перетворіть існуючі базові диски в динамічні, що підвищує надійність диска, використовуваного в якості сховища даних.

Перетворення Gpt-Дисків в Mbr-Диски й навпаки

Схему розділів диска можна змінити необхідним чином.

Імпорт чужих дисків

Динамічні диски, додані з іншої машини, можна зробити доступними в системі.

Зміна статусу диска: з оперативного на автономний і навпаки

Змініть статус диска на автономний, щоб захистити його від ненавмисного використання.

Клонування диска

За допомогою майстра клонування дисків можна замінити старий основний Mbr-Диск на новий без переустановки операційних систем і додатків. Майстер переносить усі дані з вихідного диска на цільовий. Том вихідного диска можна клонувати на цільовий диск «один в один» або змінювати їхній розмір автоматично з урахуванням розміру цільового диска.

Операції по керуванню дисками й томами

Нижче перерахований широкий спектр операцій по керуванню дисками й томами.

Зміна розміру, переміщення, копіювання, поділ і об'єднання дисків без втрати й знищення даних.

Форматування томів, присвоєння їм міток і букв, а також перемикання томів в активний стан.

Ініціалізація недавно доданих жорстких дисків.

Видалення томів.

Зміна файлових систем.

Очищення дисків.

Приховання й відображення томів.

Вказівка щільності i-node.

Зміна розміру кластера.

Огляд даних томів (навіть Linux) перед виконанням операцій.

Перегляд змін, внесених у структуру диска й тому до застосування цих змін.

Перегляд докладної інформації про всі жорсткі диски, томи в файлових системах.

Acronis Recovery Expert

Допомагає відновлювати випадково загублені або вилучені томи на основних Mbr-Дисках.

Майстер створення завантажувальних носіїв Acronis

Тепер можна створювати завантажувальні носії на основі як Winpe, так і Linux для використання Acronis Disk Director на чистій машині або без операційної системи.

Acronis Disk Editor

Професійний засіб для виконання різних дій над жорстким диском.

Журнал

Дозволяє переглядати інформацію про операції з дисками й томами, у тому числі з'ясовувати причини збоїв, якщо вони виникають.

1.2. Вимоги до встаткування та операційних систем

У таблиці 1 наведені мінімальні й рекомендовані вимоги до встаткування для установки й запуску Acronis Disk Director.

Таблиця 1

Мінімальні й рекомендовані вимоги до встаткування для установки й запуску Acronis Disk Director

Елемент	Мінімальні вимоги	Рекомендовані
Мікропрограма завантаження	На основі BIOS На основі UEFI	
Процесор	Сучасний процесор, 800 МГц або більш	Процесор 1 ГГц, 32-розрядний (x86) або 64-розрядний (x64)
Системна пам'ять	256 МБ	512 МБ або більш
Дозвіл екрана	800 x 600 пікселів	1024 x 768 пікселів або більш
Місце на диску для установки	150 МБ	
Інше встаткування	Миша	Пристрій запису CD/DVD або флэш-накопичувач для створення завантажувального носія

1.2.1.Операційні системи, які підтримуються програмою

Acronis Disk Director підтримує наступні операційні системи:

- Windows XP — усі випуски
- Windows Vista — усі випуски
- Windows 7 — усі випуски
- Windows 8 — усі випуски
- Windows 8.1 — усі випуски
- Windows 10 — усі випуски

1.2.2. Файлові системи, які підтримуються програмою

Acronis Disk Director підтримує виконання операцій у наступних файлових системах:

- FAT16
- FAT32

- NTFS
- Ext2
- Ext3
- Reiser3
- Linux SWAP

Операції, що змінюють розмір тому, такі як Создать, Изменить размер, Копировать, Переместить, Об'єднати й Розділити, недоступні для файлових систем XFS, Reiser4 і HPFS.

1.3. Підтримувані носії та томи

- Жорсткі диски (HDD) і твердотільні накопичувачі (SSD)
- Підтримка інтерфейсів IDE, SCSI і SATA
- CD-R/RW, DVD-R/RW, DVD+R (у тому числі двошарових DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE для створення завантажувальних носіїв
- Жорсткі диски USB 1.1 / 2.0 / 3.0 і Firewire (IEEE-1394)
- Пристрою зберігання PC card

Читання перезаписуваних дисків в Linux неможливо без установки відповідних відновлень ядра операційної системи.

Потрібне перезавантаження, якщо на флэш-накопичувачі USB виконується одна з наступних операцій з томами: зміна розміру, поділ, переміщення, видалення, перетворення, зміна розміру кластера.

1.3.1. Базові й динамічні диски

Кожний диск у машині выдноситься до одному із двох типів: базовому або динамічному.

Базові диски

Споконвічно на більшості машин установлені диски саме цього типу.

Базові диски звичайно можна використовувати з кожної операційною системою, у тому числі з будь-якою версією Windows.

На базовому диску може зберігатися один або кілька томів, які називаються базовими. Базовий том не може займати більш одного диска.

Випадки використання базових дисків:

- якщо на машині тільки один жорсткий диск;
- якщо на машині встановлена стара ОС Windows або ОС, відмінна від Windows.

За допомогою Acronis Disk Director можна перетворити базовий диск у динамічний.

Динамічні диски

Можливості цих дисків набагато ширшы, ніж у базових.

Динамічні диски підтримуються тільки ОС Windows, починаючи з Windows 2000.

На динамічному диску може зберігатися один або кілька томів, які називаються динамічними. На відміну від базового тому, динамічний том може займати кілька дисків.

Випадки використання динамічних дисків. Динамічні диски найбільш ефективні, якщо на машині кілька твердих дисків. У цьому випадку доступні наступні можливості:

- Створення більших томів, що займають кілька дисків.
- Забезпечення перешкодостійкості системи й даних шляхом додавання дзеркального тому на іншому диску (наприклад, для тому з операційною системою). Якщо диск із одним з таких дзеркал виходить із ладу, втрати даних тому не відбувається.

За допомогою Acronis Disk Director можна перетворити динамічний диск у базовий. Це може знадобитися, наприклад для установки на цей диск операційної системи, відмінної від Windows.

Перетворення динамічного диска в базовий може зажадати видалення деяких томів на ньому, наприклад томів, що займають кілька дисків

1.3.2.Типи базових томів

На базовому диску можуть зберігатися два типи томів: основні й логічні.

Основна відмінність між основним і логічним томом полягає в тому, що основний том може використовуватися як системний або активний тому, тобто том, з якого запускається машина або завантажується встановлена на ній операційна система Windows.

На кожному базовому Gpt-GPT-диску можна створити до 128 основних томів. Максимальний розмір тому на Gpt-Диску становить 16 экзабайт.

На відміну від базових Gpt-Дисків, на кожному базовому Mbr-MBR-диску може втримуватися до чотирьох основних томів або до трьох основних томів і необмежена кількість логічних томів. Максимальний розмір тому на Mbr-Диску рівний 2 ТБ.

Якщо використовувати більш чотирьох томів на диску не планується, то всі томи можуть бути основними. А якщо ні, то активний і системний томи можна залишити основними, а потім створити необхідне число логічних томів.

Якщо на диску вже є чотири основні томи, але необхідно створити п'ятий том, спочатку перетворіть один з томів (але не системний і не активний) у логічний том, як описано в розділі Преобразование основного тома в логический, а потім створіть новий логічний том.

Типи динамічних томів

Далі перераховані типи динамічних томів, які підтримуються в Acronis Disk Director (за умови, що вони підтримуються операційною системою, як описано в розділі (Поддержка типов динамических томов).

1.3.3. Підтримка

Том, що складається з дискового простору одного динамического диска.

Фізично **простий том** може займати дві або кілька областей дискового простору, які логічно можна представити як одну безперервну область. Якщо простий том розширити на інший диск, він стає складним томом. Якщо до простого того додати дзеркало, він стає зеркальным томом.

Складений том. Том, що складається з дискового простору двох або декількох динамических дисков, розміри яких не обов'язково рівні. Складовій тому може розміщатися на 32 дисках. На відміну від зеркального тому й тому RAID-5, складені томи не є перешкодостійкими. На відміну від томов, що чередуються, складені томи не забезпечують більш швидкого доступу до даних.

Том що чергується. Том, розташовуваний на двох або декількох динамічних дисках, дані якого рівномірно розподілені по блоках рівного розміру (іменованим блоками чергування) на цих дисках. Доступ до даних на томах, що чергуються, звичайно відбувається швидше, чим на динамічних томах інших типів, оскільки виконується одночасно на декількох жорстких дисках.

На відміну від зеркального тома, том, що чергується, не містить надлишкової інформації, тому не є перешкодостійким. Такий том називають також «томом RAID-0».

Дзеркальний том. Перешкодостійкий том, дані якого дублюються на два фізичних диска. Кожна із двох частин дзеркального тому називається «дзеркалом». Усі дані з одного диска копіюються на інший, щоб забезпечити надмірність даних. Якщо відбувається збій одного жорсткого диска, дані залишаються на іншому жорсткому диску. Зеркалювання томів можна застосовувати також до системному тому і загрузочного тому. Дзеркальний том іноді називається «томом RAID-1».

Примітка. Надмірність, забезпечувана архітектурою динамічних томів, ніколи не виключає необхідність у резервнім копіюванні. Щоб забезпечити безпеку даних, найкраще поєднувати обоє підходів до захисту даних.

1.3.4. Активний, системний і завантажувальний томи

Деякі томи на дисках машини містять відомості, необхідні для запуску машини й для завантаження певних операційних систем. Кожний такий том залежно від його функції називається активним, системним або завантажувальним томом.

Якщо на машині встановлена тільки одна операційна система Windows, то єдиний том часто є одночасно активним, системним і завантажувальним.

У зв'язку зі спеціальними ролями таких томів при виконанні операцій з ними слід працювати особливо уважно. Деякі операції для таких томів можуть виконуватися з обмеженнями (у порівнянні зі звичайними томами).

Активний том. Це тому, з якого машина завантажується після включення.Активний том звичайно містить одну з наступних програм.

- Операційна система.
- Програма, що дозволяє вибрати операційну систему, що запускається (якщо встановлено кілька операційних систем), наприклад завантажник GRUB.
- Засіб діагностики або відновлення, яке запускається до операційної системи, наприклад Відновлення при завантаженні.

В Acronis Disk Director активний том позначений значком, схожим на прапорець

Якщо обраний запуск операційної системи Windows, процес запуску триває з тому, який називається системним томом.

Системний том.Це тому, з якого запускається будь-яка встановлена операційна система Windows, навіть якщо встановлено кілька таких систем.

Системний тому містить файли, необхідні для запуску Windows, у тому числі файли boot.ini і Ntldr.

Завжди існує тільки один системний тому, у той же час кожна із установлених операційних систем Windows звичайно зберігає файли на власному томі,який називається завантажувальним томом.

Завантажувальний том. Це тому, на якім зберігаються файли певної операційної системи Windows.

Завантажувальний том містить такі папки, як папка Program Files і папка Windows.

Примітка. Поняття системного тому й завантажувального тому відносяться тільки до операційних систем Windows.

1.3.5. Підтримка типів динамічних томів

У таблиці 2 наведений список операційних систем, що підтримують ті або інші типи динамічних томів.

Таблиця 2

Список операційних систем, що підтримують ті або інші типи динамічних томів.

	Простий	Складений	Що чергується	Дзеркальний
Windows XP Home	-	-	-	-
Windows XP Professional	+	+	+	-
Windows XP Professional x64	+	+	+	-
Windows Vista Home Basic	+	+	+	-
Windows Vista Home Premium	+	+	+	-
Windows Vista Business	+	+	+	-
Windows Vista Ultimate	+	+	+	-
Windows 7 Starter	+	+	+	-
Windows 7 Home Premium	+	+	+	-
Windows 7 Professional	+	+	+	+
Windows 7 Ultimate	+	+	+	+
Windows 8	+	+	+	+
Windows 8.1	+	+	+	+
Windows 10	+	+	+	+

1.3.6. Вирівнювання томів у дисках з розміром сектору 4 КБ

Коли створюється новий том, його початок вирівнюється за границями фізичних секторів диска. У результаті кожна одиниця розміщення, використовувана файловою системою (кластер), у томі починається й закінчується на границях фізичних секторів диска. Якщо кластери тому вирівняні із секторами, цей тому й усі наступні томи також будуть вирівняні. Якщо кластери не вирівняні із секторами, томи будуть невірно вирівняні. Невірне вирівнювання знижує загальну продуктивність системи й термін служби встаткування.

Коли виникає невірне вирівнювання? Невірне вирівнювання тому виникає, коли том створюється на сучасному накопичувачі HDD або SSD з розміром сектору 4 КБ із використанням операційних систем Windows до версії Vista.

Причини невірного вирівнювання. Усі операційні системи Windows до версії Vista використовують 512-бітовий коефіцієнт для створення кластерів томів. Початок тому вирівнюється по 512-бітовим секторам. Також ці операційні системи використовують схему адресації циліндр/головка/сектор (CHS). Тому, створені за цією схемою, вирівнюються по дискових циліндрах/доріжках.

Звичайно доріжка складається з 63 фізичних секторів. Оскільки перша доріжка залишена для основного завантажувального запису (MBR) і інших службових цілей, перший том починається з початку другої дискової доріжки. Тому том, вирівнюється по 63 секторах, не вирівнюється з 4-килобайтными секторами: 63 сектору по 512 байт не відповідають цілому числу 4-килобайтных секторів.

Таким чином, перший створений тому й усі наступні томи на жорсткому диску будуть вирівняні невірно.

Чому невірне вирівнювання — серйозна проблема для жорстких дисків

Коли міняється один біт даних, операційна система повністю перезаписує кластер, що містить змінені дані. Однак при невірнім вирівнюванні кластер буде перекривати більше фізичних секторів, чим займав би при правильнім вирівнюванні. У результаті при кожній зміні даних потрібно стирати й перезаписувати більше фізичних секторів.

Зайві операції читання/запису значно сповільнюють швидкість диска й у цілому продуктивність системи.

Це також справедливо для накопичувачів SSD з розміром сектору (сторінки пам'яті) 4 КБ або більше. У накопичувачів SSD невірне вирівнювання знижує не тільки продуктивність системи, але й термін служби накопичувача. Комірки пам'яті SSD розраховані на певне число операцій читання/запису. Тому зайві операції читання/запису ведуть до раннього руйнування накопичувача SSD.

Як уникнути невірного вирівнювання тому

Новітні операційні системи, починаючи з Windows Vista, уже підтримують новий розмір секторів. Тому томи, створені цими операційними системами, будуть вирівняні правильно.

Багато виробників жорстких дисків поставляють сучасні диски разом з контролерами, які можуть перенести зсув при адресації на один сектор (63 сектор стає 64 сектором), і тому будуть вирівняними.

Як працювати з дисками з розміром сектору 4 КБ, використовуючи Acronis Disk Director

Припустимо, ви додали новий жорсткий диск із розміром сектору 4 КБ на машину, яка працює тільки під керуванням Windows XP. На цьому диску поки немає томів. Якщо почати створення томів на цьому диску, використовуючи Windows XP, продуктивність системи може знизитися при звертанні до диска. Щоб забезпечити правильне вирівнювання томів і нормальний доступ до томів на цьому диску, виконаєте наступні дії.

Створіть завантажувальну носій з Acronis Disk Director — див. розділ Створення завантажувального носія. Запустіть Acronis Disk Director із завантажувального носія — див. розділ Запуск Acronis Disk Director. Виберіть структуру диска для ОС завантажувального носія — див. розділ Структура диска.

Якщо крім Windows XP також установлена операційна система Windows Vista, Windows 7, Windows 8 або Windows 10, виберіть структуру диска для кожної із цих операційних систем.

Після створення томів над ними можна виконувати інші операції (включаючи зміну розміру) у будь-якій структурі диска.

Як виправити невірне вирівнювання томів за допомогою Acronis Disk Director?

Припустимо, ви вже створили базові томи на диску з розміром сектору 4 КБ, використовуючи Windows XP. Томи вже містять дані. Щоб вирівняти невірно вирівняні томи на диску за допомогою Acronis Disk Director, виконаєте клонування цього диска на інший, а потім назад — див. розділ Клонирование диска. Після клонування Acronis Disk Director перенесе початок першого тому зі зсувом 1 МБ, і всі томи диска будуть вирівняні правильно.

1.3.7. Обережності

Щоб уникнути можливого ушкодження структури тому або диска або втрати даних слід ухвалювати всі необхідні запобіжний заходи й слідувати наведеним нижче простим правилам.

1. Створіть резервні копії дисків, у томи яких планується вносити зміни. Наявність резервної копії найважливіших даних на іншому жорсткому диску або компакт-диску дозволяє працювати з томами диска, забезпечивши захист даних.

Компанія Acronis пропонує винятково ефективний універсальний розв'язок для резервного копіювання й відновлення даних — Acronis True Image. Воно створює резервну копію даних або диска в стислому архівному файлі, з якого дані можна відновити у випадку неполадок.

2. Перевірте тома, щоб переконатися, що вони повністю працездатні й не містять ушкоджених секторів або помилок у файлових системах.

3. Не виконуйте операції з дисками/томами під час роботи інших програм, що здійснюють доступ до дисків на низькому рівні. Acronis Disk Director повинен одержати монопольний доступ до цільового диска/тому. Це означає, що одночасно доступ до диска не зможуть одержати ніякі інші дискові утиліти (наприклад, утиліта керування дисками Windows). Якщо з'являється повідомлення, що диск або тому не вдається заблокувати, закрийте додатки керування дисками, що використовують цей диск або том, і повторіть спробу. Якщо не вдається визначити, які додатки використовують диск або тому, закрийте їх.

Ці прості запобіжний заходи дозволяють запобігти випадковій втраті даних

1.4. Запуск Acronis Disk Director в Windows

1. Натисніть кнопку **Пуск** і виберіть пункт меню > **Усі програми** -> **Acronis** -> **Disk Director** -> **Acronis Disk Director**.
2. В області керування диском перевірте поточну структуру дисків і томів.
3. Додайте одну або кілька операцій керування дисками й томами в чергу запланованих операцій. Ці операції набудуть чинності тільки після їхнього застосування.
4. В області керування дисками перевірте майбутній вид структури дисків і томів після завершення запланованих операцій.
5. Застосуйте заплановані операції.

Для виконання деяких операцій, наприклад зміни розміру тому, з якого запускається Windows, може знадобитися перезапуск машини

1.4.1. Головне вікно Acronis Disk Director

Головне вікно Acronis Disk Director (рис. 1) — це основний інтерфейс для роботи із продуктом.

1. **Меню**. Меню надає доступ до всіх дій, засобів і настроюванням продукту Acronis Disk Director.

2. **Панель інструментів**. На панелі інструментів відображається поточна структура диска. Панель дозволяє виконувати наступні дії над запланованими операціями: застосування, скасування й повтор, керування дисками. Область керування дисками містить таблицю дисків і томів, а також графічну панель.

3. **Таблиця**. У таблиці перелічуються всі диски і їх томи. Кожен із цих об'єктів можна вибрати для виконання над ним операцій. Том можна відсортувати по стовпцях. Клацніть заголовок стовпця, щоб відсортувати том в зростаючому порядку. Клацніть його ще раз, щоб відсортувати том в зворотному порядку. При необхідності можна сховати відображувані стовпці й відобразити сховані.

Як відобразити або сховати стовпці?

1. Клацніть правою кнопкою миші заголовок будь-якого стовпця, щоб відкрити контекстне меню. Відзначені прапорцями пункти меню відповідають заголовкам стовпців у таблиці.
2. Виберіть елементи, які потрібно відобразити або сховати.

4. **Графічна панель.** Графічна панель містить візуальну інформацію про всі диски і їх томи. Вона спрощує розуміння конфігурації томів. Графічна панель також дозволяє вибирати том й диски для виконання операцій над ними.
5. **Панель «Дії й інструменти».** Надає швидкий доступ до операцій, які можна виконати над обраним диском або томом, а також до інструментів Acronis.

2.

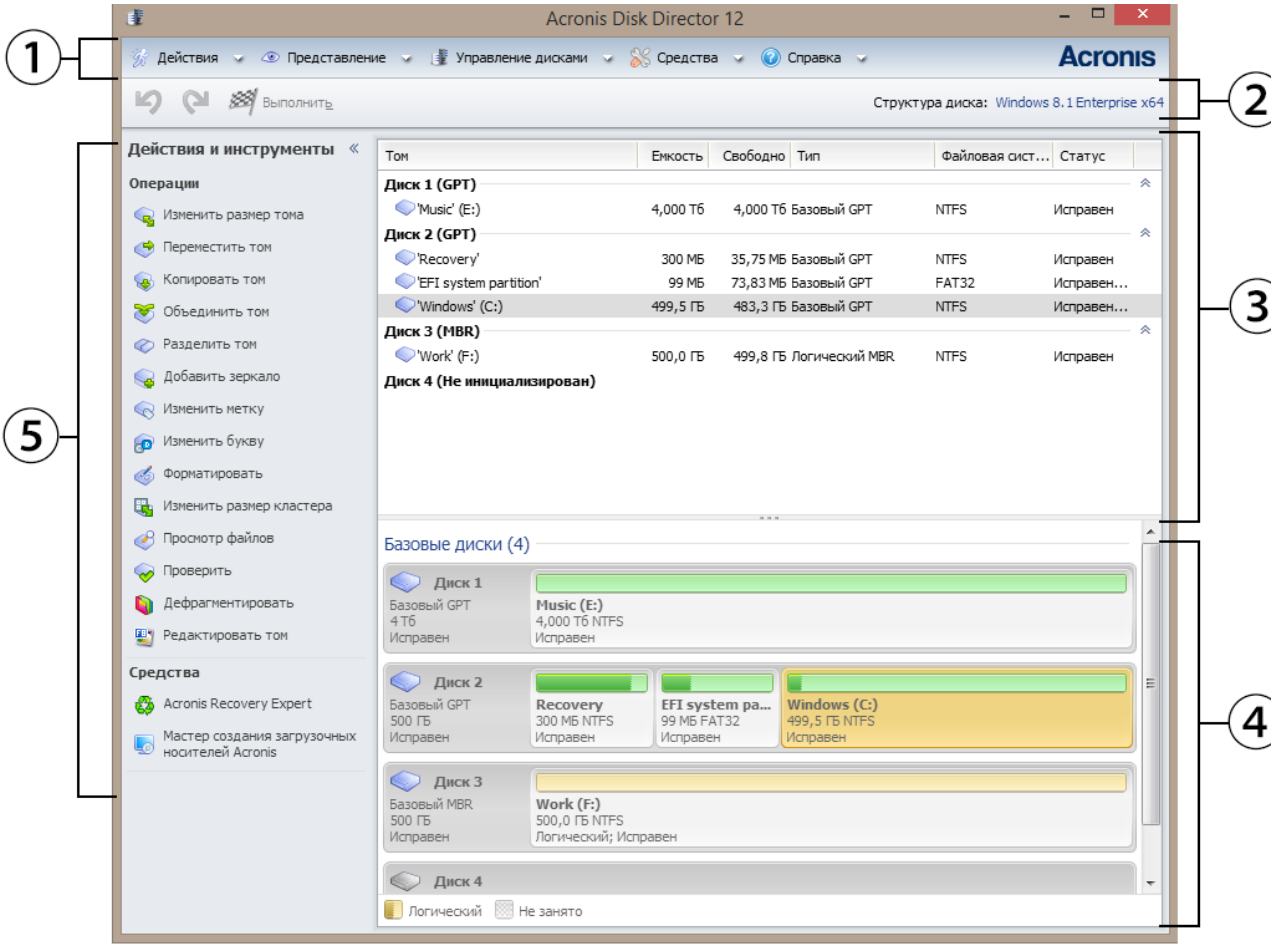


Рис. 1 Головне вікно Acronis Disk Director

1.4.2. Статуси дисків

Перевірити наявність неполадок у роботі диска можна за допомогою статусу диска. Статуси дисків відображаються в графічній панелі під даними про їхню ємність.

Нижче наведені короткі описи статусів, що найбільше часто зустрічаються.

- Оперативний

Базовий або динамічний диск доступний і працює правильно. Це нормальний статус диска. Диск можна перемкнути з оперативного режиму в автономний.

- Оперативний (з помилками)

На динамічному диску виявлені помилки вводу-виводу. Якщо на диску виявлені помилки, рекомендується якомога швидше виконати, выдновлення, щоб запобігти втраті даних.

- Автономний

Динамічний диск доступний у режимі тільки для читання (якщо раніше був переключений в автономний режим) або взагалі недоступний (якщо ушкоджений або періодично не готовий). Диск, раніше переключений в автономний режим, можна зробити знову повністю доступним.

- Чужий

Цей статус виникає при переміщенні динамічного диска на дану машину з іншої машини. Для доступу до даних на чужих дисках необхідно додати ці диски в системну конфігурацію машини, перетворити їх у базові диски.

- Выдсутній

Динамічний диск ушкоджений, відключений або в нього відключене живлення.

- Не ініціалізовано

Диск не містить дійсного підпису. Після установки новий диск повинен бути зареєстрований в операційній системі. Тільки після цього можна створювати том на цьому диску.

1.4.3. Статуси томів

Перевірте статус тому, щоб переконатися, що він доступний і працює без неполадок. Статуси томів відображаються й у таблиці, і на графічній панелі. Нижче наведені короткі описи статусів, що найбільше часто зустрічаються, томів:

- Справний

Базовий або динамічний тому доступний і працює правильно. Це нормальний статус тому. Статус Справний часто має трохи пыдстатусыв, які відображаються в табличній виставі (у дужках) і в графічній виставі (під розміром тому, через крапку з комою). Підстатуси Системний, Завантажувальний і Активний найпоширеніші.

Справний том, файлова система якого ушкоджена, позначається наступним значком: 

- Несправний

Динамічний том (, що чергується або складений) не може бути запущений автоматично, або відсутній один з необхідних для його роботи дисків.

- Збій надмірності

Дані на дзеркальному томі більше не є перешкодостійкими, оскільки один з динамічних дисків не працює в оперативному режимі. Доступ до нього можливий доти, поки в оперативному режимі працює динамічний диск, що залишився. Щоб уникнути втрати даних, рекомендується якомога швидше відновити том.

1.4.4. Структура диска

На машині із двома або декількома ОС позначення дисків і томів залежить від того, яка ОС запущена в цей момент.

У різних ОС Windows том може мати різні букви. Наприклад, том E: може відображатися під літерою D: або L: при завантаженні іншої ОС Windows, установленої на тій же машині. Також можливо, що цей том буде позначатися однієї й тою же буквою E: у всіх ОС Windows, установлених на машині. Більше того, динамічний диск, створений в одній ОС Windows, уважається чужим диском в інший ОС Windows або навіть не підтримується.

Якщо на такій машині потрібно виконати операцію по керуванню дисками, необхідно вказати, у який ОС вона буде виконана, тобто вказати структуру дисків.

Ім'я поточної ОС відображається на панелі інструментів відразу після пункту Структура дисків:. Клацніть ім'я потрібної ОС, щоб вибрати іншу ОС у вікні Вибір операційної системи.

На завантажувальному носії це вікно відображається відразу після запуску програми Acronis Disk Director. Структура дисків буде відображатися відповідно обраної ОС.

1.4.5. Заплановані операції

Майже всі операції виявляються запланованими до їхнього підтвердження. До цього моменту Acronis Disk Director тільки демонструє нову структуру томів, яка буде залежати від операцій, запланованих для виконання с дисками й томами.

Такий підхід дозволяє управляти всіма запланованими операціями й двічі перевіряти ще раз необхідні зміни, а при необхідності скасовувати операції до того, як вони будуть дійсно виконані.

Усі заплановані операції додаються в список операцій, що очікують, який можна переглянути у вікні Заплановані операції.

Як переглянути й підтвердити заплановані операції?

На панелі інструментів натисніть кнопку **Підтвердити заплановані операції**.

У вікні **Заплановані операції** можна переглянути й перевірити список запланованих операцій.

Щоб виконати операції, натисніть кнопку **Продовжити**. Після цього ні одну із цих операцій не можна буде скасувати.

Щоб вийти з вікна **Заплановані операції** без підтвердження, натисніть кнопку **Скасування**.

При спробі вийти з Acronis Disk Director без підтвердження запланованих операцій програма попросить їх підтвердити. Якщо вийти із програми без застосування запланованих операцій, вони будуть скасовані.

Будь-яку заплановану операцію можна як скасувати, так і повторити.

Щоб скасувати останню заплановану операцію в списку,

виконайте одну з наступних дій. Натисніть кнопку **Скасувати** на панелі інструментів.

Натисніть клавіші **Ctrl + Z**.

У результаті скасування однієї операції можуть бути скасовані інші заплановані операції. Коли в списку є операції, ця дія доступна.

Щоб повторити останню скасовану заплановану операцію, виконайте одну з наступних дій. Натисніть кнопку **Повторити** на панелі інструментів. Натисніть клавіші **Ctrl + Y**.

1.4.6. Дії із записами журналу

Виконайте команди **Представление/Показать журнал**. Щоб виконати кожну з описаних нижче операцій, потрібно клацнути відповідний елемент на панелі інструментів журналу (табл. 3).

Таблиця 3

Операції з журналом

Ціль	Дії
Вибрати один запис журналу	Клацніть запис журналу.
Вибрати кілька записів журналу	• *що йдуть не підряд*: утримуючи клавішу **CTRL**, клацніть кожнен з потрібних записів; • *що йдуть підряд*: виберіть один запис журналу, потім, утримуючи клавішу **SHIFT**, клацніть іншу. Будуть виділені всі записи між першого до останнього.
Перегляд докладних відомостей про запис журналу	1. Виберіть один запис журналу. 2. Виконайте одну з наступних дій. • Клацніть Перегляд відомостей. Докладні відомості про запис журналу будуть показані в окремім вікні. • Розгорніть панель Інформація, клацнувши подвійну кутову дужку .
Зберегти виділені записи журналу у файлі	1. Виберіть одну або кілька записів журналу. 2. Клацніть Зберегти обрані у файл. 3. Відкриється вікно, у якім потрібно вказати шлях і ім'я файлу.
Зберегти всі записи журналу у файлі	1. Переконайтеся, що не заданий жоден фільтр. 2. Клацніть Зберегти все у файл. 3. Відкриється вікно, у якім потрібно вказати шлях і ім'я файлу.
Зберегти у файлі всі записи журналу, відібрані за	1. Задайте фільтри, щоб одержати список записів журналу, що задовольняють критеріям фільтрації. 2. Клацніть Зберегти все у файл.

допомогою фільтра	3. Відкриється вікно, у якім потрібно вказати шлях і ім'я файлу. У результаті будуть збережені всі записи журналу із цього списку.
Вилучити всі записи журналу	Клацніть Очистити журнал. Усі записи будуть вилучені з журналу, і з'явиться новий запис про це. У ньому буде інформація про те, хто й коли вилучив записи.

1.4.7. Фільтрація й сортування записів журналу

Нижче (табл. 4) наведені інструкції про дії з фільтрації й сортування записів журналу.

Таблиця 4

Інструкції про дії з фільтрації й сортування записів журналу

Ціль	Дії
Відобразити записи журналу за даний період	1. У поле З виберіть дату, починаючи з якої потрібно відобразити запису журналу. 2. У поле По виберіть дату, до якої потрібно показати запису журналу.
Відфільтрувати записи журналу по власникові й коду	Уведіть потрібне значення (ім'я власника, код) у поле під заголовком відповідного стовпця. У результаті відображається список записів журналу, які повністю або частково збігаються з уведеним значенням.
Відфільтрувати записи журналу по типу	Натисніть або відіжміть наступні кнопки на панелі інструментів: , щоб відфільтрувати повідомлення про помилки; , щоб відфільтрувати попереджуючі повідомлення; , щоб відфільтрувати інформаційні повідомлення.
Сортувати записи журналу зак датою й часом, типом, повідомленню	Клацніть заголовок стовпця, щоб сортувати записи журналу по зростанню. Клацніть його ще раз, щоб сортувати записи журналу по убуванню.

За замовчуванням у таблиці є три відображувані стовпці. Інші стовпці сховані. При необхідності можна сховати відображувані стовпці й відобразити сховані.

Як відобразити або сховати стовпці?

1. Клацніть правою кнопкою миші заголовок будь-якого стовпця, щоб відкрити контекстне меню. Відзначені прапорцями пункти меню відповідають заголовкам стовпців у таблиці.
2. Виберіть елементи, які потрібно відобразити або сховати

Як зібрати системну інформацію?

1. У верхньому меню виберіть пункт Довідка -> Відомості -> Збір системної інформації.
2. Укажіть місце зберігання файлу із системною інформацією

1.5. Дії з томами

1.5.1.Створення тому

Створення нового тому може знадобитися для наступних цілей:

- зберігання даних, наприклад музичної колекції, фотоальбомів або відеофайлів;

- зберігання архівів (образів) інших томів/дисків (зокрема, завантажувальних томів) для можливості відновлення системи у випадку збою;
- установка нової операційної системи (або створення файлу підкачування).

Як створити том

1. Запустіть майстер створення тому, клацнувши правою кнопкою миші в будь-якім місці незайнятого простору, потім виберіть команду **Створити том**, або вибравши диск виберіть **Змінити розмір тому** (рис. 2).

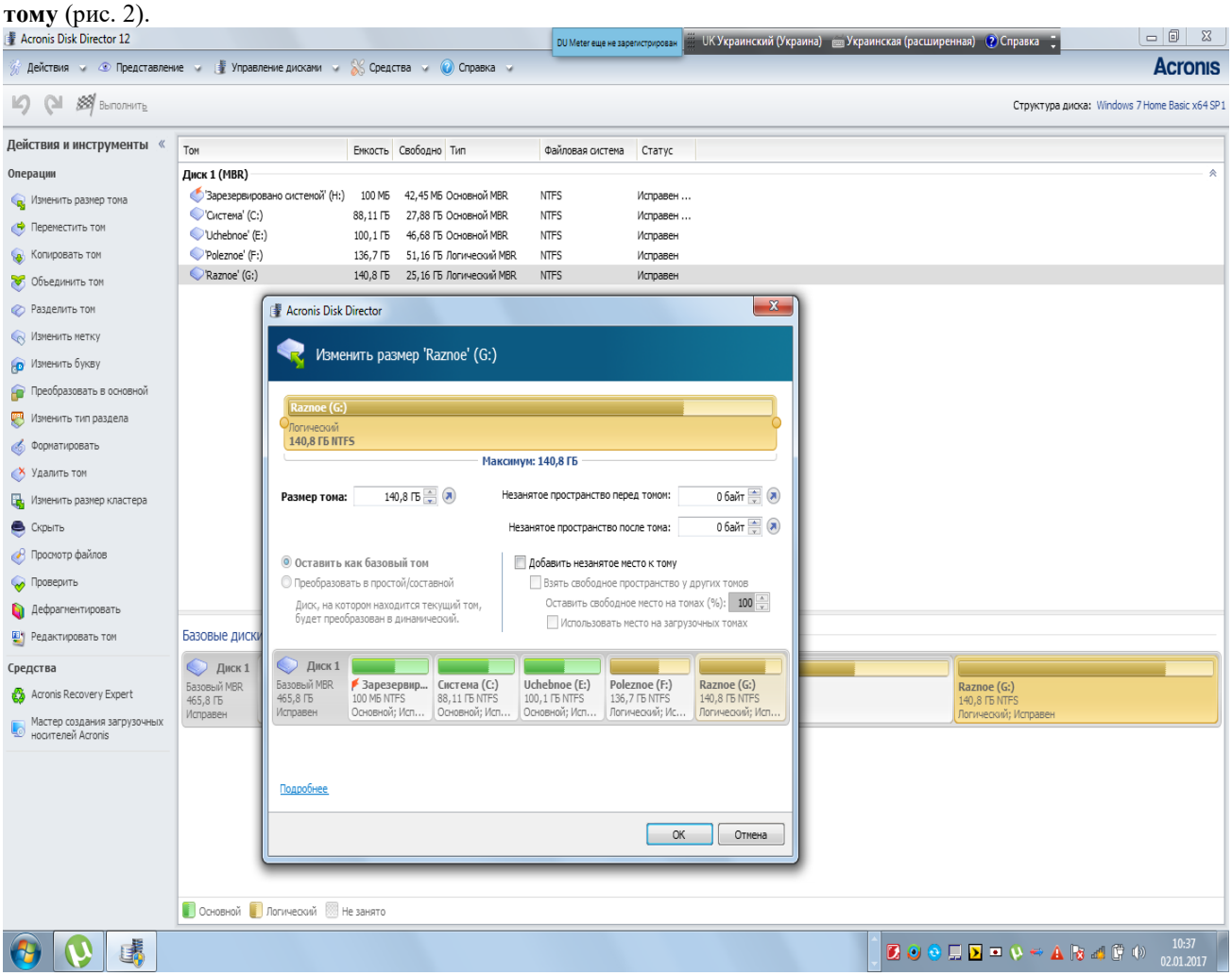


Рис. 2 Створення нового тому

2. Укажіть тип нового тому. Для кожного типу тому виводиться короткий опис, що включає переваги й обмеження при використанні даного типу тому. Список типів томів містить тільки типи, підтримувані поточної операційною системою.

3. Залежно від типу нового тому вкажіть один або кілька дисків, на яких потрібно створити новий том.

- Якщо новий том базовий, виберіть один базовий диск і вкажіть на цьому диску одну область незайнятого простору.

Примітка. Створити базовий тому на диску, що вже містить чотири основні томи, неможливо. Спочатку необхідно перетворити один з існуючих томів у логічний. Це обмеження не ставиться до Gpt-Дискам.

- Якщо новий том простий або складовий, виберіть один або кілька дисків.
- Якщо новий том, що чергується, виберіть два або більш дисків.
- Якщо новий том дзеркальний, виберіть два диски.

Примітка для, тому, що чергуються й дзеркальних томів. Ці томи займають рівне місце на своїх дисках, тому максимальний розмір такого тому буде залежати від обраного диска з меншим обсягом незайнятого простору.

4. При створенні динамічного тому й виборі одного або декількох базових дисків для його розміщення обрані диски будуть автоматично перетворені в динамічні.

5. Укажіть розмір нового тому. За замовчуванням установлюється максимальний розмір тому. Щоб задати інший розмір, перемістіть повзунка або введіть потрібне значення в **поле Розмір** тому.

Якщо після завдання розміру тому на диску усе ще є незайнятий простір, можна задати обсяг незайнятого простору перед базовим томом і за ним. Для цього перетягніть тому в межах незайнятого простору або введіть необхідний обсяг простору перед томом і за ним у відповідні поля.

У діаграмі структури тому в нижній частині вікна можна вказати простір, який том буде займати на кожному з обраних дисків, увівши відповідні обсяги або перетаскуючи повзунки.

6. Укажіть наступні параметри нового тому.

- Файлова система (за замовчуванням NTFS). Деякі з підтримуваних файлових систем можуть бути недоступні залежно від обраних типу й розміру тому. Наприклад, FAT32 буде відключена, якщо обраний розмір тому більше 2 ТБ.
- Розмір кластера. Виберіть розмір кластера — найменший розмір дискового простору, що виділяється для зберігання окремого файлу. Рекомендується залишити розмір за замовчуванням, який відзначений у списку словами (за замовчуванням). Розмір кластера за замовчуванням залежить від розміру тому й типу файлової системи. Наприклад, для томів NTFS обсягом до 2 ТБ за замовчуванням розмір кластера становить 4 КБ.
- Мітка тому (за замовчуванням NONE — «HI»). Коротке ім'я, яке можна привласнити тому, щоб відрізняти його від інших томів. Максимальна довжина мітки тому залежить від файлової системи тому
- Буква (за замовчуванням перша вільна буква алфавіту). Призначте тому букву диска, щоб на ньому можна було знаходити файли й папки.

Якщо новий том є базовим, укажіть, чи буде він основним або логічним.

- Основний. **Виберіть Основний**, якщо планується встановити на цей том операційну систему. Позначте основний том як Активний, щоб машина запускалася із цього тому.
- Логічний. **Виберіть Логічний**, якщо том призначений для зберігання даних.

7. Натисніть кнопку **Готово**, щоб додати операцію створення тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібно підтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

1.5.2. Зміна розміру тому

Операція розширює базовий або динамічний том, використовуючи незайнятий простір на одному або декількох дисках. Вона також може зменшити розмір тому, тоді частина вільного простору тому перетвориться в незайнятий простір диска.

Розширення базового тому. Базовий том займає одну область на одному базовому диску. При розширенні базового тому можна вибрати варіант залишити диск базовим і використовувати тільки суміжний з томом незайнятий простір. Також можна вибрати варіант перетворити диск у динамічний і використовувати незайнятий простір із усіх динамічних дисків на машині. У другому випадку том стане простим або складеним.

Зміна розміру тому, з якого запускається машина або операційна система. Розмір системного, завантажувального або активного томи можна змінити тільки тоді, коли цей тому є базовим.

Як змінити розмір тому?

1. Виберіть том, для якого необхідно змінити розмір, потім виберіть **Змінити розмір тому.**

2. Задайте новий розмір тому, увівши його або перемістивши повзунок.

Зміна розміру базового тому.

- У випадку використання тільки незайнятого простору, суміжного з томом, виберіть варіант **Залишити тому базовим**. Том залишиться базовим томом.

- Щоб використовувати незайнятий простір із усіх динамічних дисків у машині, виберіть варіант **Перетворити том в простий/складений**. Том буде перетворений у простий або складений, а відповідний диск стане динамічним.

Примітка. Якщо том є системним, завантажувальним або активним, цей параметр буде недоступний.

3. Якщо обраний варіант **Залишити том базовим**, доступні наступні варіанти.
   - Додати до того весь незайнятий дисковий простір

За допомогою цього варіанта весь незайнятий простір на диску приєднується до того, розмір якого змінюється. Може знадобитися переміщення інших томів на диску.

У результаті том буде розширений і займе весь незайнятий простір на диску, включаючи простір, на даний момент не суміжний з томом, а диск залишиться базовим.

Якщо встановлений прапорець, буде доступний наступний параметр.

- Використовувати вільний простір інших томів

При установці цього параметра інші томи на диску будуть зменшені й на кожному із цих томів залишиться тільки встановлена частка від наявного вільного простору.

У результаті звільниться додатковий незайнятий простір, суміжний з томом, розмір якого змінюється.

За замовчуванням цей параметр не застосовується до завантажувальних томів на диску. Щоб включити ці томи, установіть прапорець **Використовувати вільний простір на завантажувальних томах.**

4. В області перегляду в нижній частині вікна перевірте розміщення тому зі зміненим розміром на диску (дисках).
5. Натисніть кнопку **ОК**, щоб додати операцію зміни розміру тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібно підтвердити.

1.5.3. Копіювання тому

Ця операція копіює том за допомогою створення нового тому й копіювання в нього вмісту вихідного тому.

На відміну від операції копіювання всіх файлів з тому, копіювання самого тому забезпечує ідентичність усього вмісту томів.

Типи й розміри вихідного й нового томів можуть різнитися. Наприклад, том, що чергується можна скопіювати в простий тому більшого розміру.

Увага! При копіюванні системного, активного або завантажувального томи завантаження машини з нового тому може виявитися неможливою.

Як копіювати том?

1. Виберіть том, який необхідно скопіювати, потім виберіть **Копіювати том**.
2. Виберіть тип нового тому. За замовчуванням обраний тип вихідного тому.
3. Залежно від типу нового тому вкажіть один або кілька дисків, на яких потрібно створити новий тому.
   - Якщо новий том базовий, виберіть один базовий диск і вкажіть на цьому диску одну область незайнятого простору.
   - Якщо новий том простий або складений, виберіть один або кілька дисків.
   - Якщо новий том, що чергується, виберіть два або більш дисків.
   - Якщо новий том дзеркальний, виберіть два диски.

Примітка для, тому, що чергуються й дзеркальних томів. Ці томи займають рівне місце на своїх дисках, тому максимальний розмір такого тому буде залежати від обраного диска з меншим обсягом незайнятого простору.

4. Укажіть розмір нового тому. Цей розмір не може бути менше, ныж простір, який займають дані на вихідному томі. Розмір базового тому можна збільшити тільки шляхом приєднання до нього суміжного незайнятого простору.

На діаграмі структури розділів тому в нижній частині вікна можна задати простір, який буде займати том на кожному з обраних дисків, увівши розміри або перетягнувши повзунок.

5. Натисніть кнопку **Готово**, щоб додати операцію копіювання тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібнопыдтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

1.5.4. Об'єднання базових томів

Дана операція дозволяє об'єднати два суміжні базові томи, навіть якщо їх файлові системи відрізняються. Усі дані зберігаються на результуючому томі. Результуючий том, на який будуть додані дані з іншого тому, буде мати таку ж мітку, букву й файлову систему, що й основний том.

Вимоги до вільного простору. Загальний розмір вільного простору на основному томі й на іншому томі повинен становити не менш 5 відсотків від обсягу даних на іншому томі. Наприклад, якщо файли й папки на іншому томі займають 100 ГБ, необхідно 5 ГБ сумарного вільного простору (припустимо, 2 ГБ на одному томі й 3 ГБ на іншому).

Увага! Томи, що містять зашифровані файли, не можуть бути об'єднані.

Як об'єднати базові томи?

Клацніть правою кнопкою миші по тому, який необхідно об'єднати, і виберіть пункт **Об'єднати томи**.

Виберіть другий том, який необхідно об'єднати.

У поле **Основні томи** вкажіть, який з обраних томів буде вважатися основним. Дані з іншого тому будуть додані в окрему папку на основному томі. Ця папка одержить ім'я відповідно до мітки й буквою тому (при наявності таких), наприклад: Об'єднаний тому 'System' (C).

Натисніть кнопку **ОК**, щоб додати заплановану операцію об'єднання.

У нижній частині вікна відображається вид результуючого тому після об'єднання.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібно підтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

Об'єднання тому NTFS з томом з файловою системою, що не підтримує параметри безпеки (наприклад, FAT32), приведе до втрати налагодження безпеки (відомостей про власників даних і дозволах на доступ). При виконанні протилежної дії (об'єднання небезпечного тому з безпечним) параметри безпеки основного тому будуть привласнені результуючому тому.

1.5.5. Форматування тому

Операція форматування підготовляє том для зберігання файлів і папок, створюючи на ньому файлову систему.

Увага! У результаті форматування будуть знищені всі дані, що зберігаються в даний момент на томі.

Форматування тому може знадобитися в наступних випадках.

- При створенні тому. У цьому випадку вікно форматування з'являється в Майстру створення тому.
- Якщо необхідно швидко знищити дані на томі, наприклад з метою забезпечення безпеки.
- Якщо необхідно змінити файлову систему тому для більш ефективного зберігання файлів надалі.

Як відформатувати том?

1. **Клацніть правою кнопкою миші по тому**, який необхідно відформатувати, і виберіть пункт **Форматувати**.

2. У вікні **Файлова система** виберіть файлову систему, яку необхідно створити на томі. Для більшості ОС сімейства Windows рекомендується файлова система NTFS.

Примітка. Файлові системи FAT16 і FAT32 можуть бути створені на томі розміром до 2 ГБ і до 2 ТБ відповідно.

3. У поле **Розмір кластера** вкажіть розмір кластера або розмір одиниці розподілу для файлової системи.

Рекомендується залишити розмір за замовчуванням, який відзначений у списку словами (за замовчуванням).

Додаткові відомості про вибір розміру кластера див. у підрозділі «Додаткові відомості про розміри кластера» далі в цьому розділі.

4. У поле **Мітка тому** введіть мітку тому, яку необхідно привласнити тому, щоб швидше знаходити його серед інших томів (необов'язково).

Максимальна кількість символів у мітці тому залежить від обраної файлової системи Натисніть кнопку ОК, щоб додати операцію форматування тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібнопідтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

Додаткові відомості про розміри кластера

Використання розміру кластера за замовчуванням звичайно є найбільш підходящим вибором.

Зменшення розміру кластера дозволяє оптимізувати зберігання, якщо в тому буде містити велика кількість дуже маленьких файлів.

Збільшення розміру кластера не дозволяє тому мати розмір, що перевищує звичайні розміри. Наприклад, у файловій системі FAT16 можна створити тому розміром 4 ГБ, використовуючи розмір кластера 64 КБ.

Увага! Деякі програми працюють неправильно з томами, файлові системи яких мають великий розмір кластера, наприклад у файлових системах FAT16 і FAT32 розміром 64 КБ і від 8 до 64 КБ — у файловій системі NTFS. Наприклад, ці програми можуть неправильно обчислювати загальний і доступний простір на таких томах.

Видалення тому

Дана операція видаляє обраний том. Простір, зайнятий томом, стає незайнятим простором на відповідному диску або дисках.

Увага! Після видалення тому всі дані, що зберігаються на ньому, будуть загублені.

Підказка. Видалення дзеркального тому припускає видалення обох його дзеркал.

Як вилучити том?

1. **Клацніть правою кнопкою миші по тому**, який необхідно вилучити, і виберіть пункт **Вилучити том**.

2. Натисніть кнопку **ОК**, щоб додати операцію видалення тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібно підтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування

1.5.6. Перегляд умісту тому

Перед вибором яких-небудь операцій над томом рекомендується переглянути вміст тому, щоб переконатися в правильності вибору тому. Це може бути особливо корисно у випадках, коли том не видний в провіднику Windows, наприклад якщо мова йде про том з

файловою системою Linux або при запуску Acronis Disk Director із завантажувального носія, коли немає спеціальних засобів для перегляду даних, збережених на томі.

Як переглянути вміст тому

1. **Клацніть правою кнопкою миші по тому**, уміст якого необхідно переглянути, і натисніть кнопку **Перегляд файлів**.
2. У вікні **Перегляд** розгорніть дерево папок для перегляду файлів і папок на обраному томі.
3. Після завершення перегляду натисніть кнопку **ОК**.

Примітка. Вікно Перегляд відображає реальний уміст тому, зчитуваний з диска. Якщо існують заплановані операції, наприклад поділ тому, заблоковані томи не можна переглядати доти, поки операції не будуть виконані або скасовані. А якщо ні, то операції з папками у вікні Перегляд виконуються негайно.

1.5.7. Зміна мітки тому

Мітка тому — це коротке ім'я, яке можна привласнити тому, щоб швидше знайти його серед інших томів.

В Acronis Disk Director мітка тому відображається в списку томів з наступною вказівкою букви диска (якщо вона привласнена), наприклад: System (C:).

На відміну від букви диска, яка може різнитися в різних встановлені на машині операційних системах Windows, мітка тому залишається однієї й тієї ж навіть після установки жорсткого диска з томом на іншу машину.

Максимальна довжина мітки тому залежить від файлової системи тому. Зокрема, у файловій системі NTFS максимальної припустимий розмір — 32 символи, в FAT16 — 11 символів, а в ext2 і ext3 — 16 символів.

Як змінити мітку тому?

1. **Клацніть правою кнопкою по тому**, мітку якого необхідно змінити, і виберіть пункт **Змінити мітку**.
2. У поле **Нова мітка** введіть нову мітку тому.

Примітка. У деяких файлових системах, наприклад FAT16 і FAT32, ряд символів є неприпустимими в мітці тому. Кнопка **ОК** залишається відключеної, якщо введена мітка містить такі символи.

3. Натисніть кнопку **ОК**, щоб додати операцію зміни мітки тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібнопыдтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

Символи мітки, неприпустимі в FAT16 і FAT32

У файлових системах FAT16 і FAT32 не дозволяється використовувати наступні символи в мітці тому: зворотна коса риса (\), коса риса (/), двокрапка (:), зірочка (*), знак питання (?), лапки ("), знак «менше» (<), знак «більше» (>) і пряма лінія (|).

Томи, мітки яких не можуть бути змінені

Не можна привласнити мітку тому, файлова система якого відзначена як Не підтримується, Не відформатована або Linux swap.

Якщо на машині встановлена програма резервного копіювання Acronis, наприклад Acronis True Image Home, можливо, на диску є том з іменем Acronis Secure Zone (ASZ). Мітка цього тому не може бути змінена.

1.5.8. Призначення параметра «Активний» для тому

Дана операція застосовна до основних томів на базових Mbr-Дисках.

Щоб указати том, з якого буде запущена машина, необхідно зробити цей тому активним. Диск може мати тільки один активний том, тому, якщо зробити том активним, раніше активний том автоматично перестане їм бути.

Як задати тому параметр «Активний»?

1. **Клацніть правою кнопкою основний том**, який необхідно зробити активним, і виберіть пункт **Відзначити як активний**.

Якщо в системі немає іншого активного тому, у чергу очікування буде додана операція завдання активного тому.

Примітка. У результаті того, що інший том стає активним, буква раніше активного тому може змінитися й деякі встановлені програми можуть перестати працювати.

2. Якщо в системі присутній інший активний том, з'явиться попередження про те, що раніше активний том перестане бути активним. Натисніть кнопку **ОК** у вікні Попередження, щоб додати операцію завдання активного тому в чергу очікування.

Навіть якщо на новому активному томі є операційна система, у деяких випадках машина не зможе завантажитися з нього. Необхідно підтвердити призначення нового активного тому.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібнопідтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

1.5.9. Додавання дзеркала

Дзеркальні томи забезпечують перешкодостійкість за рахунок зберігання двох точних копій даних, які називаються дзеркалами, на двох різних дисках.

Додавання дзеркала існуючого базового або простого тома означає перетворення даного тому в дзеркальний, що припускає копіювання даних тому на інший диск.

Як додати дзеркало тому?

1. **Клацніть правою кнопкою миші базовий або простий том**, на який необхідно додати дзеркало, і виберіть пункт **Додати дзеркало**.

2. Виберіть диск, на якім необхідно розмістити дзеркало. Диски, на яких недостатньо незайнятого простору для створення дзеркала, не можуть бути обрані.

При додаванні дзеркала на базовий том або при розміщенні дзеркала на базовому диску виникає попередження про те, що відповідні диски будуть перетворені в динамічні диски.

3. Натисніть кнопку **ОК**, щоб додати операцію додавання дзеркала на тому в чергу очікування.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Для виконання запланованої операції її потрібнопідтвердити. Вихід із програми без застосування запланованих операцій приводить до їхнього скасування.

1.5.10. Перевірка тому на наявність помилок

Дана операція можлива в операційних системах Windows і відключена для завантажувальних носіїв.

Дана операція дозволяє перевірити логічну цілісність файлової системи на томі (для файлових систем FAT16/32 і NTFS) і виправити знайдені помилки.

Перед виконанням якої-небудь операції з жорсткими дисками слід перевірити том жорсткого диска.

Acronis Disk Director не виконує перевірку самостійно. Програма запускає засіб перевірки диска (Chkdsk.exe), що входить до складу ОС Windows.

Як перевірити том?

1. **Клацніть правою кнопкою миші по тому**, файлову систему якого необхідно перевірити, і натисніть кнопку **Перевірити**.

2. Щоб знайти й усунути помилки (у випадку їх виявлення), установіть прапорець **Виправляти знайдені помилки**.

3. Щоб знайти ушкоджені сектори й відновити інформацію, яку вдасться прочитати, установіть прапорець **Намагатися виправляти знайдені ушкоджені сектори**.

4. Натисніть кнопку ОК, щоб виконати перевірку тому. Якщо том містить дуже велику кількість файлів (порядку мільйонів), перевірка може зайняти багато часу. Результати операції будуть представлені в окремім вікні.

Примітка. Якщо томФ використовується, засіб може тільки перевірити його на наявність помилок, але не може виправити їх. Перевірка й виправлення помилок на цьому томі будуть виконані під час наступного перезавантаження системи.

1.5.11. Приховання тому

Дана операція застосовна до томів на базових Mbr-Дисках.

Приховання тому означає зміну типу тому таким чином, щоб операційна система не могла «бачити» цей тому. Іноді том необхідно сховати для захисту інформації від несанкціонованого або випадкового доступу. Приховання тому не впливає на букви, призначені іншим томам, але схований том втрачає свою букву, і вона стає вільною для призначення.

Увага! Приховання тому, що містить файл підкачування, заблокує можливість завантаження машини. Приховання системного тому або завантажувального тому із запущеної в цей момент операційною системою відключене з метою збереження можливості завантаження машини.

Якщо на комп'ютері встановлена програма Acronis OS Selector, тому, який потрібно сховати, повинен бути позначений як схований і в Acronis OS Selector.

Як сховати том?

1. **Клацніть правою кнопкою миші по тому**, який необхідно сховати, і виберіть пункт **Сховати том.**

Якщо в томы є точки підключення, вони будуть автоматично вилучені.

2. Натисніть кнопку **ОК**, щоб додати заплановану операцію приховання тому.

1.5.12. Відображення тому

Дана операція застосовна до схованих томів на базових Mbr-Дисках.

Відображення схованого тому означає зміну його типу таким чином, щоб він був видний операційній системі. Відображення тому потрібно для наступних цілей:

- зробити раніше схований том знову видимим для операційної системи;
- одержати доступ до даних і внести зміни у файли, що зберігаються на схованому Oem-Томі.

Якщо на комп'ютері встановлена програма Acronis OS Selector, то том, який необхідно зробити видимим, повинен бути позначений як видимий і в Acronis OS Selector.

Як відобразити схований том?

1. **Клацніть правою кнопкою миші на схований том**, який необхідно відобразити, і виберіть команду **Відобразити том**. Програма автоматично призначить цьому тому першу вільну букву диска.

2. Натисніть кнопку **ОК**, щоб додати заплановану операцію відображення схованого тому.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

1.6. Робота з дисками

1.6.1. Ініціалізація диска

Якщо в машину додається один або кілька нових дисків, необхідно їх ініціалізувати , тобто зареєструвати диски в операційній системі. Виявлені диски будуть відображатися в списку дисків і томів, як Неініціалізовані.

Як ініціалізувати диск або диски?

1. **Клацніть правою кнопкою миші на знову доданий**, потім натисніть кнопку **Ініціалізувати**.

2. У вікні **Ініціалізація** диска виберіть інші неініціалізовані диски і задайте схему розбивки диска (MBR або GPT), а також тип диска (базовий або динамічний) для кожного з обраних дисків.

Схема розділів Gpt-Дисків не распізнаєтся в ОС Windows XP Home/XP Professional x86.

3. Натисніть кнопку **ОК**, щоб додати заплановану операцію ініціалізації диска.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Після ініціалізації весь простір диска залишиться нерозподіленим, тобто його поки неможливо використовувати для установки програм або зберігання файлів. Щоб використовувати його, необхідно або створити новий том, або розширити на цей диск існуючі томи.

Якщо потрібно змінити налагодження диска, можна зробити це пізніше за допомогою Acronis Disk Director 12.

1.6.2. Перетворення диска з динамічного в базовий

Перетворення динамічного диска в базовий може знадобитися, наприклад для використання на машині операційної системи, яка не підтримує динамічні диски.

Дана операція доступна тільки для порожніх динамічних дисків і для динамічних дисків, що містять один або кілька простих томів, причому кожний із простих томів повинен займати на диску одну область. Ці томи будуть перетворені в базові томи.

Як перетворити динамічний диск у базовий?

1. **Клацніть правою кнопкою миші динамічний диск**, який необхідно перетворити, потім виберіть пункт **Перетворити в базовий**. Відобразиться останнє попередження про перетворення динамічного диска в базовий.

У ньому будуть описані зміни, що відбуваються в системі після перетворення обраного динамічного диска в базовий. Наприклад, якщо преутворений у базовий диск містить томи, які підтримуються тільки динамічними дисками (усі типи томів, крім простих томів), то відобразиться попередження про можливе ушкодження даних у процесі перетворення.

2. Натисніть кнопку **ОК**, щоб додати операцію, що очікує виконання, перетворення динамічного диска в базовий.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Після перетворення останні 8 МБ дискового простору резервуються на випадок перетворення диска з базового в динамічний у майбутньому.

У деяких випадках обсяг незайнятого простору й пропонований максимальний розмір томів може різнитися (наприклад, якщо розмір одного дзеркала визначає розмір іншого дзеркала або якщо останні 8 МБ дискового простору резервуються на випадок перетворення диска з базового в динамічний у майбутньому).

Перетворення завантажувального диска

Програма не вимагає перезавантаження операційної системи після перетворення динамічного диска в базовий, якщо виконуються наступні умови:

1. На диску встановлено одна операційна система Windows Vista, Windows 7, Windows 8 або Windows 8.1.
2. На машині виконується ця операційна система.

Увага! Зміна файлової системи диска, що містить завантажувальні томи, забирає певний час. Відключення живлення, ненавмисне вимикання машини або випадкове натискання кнопки Reset під час цієї процедури може зробити завантаження із цих томів неможливої.

Програма забезпечує:

- можливість завантаження кожної з операційних систем (на машинах на яких установлено більш однієї операційної системи);
- безпечне перетворення динамічного диска з даними в базовий, якщо диск містить тільки прості томи.

1.6.3. Імпорт чужих дисків

На машині із двома або декількома операційними системами встановлення дисків і томів залежить від того, яка операційна система запущена в цей момент.

Звичайно всі динамічні диски, створювані на одній машині й в одній операційній системі, входять в одну групу дисків. При переносі на іншу машину або додаванні в іншу операційну систему на тій же машині група дисків уважається чужою. Група чужих дисків не може використовуватися, поки вона не буде імпортована в існуючу дискову групу. Група чужих дисків імпортується «один в один» (зберігає вихідне ім'я), якщо на машині відсутня дискова група.

Для доступу до даних на чужих дисках ці диски необхідно додати в системну конфігурацію машини за допомогою операції Імпорт чужих дисків.

Усі динамічні диски із групи чужих дисків імпортуються одночасно; імпортувати тільки один динамічний диск неможливо.

Як імпортувати чужі диски?

1. **Клацніть правою кнопкою миші один із чужих дисків** і виберіть пункт **Імпорт чужих дисків.**

У вікні, що відобразилося, з'явиться список усіх доданих на машину чужих динамічних дисків, а також будуть наведені відомості про томи, які будуть імпортовані. Відомості про статуси томів дозволять визначити, чи всі необхідні диски з дискової групи імпортуються. Якщо імпортуються всі необхідні диски, то у всіх томів цих дисків буде статус Справний. Будь-який статус, крім статусу Справний, указує, що імпортовані не всі диски.

2. Натисніть кнопку **ОК**, щоб додати операцію, що очікує виконання, імпорту чужих дисків.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

1.6.4. Очищення диска

Дана операція видаляє з диска всі томи й дані, роблячи його неініціалізованим. Усі томи, що навіть простираються й на інші диски, віддаляються з дисків, і зайнятий ними простір стає незайнятим. Щоб використовувати очищений диск, його необхідно ініціалізувати ще раз.

Як очистити диск?

1. **Клацніть правою кнопкою миші диск**, який необхідно очистити, і виберіть команду **Очистити диск.**
2. Натисніть кнопку **ОК**, щоб додати заплановану операцію очищення диска.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

Примітка. Якщо випадково був очищений Mbr-Диск із важливими даними, відновити том на цьому диску усе ще можна за допомогою програми Acronis Recovery Expert.Однак не забудьте спочатку ініціалізувати диск і задати схему розділів MBR.

1.6.5. Перетворення диска GPT в MBR

Перетворення базового Gpt-Диска в базовий Mbr-Диск може знадобитися, якщо необхідно встановити операційну систему й програмне забезпечення, що не підтримують Gpt-Диски.

Програма дозволяє перетворити Gpt-Диск в Mbr-Диск, при цьому необхідно враховувати наступне.

- Усі томи диска будуть логічними.
- Завантажувальні томи (якщо вони є) не зможуть завантажуватися, поки вони не будуть перетворені в основні.
- Томи, для яких розподілено більш 2 ТБ від початку диска, стають недоступними.

Як перетворити Gpt-Диск в Mbr-Диск

1. **Клацніть правою кнопкою миші Gpt-Диск**, який необхідно перетворити в Mbr-Диск, і виберіть **пункт Перетворити в MBR**.

Відобразиться вікно попередження, що вказує, що Gpt-Диск буде перетворений в Mbr-Диск.

У цьому вікні описуються зміни, що відбуваються в системі після перетворення обраного Gpt-Диска в Mbr-Диск. Наприклад, якщо після перетворення диск стане недоступний для системи, якщо операційна система перестане завантажуватися або якщо деякі томи на Gpt-Диску стануть недоступні після перетворення в Mbr-Диск (наприклад, томи, для яких виділено більш 2 ТБ), саме такі наслідки будуть зазначені у вікні попередження.

2. Натисніть кнопку **ОК**, щоб додати операцію, що очікує виконання, перетворення Gpt-Диска в Mbr-Диск.

Результати запланованої операції відображаються негайно, начебто операція вже виконана.

2. Хід роботи

1. Запустити програму на виконання
2. переглянути головне вікно програми та вивчити основні елементи
3. Перевірити наявність неполадок у роботі дисків на ПК
4. Відкрийте журнал та проведіть роботи згідно п.1.4.7, 1.4.8.
5. Створіть том на диску D/ /
6. . Змініть розмір тому
7. Проведіть переміщення та копіювання тому
8. Проведіть об'єднання базових томів
9. Проведіть форматування тому
10. Прегляньте умісту тому
11. Змініть мітку тому
12. Призначте параметр «Активний» для тому
13. Перевірте том на наявність помилок
14. Проведіть приховання та відображення тому

3. Контрольні питання

1. Основні можливості програми
2. Вимоги до встаткування та операційних систем
3. Файлові системи, які підтримуються програмою
4. . Підтримувані носії та томи
5. Поняття . базові й динамічні диски
6. Типи базових томів
7. Типи динамічних томів
8. Активний, системний і завантажувальний томи
9. Підтримка типів динамічних томів
10. Вирівнювання томів у дисках з розміром сектору 4 КБ
11. Правила безпеки при роботі з програмою
12. Запуск Acronis Disk Director в Windows та головне вікно програми
13. . Статуси дисків та томів
14. Структура дисків
15. Поняття заплановані операції
16. Дії із записами журналу
17. Створення тому

18. . Зміна розміру тому
19. Копіювання тому
20. Об'єднання базових томів
21. Форматування тому
22. Перегляд умісту тому
23. Зміна мітки тому
24. Призначення параметра «Активний» для тому
25. Додавання дзеркала
26. Перевірка тому на наявність помилок
27. Приховання та відображення тому
28. Ініціалізація диска
29. Перетворення диска з динамічного в базовий і навпаки
30. Імпорт чужих дисків
31. Очищення диска
32. Перетворення диска GPT в MBR і навпаки

РОЗДІЛ 6
Захист інформації за допомогою антивірусних програм

Лабораторна робота 27
Антивірусна програма NOD 32

Мета роботи – Засвоїти принципи й елементи технології захисту інформації від вірусів та інших шкідливих програм. Ознайомитись з рівнями захисту комп'ютера, можливістю використання налагоджень та можливостей програми , вбудованого брандмауера.

ПЛАН

1. Теорія
1.1 Звичайна установка
1.2 Уведення імені користувача й пароля
1.3 Налагодження відновлень
1.4 Сканування комп'ютера на вимогу
1.5 Налагодження довіреної зони
1.6 Налагодження прокси-сервера
1.7 Сканування носіїв
1.8 Сканування ПЗ події
1.9 Перевірка недавно створених і змінених файлів
1.10 Додаткові налагодження
1.12 Поведінка модуля захисту від вірусів і втручання користувача
1.13 Рівні очищення
1.14 Термін зміни параметрів захисту в режимі реального часу
1.15 Вирішення проблем, що виникають при роботі модуля захисту в режимі реального часу
1.16 Захист електронної пошти
1.17 Веб-браузери
1.18 Типи сканування
1.19 Профілі сканування
1.20 Створення нових правил
1.21 Аутентифікація зон: конфігурація клієнта
1.22 Спам
2. Хід роботи
3. Контрольні питання

1. Теорія
1.1 Звичайна установка

Звичайна установка рекомендується для користувачів, що хочуть установити ESET Smart Security зі стандартними параметрами. Стандартні параметри за замовчуванням забезпечують найвищий ступінь безпеки. Цей варіант рекомендується для користувачів, які не прагнуть виконувати докладне налагодження програми вручну.

На першому й дуже важливому кроці налагодження пропонується ввести ім'я користувача й пароль, необхідні для одержання автоматичних відновлень програми. Процес відновлень відіграє найважливішу роль у забезпеченні безперервного захисту комп'ютера.

У відповідних полях уведіть свої ім'я користувача й пароль, тобто ті самі дані, які були отримані при придбанні або реєстрації програми. Якщо ім'я користувача й пароль ще невідомі, виберіть Установити параметри відновлення пізніше. Дані аутентифікації можуть бути зазначені пізніше.

Наступним кроком є налагодження системи своєчасного виявлення ThreatsenseNet. Система своєчасного виявлення ThreatsenseNet призначена для своєчасного й постійного інформування компанії ESET про появу нових погроз. Вона дозволяє швидко реагувати й захищати користувачів. Система передбачає передачу зразків зловмисного коду в лабораторію ESET. Там вони аналізуються, обробляються й додаються в бази даних сигнатур вірусів.

Для активізації цієї функції встановіть прапорець Включити систему своєчасного виявлення. Для зміни параметрів передачі підозрілих файлів натисніть Додаткові налагодження.

Наступним кроком налагодження є налагодження захисту від потенційно небажаного програмного забезпечення. Додатки, що відносяться до потенційно небажаного ПЗ, не обов'язково є зловмисними. Однак вони можуть тим або іншим способом знижувати продуктивність системи. Такі додатки звичайно вимагають згоди користувача при установці. Однак їх установка найчастіше відбувається під час налагодження інших корисних програм. Тому помітити спробу налагодження такого ПЗ досить важко. Установка потенційно небажаного ПЗ може негативно позначитися на роботі операційної системи.

Виберіть Включити виявлення потенційно небажаного ПЗ, щоб дозволити виявлення системою ESET Smart Security такого типу погроз. Рекомендується включити цю функцію.

Останнім кроком звичайної налагодження є підтвердження налагодження. Для цього натисніть кнопку Установити.

1.2 Уведення імені користувача й пароля

Для того щоб використовувати програму щонайкраще, необхідно регулярно обновляти її. Це можливо тільки при наявності правильних даних аутентифікації (імені користувача й пароля), які вказуються в параметрах відновлення.

Якщо ім'я користувача й пароль не зазначені при установці, це можливо зробити пізніше. У головному вікні програми виберіть **Восстановление**, потім Уведення імені користувача й пароля. Відкриється вікно (рис. 1) з інформацією про ліцензію. Уведіть у цьому вікні дані, отримані разом з ліцензією на програму.

1.3 Налагодження відновлень

Процес відновлення бази даних сигнатур вірусів і компонентів програми є найважливішою частиною забезпечення захисту комп'ютера від зловмисного коду. Приділіть особливої увагу вивченню налагодження й роботи цього процесу. Для того щоб відкрити вікно відновлення, виберіть у головному меню пункт Відновлення. Щоб перевірити доступність відновлення бази даних сигнатур вірусів, натисніть **Обновити базу даних сигнатур вірусів** (рис. 2). Виберіть **ввести имя и пароль пользователя**, щоб указати ім'я користувача й пароль, які надаються компанією ESET.

Якщо ім'я користувача й пароль були зазначені під час налагодження програми ESET Smart Security (рекомендується), то вони не будуть запитані на цьому етапі.

1.4 Сканування комп'ютера на вимогу

Після налагодження програми ESET Smart Security потрібно запустити сканування комп'ютера на наявність зловмисного коду (який міг потрапити на комп'ютер до налагодження ESET Smart Security). Для швидкого запуску сканування в головному вікні програми виберіть **Сканирование компьютера**, а потім **Обычное сканирование** (рис. 4).

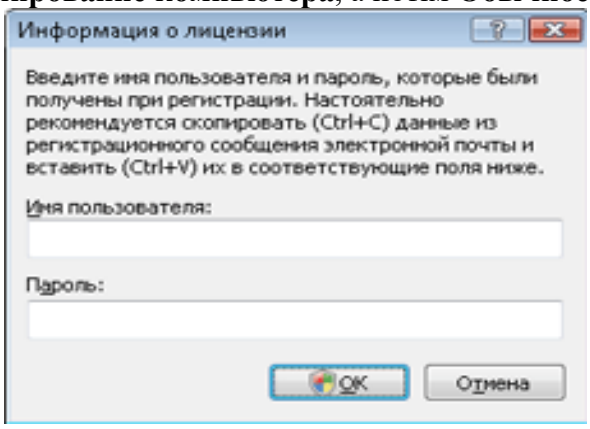


Рис. 1. Уведення імені користувача й пароля.

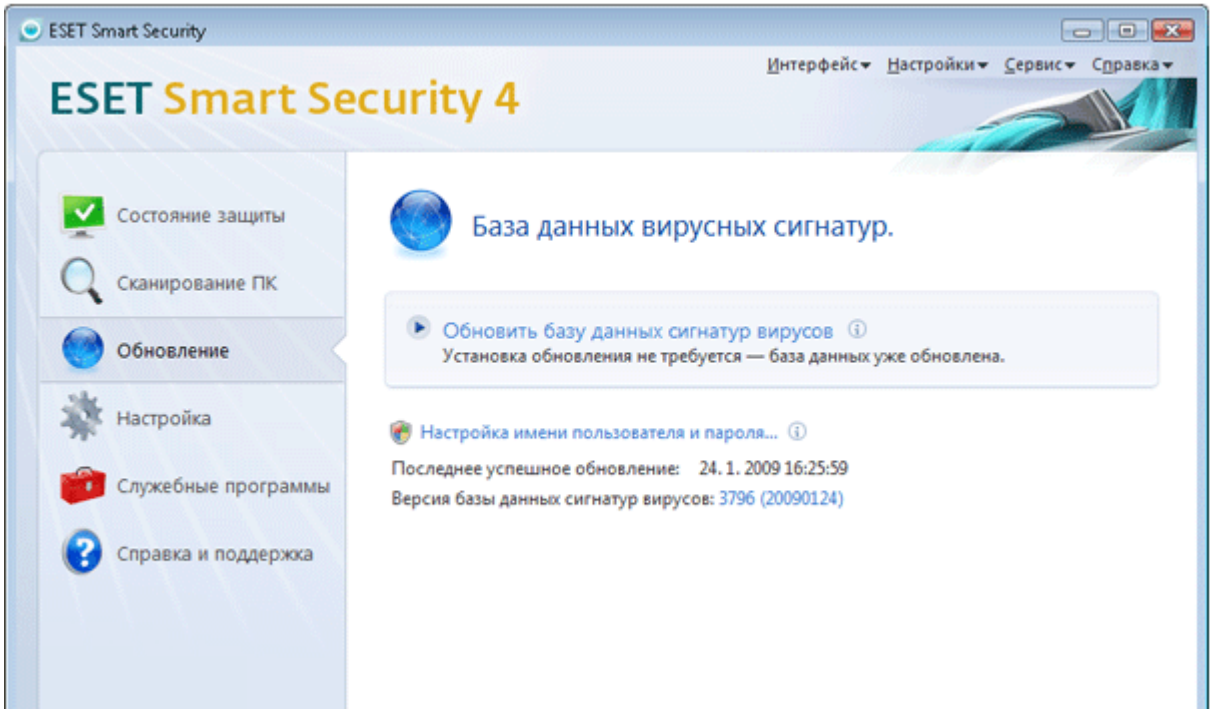


Рис. 2. Відновлення баз

1.5 Налагодження довіреної зони

Попередження. Неправильне налагодження довіреної зони може викликати зниження рівня безпеки комп'ютера.

Процес налагодження довіреної зони є найважливішою частиною забезпечення мережевої безпеки. При налагодженні довіреної зони користувач може надати доступ іншим користувачам мережі до свого комп'ютера і його ресурсів. Виберіть **Настройка** – **Персональный брандмауэр** (рис. 5). Відкриється вікно **Зміна режиму захисту комп'ютера в мережі**, у якому можна налагодити параметри режиму захисту в поточній мережі або зоні.

Автоматичне визначення довіреної зони виконується після налагодження програми ESET Smart Security або після підключення комп'ютера до нової мережі. Таким чином, найчастіше немає необхідності задавати довірену зону. За замовчуванням при виявленні нової зони виводиться діалогове вікно, що дозволяє налагодити рівень захисту для цієї зони.

Примітка. За замовчуванням робочі станції з довіреної зони мають доступ до файлів і принтерів загального користування локального комп'ютера з'єднання, що входять, RPC дозволені, служба вилученого робочого столу також дозволена.

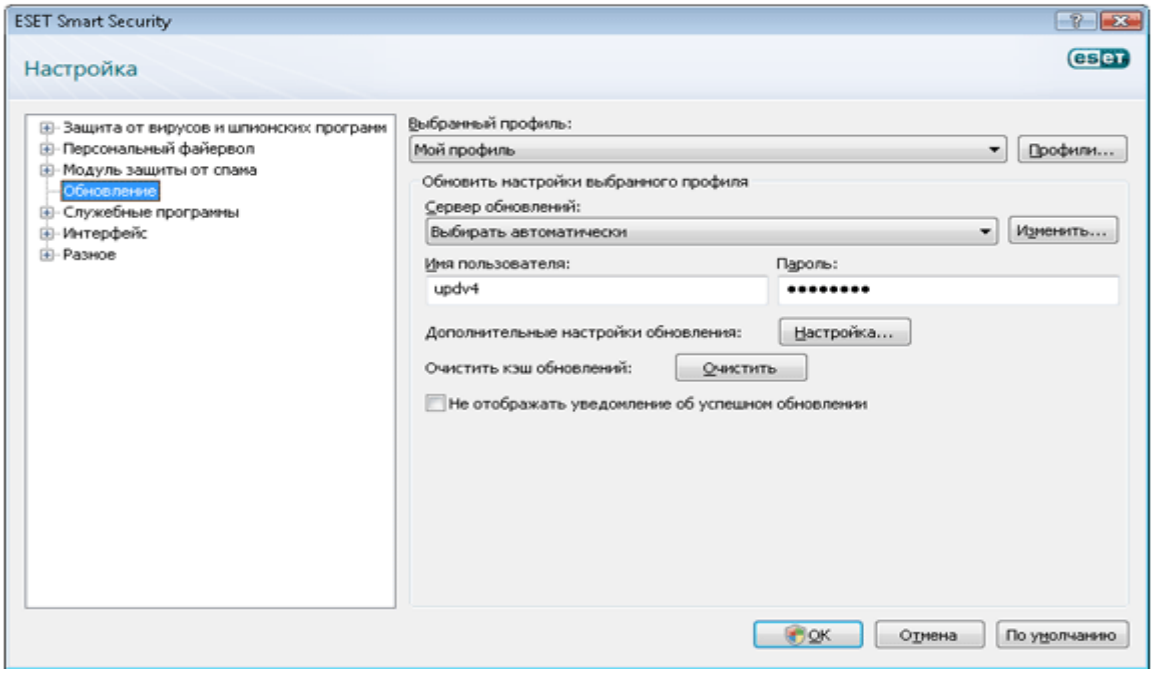


Рис. 3. Додаткове налагодження

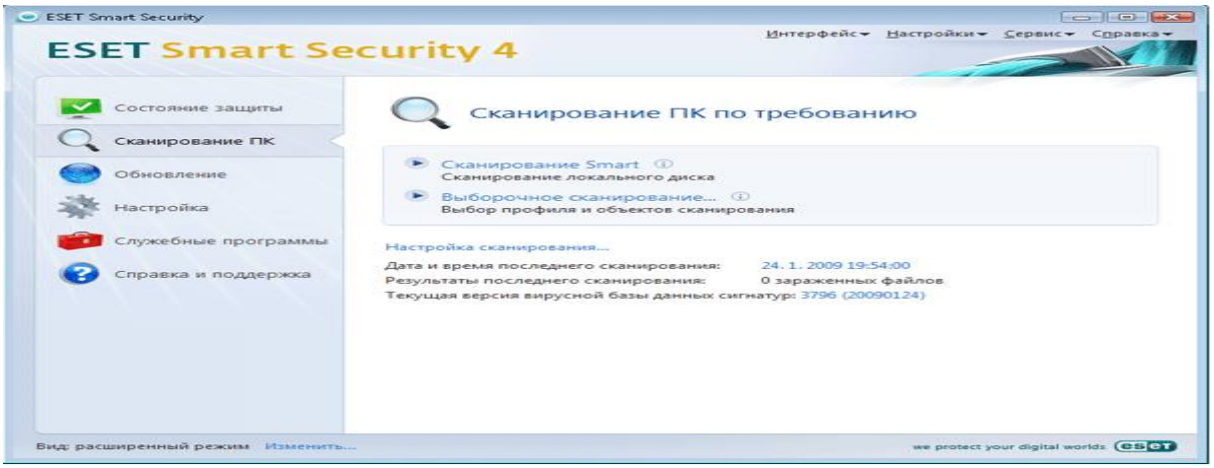


Рис. 4. Сканування комп'ютера

1.6 Налагодження прокси-сервера

Якщо для підключення до Інтернету використовується прокси-сервер, він повинен бути зазначений у додаткових параметрах. Для доступу до загальних параметрів виберіть у головному меню пункт Налагодження, потім Налагодження прокси-сервера. Вікно параметрів (рис. 7) дозволяє користувачеві вказати адреса й порт прокси-сервера, а також дані аутентифікації.

Примітка. Параметри прокси-сервера для різних профілів відновлення можуть різнитися. У цьому випадку налагодьте прокси-сервер у розділі додаткових налагоджень відновлення. Якщо немає інформації про підключення до Інтернету, можна автоматично визначити параметри прокси-сервера для програми ESET Smart Security. Для цього натисніть кнопку Знайти прокси-сервер.

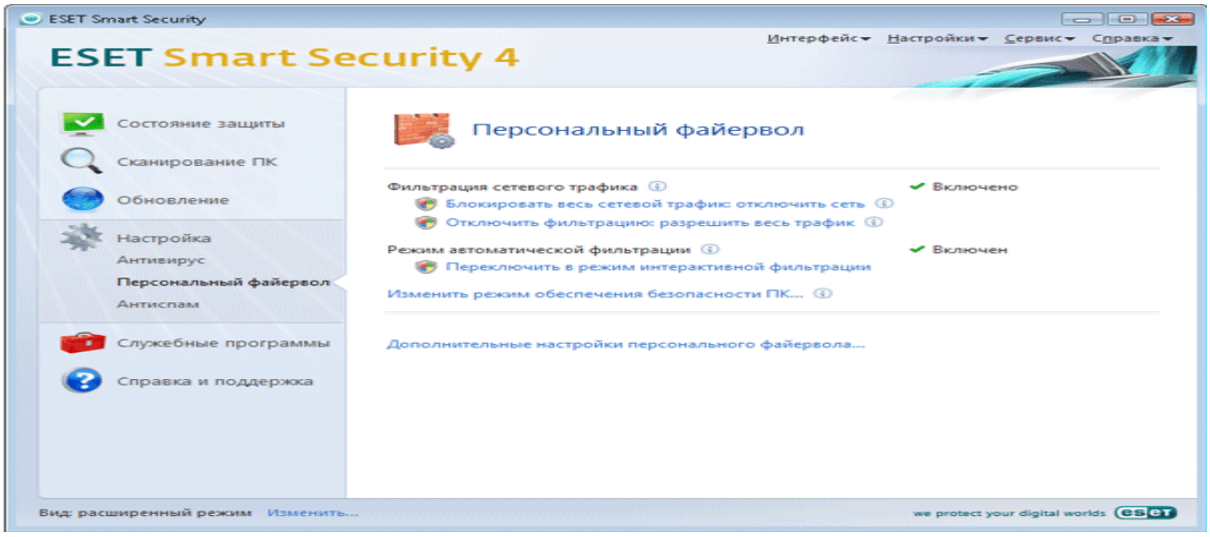


Рис. 5. Персональний фаєрвол

Рис. 6. Вибір доступу

1.7 Сканування носіїв

За замовчуванням перевіряються всі доступні носії. Команда Жорсткі диски – контролюються всі жорсткі диски комп'ютера, Знімні носії – контролюються дискети, накопичувачі USB і т.д., Мережеві диски – контролюються всі підключені мережеві диски.

Рекомендується використовувати параметри за замовчуванням. Ці параметри можуть змінюватися тільки в особливих випадках (наприклад, якщо контроль файлової системи приводить до значного вповільнення швидкості обміну даними).

1.8 Сканування ПЗ події

За замовчуванням усі файли скануються при відкритті, виконанні або створенні. Рекомендується зберігати налагодження за замовчуванням, при яких забезпечується максимальний рівень безпеки комп'ютера. Функція перевірки дискет забезпечує контроль умісту завантажувального сектору дискет, що перебувають у приводі. Функція перевірки при вимиканні забезпечує перевірку завантажувальних секторів комп'ютера під час його вимикання. Незважаючи на те, що завантажувальні віруси в цей час зустрічаються рідко, рекомендується включити цю функцію.

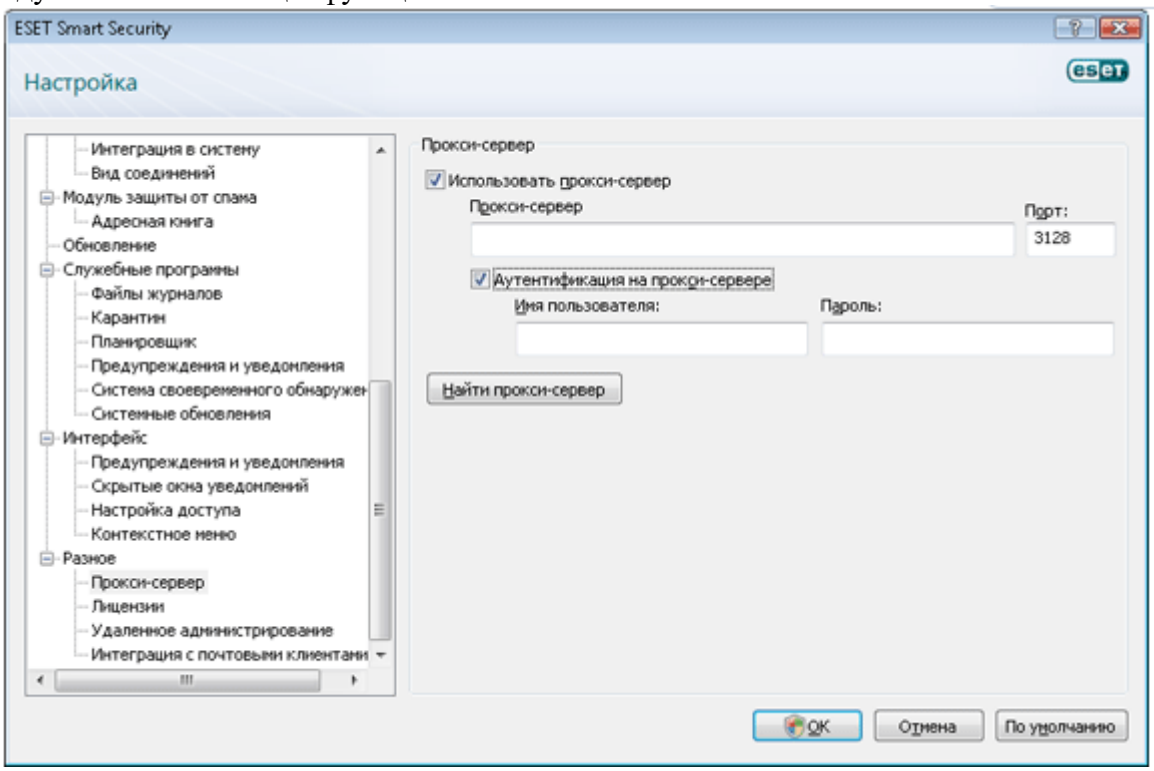


Рис. 7. Вікно параметрів

1.9 Перевірка недавно створених і змінених файлів

Імовірність того, що недавно створені файли виявляться заражені, вище, ніж для існуючих файлів, тому вони перевіряються з додатковими параметрами. На додаток до звичайних методів перевірки, заснованими на пошуку в базі даних сигнатур вірусів, застосовуються методи розширеної евристики, що значно збільшує ймовірність виявлення вірусів. Перевіряються файли, що саморозпаковуються (SFX) і файли упаковщиків в режимі реального часу. За замовчуванням перевіряються архіви із глибиною вкладеності до 10 незалежно від їхнього фактичного розміру. Зніміть прапорець Параметри сканування архівів за замовчуванням, щоб змінити параметри перевірки архівів.

1.10 Додаткові налагодження

Для мінімізації перешкод при роботі комп'ютера з використанням захисту файлової системи в режимі реального часу вже перевірені файли не перевіряються повторно, якщо тільки вони не були змінені (файли перевіряються знову відразу ж після відновлення бази даних сигнатур вірусів). Для перевірки всіх файлів при звертанні до них зніміть прапорець Оптимізоване сканування у вікні додаткових параметрів Захист файлової системи в режимі реального часу.

Захист файлової системи в режимі реального часу запускається при завантаженні операційної системи, що забезпечує безперервність перевірки. В особливих випадках (наприклад, у випадку конфлікту з іншим модулем сканування в режимі реального часу) захист файлової системи в режимі реального часу можна відключити, знявши прапорець Автоматичний запуск захисту файлової системи в режимі реального часу.

За замовчуванням розширена евристика для файлів, що запускаються, не використовується, але її можна включити, установивши прапорець Розширена евристика при запуску файлів. Після включення цієї функції може сповільнитися виконання деяких програм внаслідок підвищення вимог до системи.

1.11 Поведінка модуля захисту від вірусів і втручання користувача

Вікно попередження про погрозу виводиться, якщо один з модулів захисту системи ESET Smart Security виявляє погрозу або шкідливий код. Програма відображає вікна попереджень двох видів.

1. Попередження про погрозу, що не вимагає втручання користувача (рис. 8).

Це попередження виводиться в тому випадку, якщо ESET Smart Security виконує дію, що не вимагає втручання користувача. Це повідомлення носить інформаційний характер.

Об'єкт

Ім'я зараженого файлу.

«Примітка»

Термінологія може різнитися залежно від виробників антивірусного забезпечення. Додаткові відомості про зараження файлів.

«Погроза»

Найменування вірусу (відповідно до термінології ESET).

«Інформація»

Дія, яку вживає програма при виявленні вірусу.

«Закрити»

Натисніть x, щоб закрити вікно попередження до того, як воно закриється автоматично.

«Показати параметри»

Натисніть v, щоб відключити висновок попереджень і налагодити режим їх відображення.

2. Попередження про погрозу, що вимагає втручання користувача.

Залежно від параметрів, заданих в налагодженнях модуля Threatsense, ESET Smart Security може вимагати від користувача виконання певних дій.

Об'єкт

Ім'я зараженого файлу.

Погроза

Найменування вірусу (відповідно до термінології ESET).

Примітка

Відомості про заражений файл.

«Скопіювати в карантин»

Копія зараженого файлу зберігається в безпечній карантинній папці (незалежно від дії, що вживає).

Передати на аналіз

Установіть цей прапорець, щоб дозволити відправлення файлу в лабораторію ESET.

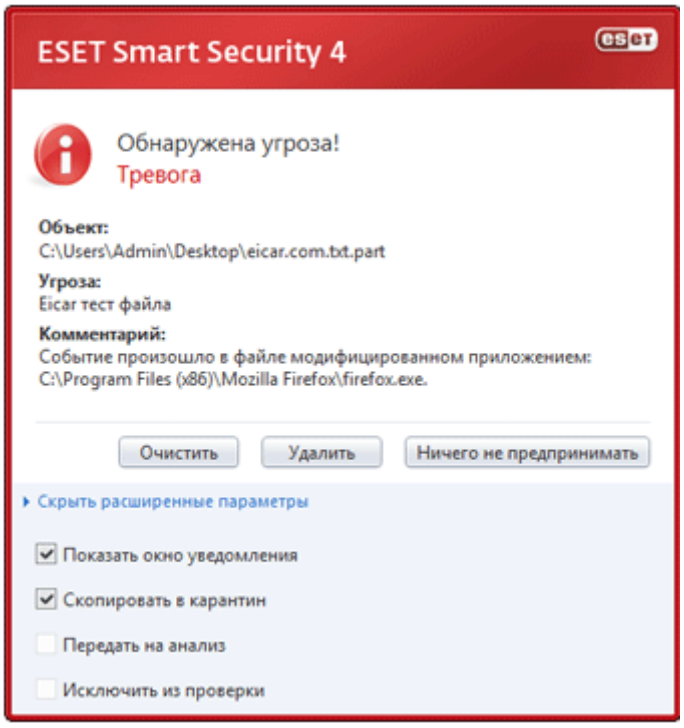


Рис. 8. Попередження про погрозу

Виключити з перевірки

Виберіть цей варіант, щоб виключити файл зі сканування й додати його в список виключень.

Очистити

Ця дія виконується в тому випадку, коли виявлений заражений файл, який можна очистити. Його також можна викликати при виявленні вірусів, які не можна очистити і які залишають інформацію в реєстрі Windows. Якщо користувач вибирає цю дію, заражений файл видаляється, а шкідлива інформація стирається з реєстру.

Вилучити

Ця дія видаляє виявлені файли. Якщо є можливість очищення зараженого об'єкта, дія Вилучити не пропонується.

Попередження

При натисканні цієї кнопки користувач ризикує залишити комп'ютер зараженим! Використовуйте її тільки при 100%-ній упевненості в тому, що файл безпечний.

Пропустити

Закриває вікно повідомлення й не виконує ніяких дій.

Показувати параметри

Натисніть v для встановлення додаткових параметрів.

Попередження

Якщо користувач відключив висновок попереджень, то при виникненні ситуації, що вимагає його втручання, не буде виконано ніяких дій.

Показувати вікно попередження

Перемикає режим попереджень.

1.12 Рівні очищення

Захист у режимі реального часу передбачає три рівні очищення (рис. 9).

- У режимі першого рівня програма показує вікно повідомлення й пропонує на вибір дії для кожного з випадків зараження. Користувач повинен вибрати дію для кожного зараження окремо. Цей рівень розроблений для досвідчених користувачів, які знають, як поводитися в кожному конкретному випадку.
- У режимі середнього рівня програма автоматично вибирає й виконує попередньо певну дію (залежно від типу зараження). Виявлення й видалення заражених файлів супроводжується інформаційним повідомленням, що розташовуються в правому нижньому куті екрана. Однак автоматичні дії не вживаються у випадку виявлення зараження в архівах, які містять, крім заражених, файли без шкідливого коду, а також якщо дій для цього випадку не передбачені.
- У режимі третього, найбільше агресивного рівня – усі заражені об'єкти видаляються. Тому що цей рівень може привести до втрати корисної інформації, рекомендується використовувати його тільки в особливих випадках.

1.13 Термін зміни параметрів захисту в режимі реального часу

Захист файлової системи в режимі реального часу є ключовим компонентом комп'ютерної безпеки. Таким чином, необхідно бути уважним при зміні її параметрів. Рекомендується змінювати її параметри тільки в особливих випадках. Наприклад, при виникненні конфліктів з якими-небудь додатками або модулями сканування в режимі реального часу інших антивірусних програм. Після налагодження ESET Smart Security усі параметри налагоджені оптимально й забезпечують максимальний рівень захисту системи. Для того щоб відновити параметри за замовчуванням, натисніть кнопку За замовчуванням у вікні параметрів захисту файлової системи в режимі реального часу (Додаткові налагодження, Захист від вірусів і шпигунських програм, Захист файлової системи в режимі реального часу).

Перевірка модуля захисту в режимі реального часу

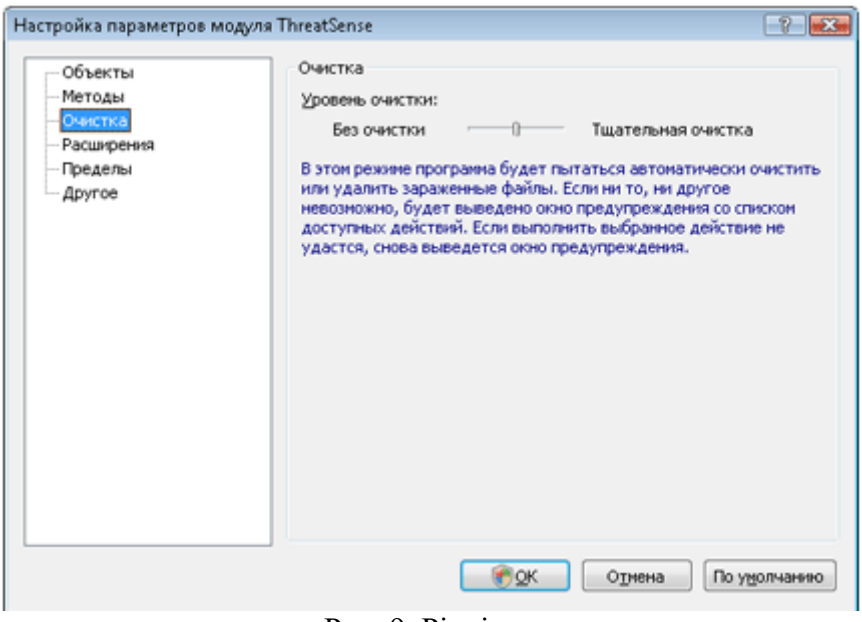


Рис. 9. Рівні очищення

Примітка. Перед здійсненням перевірки необхідно відключити персональний брандмауера. Якщо цей модуль буде включений, він виявить спробу завантаження шкідливого файлу й не пропустить його.

Для того щоб перевірити функціонування захисту файлової системи в режимі реального часу, використовуйте перевірочний файл eicar.com. Цей файл містить нешкідливий код, який, однак, виявляється всіма програмами захисту від вірусів. Файл створений компанією EICAR (Європейський інститут антивірусних комп'ютерних досліджень) для перевірки функціонування програм захисту від вірусів. Файл eicar.com доступний для завантаження за адресою http://www.eicar.org/download/eicar.com.

1.14 Вирішення проблем, що виникають при роботі модуля захисту в режимі реального часу

Якщо захист файлової системи в режимі реального часу ненавмисно був відключений користувачем, його потрібно включити. Для того щоб включити захист файлової системи в режимі реального часу, перейдіть на сторінку Налагодження/Захист від вірусів і шпигунських програм і натисніть Включити захист файлової системи в режимі реального часу.

Якщо захист файлової системи в режимі реального часу не запускається при завантаженні операційної системи, можливо, відключена функція Автоматичний запуск захисту файлової системи в режимі реального часу. Для того щоб включити цю функцію, перейдіть у вікно розширених налагоджень (F5) і виберіть у лівому стовпці Захист файлової системи в режимі реального часу (рис.10). Розділ Додаткові налагодження розташований у нижній частині вікна. Установіть прапорець Автоматичний запуск захисту файлової системи в режимі реального часу.

Захист файлової системи в режимі реального часу не виявляє віруси

Переконайтеся в тому, що на комп'ютері не встановлений інший антивірусний додаток. При одночасній роботі двох систем захисту від вірусів можуть виникнути конфлікти.

Захист файлової системи в режимі реального часу на запускається

Якщо захист не запускається при завантаженні системи, але функція Автоматичний запуск захисту файлової системи в режимі реального часу включена, можливо, виник конфлікт із іншими додатками. У цьому випадку зверніться за консультацією до фахівців служби технічної підтримки ESET.

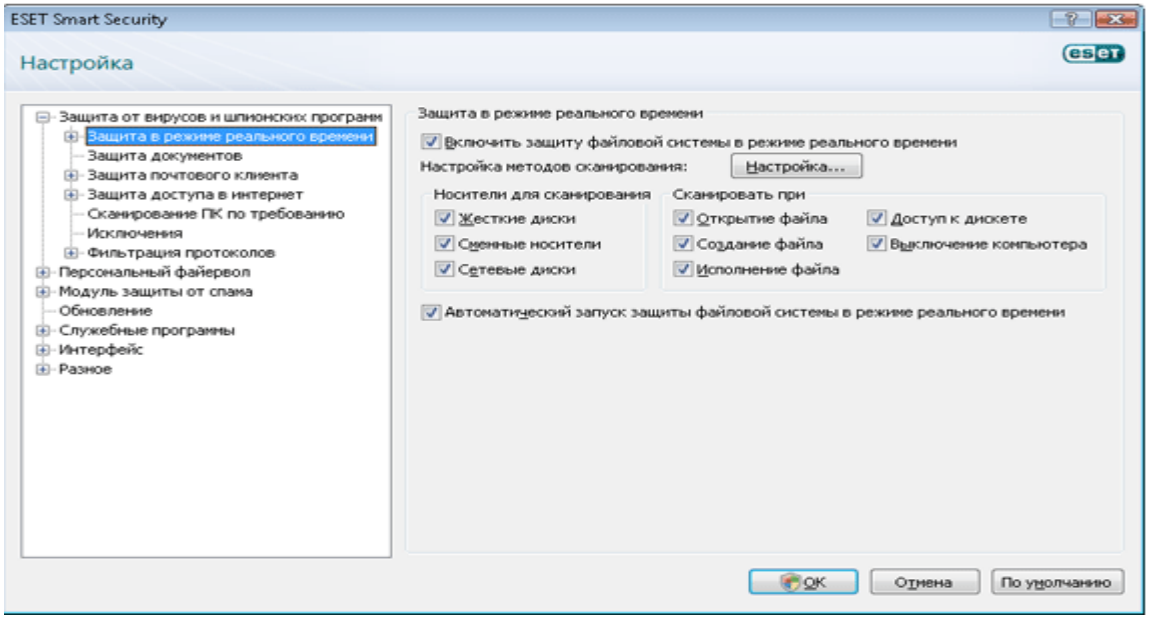


Рис. 10. Параметри захисту

1.15 Захист електронної пошти

Сумісність

У деяких поштових клієнтах можуть виникати проблеми при одержанні повідомлень (наприклад, при повільному з'єднанні із сервером процес одержання повідомлень може перериватися). У цьому випадку змініть спосіб контролю трафіка. Зниження рівня контролю може вплинути на процес очищення.

Якщо включений режим максимальної ефективності (рис. 11), шкідливий код видаляється із заражених повідомлень (якщо включені функції Вилучити або Очистити або включений середній або найвищий рівень очищення), а інформація про зараження вставляється перед вихідною темою листа.

Режим середньої сумісності змінює спосіб одержання повідомлень. Повідомлення поступово відправляються поштовому клієнтові й скануються тільки після одержання останньої частини. Однак при цьому зростає ризик зараження. Рівень очищення й застосування повідомлень (текстової інформації, що прикріплюється до теми або тіла повідомлення) залишаються тими ж, що й для режиму найбільшої ефективності.

У режимі максимальної сумісності програма виводить вікно з повідомленням про одержання зараженого повідомлення. При цьому не додається повідомлень до теми або тіла повідомлення, а віруси автоматично не віддаляються. Видалення вторгнення повинне проводитися користувачем вручну в поштовому клієнтові.

Додавання повідомлень до тексту повідомлень електронної пошти

Кожне з відправлених і отриманих повідомлень, що перевіряються системою ESET Smart Security, може бути позначене, таким що включаються в тему або текст повідомлення повідомленням. З його допомогою користувач інформується про те, що повідомлення перевірене й не заражене. Ця функція піднімає рівень довіри користувача, що відправляє, повідомленням, а при виникненні зараження надає важливу інформацію про його ступені й небезпеки, що виходить від відправника. Налагодження цієї функції перебувають у меню Додаткові налагодження (клавіша F5) Захист від вірусів і шпигунських програм/Захист поштового клієнта. Примітки можуть додаватися в усі повідомлення, тільки в заражені повідомлення або не додаватися взагалі. ESET Smart Security також дозволяє додавати повідомлення у вихідну тему заражених повідомлень. Для цього потрібно вибрати Додавання приміток у поле теми отриманих і прочитаних заражених повідомлень і Додавання приміток у поле теми відправлених заражених повідомлень. Уміст повідомлень можна змінювати в полі Шаблон повідомлення, що додається в тему заражених листів. Ці зміни допомагають автоматизувати процес фільтрації заражених повідомлень електронної пошти (якщо це підтримується поштовим клієнтом) шляхом переміщення заражених повідомлень в окрему папку

Видалення заражень

У випадку виявлення зараженого повідомлення електронної пошти виводиться вікно повідомлення. Вікно повідомлення містить ім'я відправника, адреса його електронної пошти й назва погрози. У нижній частині вікна перебувають функції, які можна застосувати до цього об'єкта. У більшості випадків рекомендується вибирати очищення або видалення. В особливих ситуаціях, якщо є бажання прийняти заражений об'єкт, виберіть Пропустити. Якщо обраний максимальний рівень очищення, інформаційне вікно не містить інформацію про вибір дії.

Керування адресами

У цьому розділі можна задавати списки Http-Адрес, які будуть блокуватися, дозволятися або виключатися з перевірки. Кнопки Додати, Змінити, Вилучити і Експорт

дозволяють управляти списками адрес. Веб-сайти зі списку заблокованих будуть недоступні. Веб-сайти зі списку виключених адрес завантажуються без перевірки на шкідливий код. Якщо вибрати варіант Дозволити доступ тільки для Http-Адрес зі списку дозволених адрес, будуть доступні тільки адреси зі списку дозволених, а інші веб-сайти HTTP будуть заблоковані. У всіх списках припустиме використання символів шаблону «*» (зірочка) і «?» (знак питання). Символ зірочки позначає будь-яку послідовність символів, а знак питання – будь-який символ. Працювати із умістом списку виключених адрес необхідно з особливою старанністю, тому що він повинен містити тільки перевірені й безпечні адреси. Необхідно бути впевненим у правильності використання символів шаблону в цьому списку. Щоб активувати список, установіть прапорець Список активний. Щоб включити відображення повідомлень при завантаженні адреси з поточного списку, установіть прапорець Повідомляти про спів падання адреси із шаблоном зі списку.

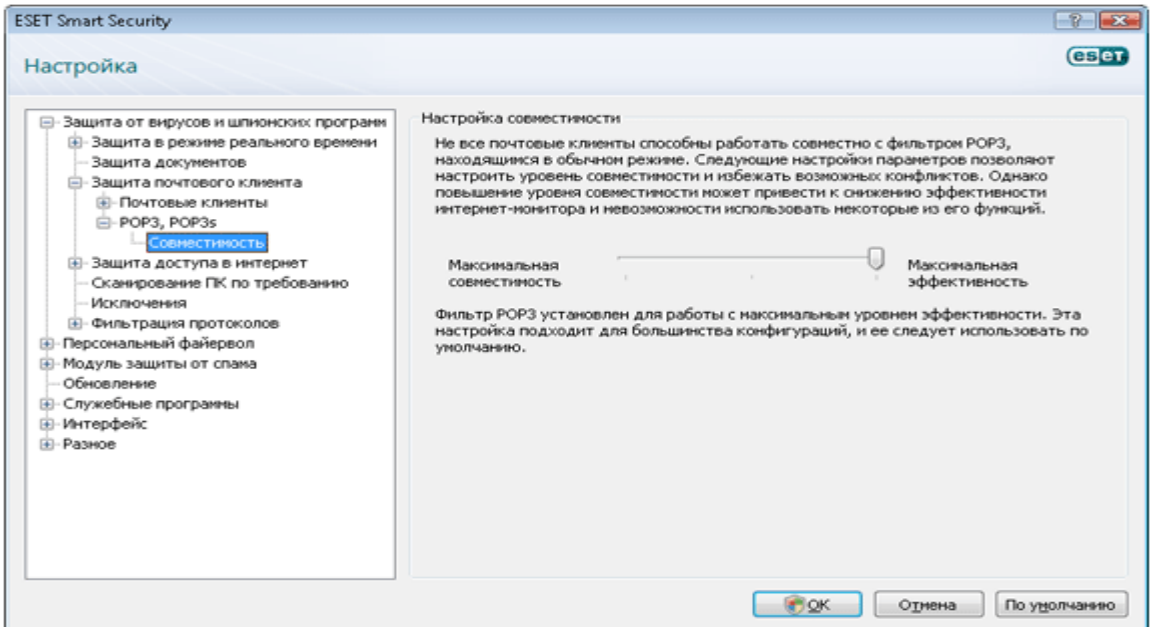


Рис. 11. Сумісність

1.16 Веб-браузери

Система ESET Smart Security містить функцію, яка дозволяє користувачам указати, чи є додаток веб-браузером. Якщо додаток класифікується як веб-браузер, увесь обмін даними із цим додатком відслідковується незалежно від портів, використовуваних у мережевім з'єднанні. Ця функція доповнює функцію перевірки протоколу HTTP, тому що перевірка HTTP контролює тільки певні порти. Багато служб в Інтернеті використовують динамічний розподіл портів або невідомі заздалегідь значення портів. За допомогою функції вказівки веб-браузерів ESET Smart Security здатна контролювати мережеві з'єднання незалежно від параметрів з'єднання.

Список додатків, класифікованих як веб-браузери, доступний на сторінці параметрів перевірки протоколу HTTP у розділі Веб-браузери. Цей розділ містить підменю Активний режим, яке визначає режим перевірки для інтернет-браузерів. Функція Активний режим досить корисна для повної перевірки всього трафіка. Якщо вона відключена, обмін даними контролюється в пакетному режимі. Це знижує ефективність перевірки передачі даних, але забезпечує кращу сумісність із перерахованими додатками. Якщо проблем із сумісністю немає, рекомендується використовувати активний режим.

1.17 Типи сканування

Інтелектуальне сканування

Звичайне сканування є інтуїтивно зрозумілим методом, що дозволяють користувачеві запускати сканування комп'ютера й очищати заражені файли без участі самого користувача. Головною перевагою цього методу є простота експлуатації без розширеного керування параметрами сканування. Звичайне сканування перевіряє всі файли на локальних дисках (за винятком електронної пошти й архівів) і автоматично очищає або видаляє виявлений шкідливий код. Рівень очищення автоматично встановлений на рівень за замовчуванням. Стандартний профіль очищення розроблений для користувачів, що бажають швидко й просто сканувати комп'ютери. Він пропонує ефективний розв'язок для сканування й очищення без поглибленого налагодження процесу

Вибіркове сканування

Сканування з користувацькими налагодженнями є оптимальним розв'язком у тому випадку, коли потрібно вказати параметри сканування (наприклад, об'єкти сканування й методи сканування). Перевагою такого сканування є можливість докладного налагодження. Набори параметрів можуть бути збережені у вигляді профілів сканування. Ці профілі особливо корисні, якщо сканування виконується регулярно з однаковими користувацькими параметрами.

Для того щоб вибрати об'єкти сканування, використовуйте меню швидкого вибору об'єктів або виберіть об'єкти в дереві об'єктів, доступних для сканування. Користувач може задати три рівні очищення в меню Налагодження, Очищення. Якщо необхідно сканування без виконання додаткових дій, виберіть параметр Сканувати без очищення.

Сканування з користувацькими налагодженнями підходить для досвідчених користувачів систем захисту від вірусів.

Об'єкти сканування

За допомогою параметра Вибір об'єктів сканування можна вказати об'єкти (оперативна пам'ять, жорсткі диски, сектори, файли й каталоги), які підлягають перевірці на наявність вірусів.

У меню, що розкривається, Об'єкти сканування можна вибрати попередньо певні об'єкти перевірки.

ПЗ параметрах профілю – об'єкти, зазначені в обраному профілі. З’ємний носій – усі з’ємні носії, Локальні диски – усі локальні диски, Мережеві диски – усі підключені мережеві диски, Нічого не вибирати – скасувати вибір об'єктів.

Установіть прапорці напроти об'єктів, які потрібно перевіряти.

Щоб швидко позначити обраний об'єкт або додати його безпосередньо, укажіть потрібний об'єкт у порожньому полі під списком каталогів. Це можливо тільки у випадку, якщо в списку каталогів не обраний жоден об'єкт.

1.18 Профілі сканування

Набір параметрів сканування комп'ютера може бути збережений у вигляді профілю. За допомогою профілів сканування можна зберегти параметри й використовувати їх у майбутньому. Рекомендується створити профілі для кожного з регулярно використовуваних наборів параметрів (для різних об'єктів сканування, методів сканування й інших параметрів).

Для того щоб створити новий профіль, який буде використовуватися на регулярній основі в майбутньому, відкрийте вікно Додаткові налагодження (F5) Сканування

комп'ютера на вимогу. Натисніть кнопку Профілі, яка розташована в правій частині. У результаті відобразиться список існуючих профілів сканування. Виберіть Створення нового профілю (рис. 12).

Припустимо, необхідно створити окремий профіль сканування, а конфігурація профілю Розумне сканування частково підходить. Однак додатково необхідно включити сканування файлів пакувальників у режимі реального часу й потенційно небезпечного ПЗ, а також застосувати режим ретельного очищення. Натисніть кнопку Додати у вікні Профілі конфігурації, потім виберіть профіль Розумне сканування у розділі копіювання налагоджень у меню профілів. Налагодьте необхідні параметри.

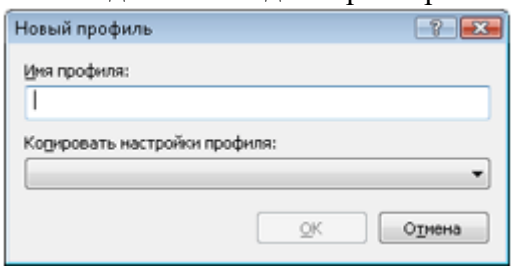


Рис. 12. Новий профіль

Об'єкти.

Цей розділ призначений для вибору об'єктів сканування.

Оперативна пам'ять – включає сканування оперативної пам'яті на предмет наявності активних погроз. Завантажувальні сектори – включає сканування завантажувальних і Mbr-Секторів жорсткого диска. Файли – включає сканування окремих файлів (не архівів). Поштові файли – включає сканування поштових файлів (у форматі EML). Архіви – включає сканування файлів в архіві (RAR, ZIP, ARJ, TAR і т.п.). Архіви, що саморозпаковуються, – включает сканування файлів в архівах, що само розпаковуються. Пакувальники – включає сканування файлів, що виконуються, які розпаковуються в оперативну пам'ять при виконанні (UPX, yoda, Aspack і т.п.).

Параметри.

Розділ Параметри призначений для вибору використовуваних методів сканування й типів додатків, які слід виявляти. Доступні наступні варіанти:

Сигнатури – надійний і точний метод виявлення й класифікації шкідливих програм за допомогою бази даних сигнатур вірусів. Евристичний аналіз – алгоритм, що аналізує активність програм у віртуальнім середовищі. Основною перевагою методу є здатність виявляти нове шкідливе програмне забезпечення, відомості про який ще не потрапили в базу даних сигнатур вірусів. Розширена евристика – цей метод заснований на застосуванні унікальних складних алгоритмів, розроблених компанією ESET, оптимізованих для виявлення шкідливих програм і написаних на мовах програмування високого рівня. Розширена евристика значно поліпшує можливості програм ПЗ профілактичнім виявленню вірусів. Рекламне/шпигунське/небезпечне ПЗ – ця категорія містить у собі програми, що збирають важливу інформацію про користувачів без їхньої згоди. Крім того, сюди ставляться програми, що відображають рекламні матеріали. Потенційно небажане ПЗ – ці додатки не обов'язково є зловмисними, але вони можуть тим або іншим способом знижувати продуктивність системи. Такі додатки звичайно вимагають згоди користувача при установці. Після їхньої налагодження поведінка системи змінюється (у порівнянні з тим, як вона поводилася до налагодження цих програм). Найбільш істотні зміни пов'язані з виникненням небажаних спливаючих вікон, запуском і роботою схованих процесів, збільшенням рівня використання системних ресурсів, зміною результатів пошукових запитів і з'єднанням додатків з вилученими серверами. Потенційно небезпечне ПЗ –

комерційні легітимні додатки можуть бути класифіковані як потенційно небезпечне ПЗ. Сюди ставляться програми, які можуть бути використані в шкідливих цілях без згоди користувача (наприклад, засобу вилученого адміністрування). При включенні даного параметра в мережевім середовищі переконайтеся в тому, що використовувані вами засобу вилученого адміністрування не виявлені. А якщо ні, то їх можна виключити зі сканування, якщо відключення потенційне небезпечних програм небажане.

Очищення.

Параметри процесу очищення визначають поведінка модуля сканування під час очищення заражених файлів. Передбачено три рівні очищення:

Попередження.

У режимі за замовчуванням тільки заражені файли архіву підлягають видаленню. Якщо при цьому є незаражені файли, вони залишаються в архіві. Якщо заражений архів виявлений у режимі ретельного очищення, увесь архів віддаляється, навіть якщо присутні файли без шкідливого коду.

Не очищати Заражені файли не будуть очищатися автоматично. Програма виводить попередження й пропонує користувачеві вибрати дія.

Рівень за замовчуванням Програма намагається автоматично очистити або вилучити заражений файл. При неможливості вибрати необхідна дія автоматично програма пропонує зробити вибір користувачеві. Вибір користувачеві надається й у тому випадку, якщо визначена дія не може бути виконана.

Ретельне очищення. Програма очищає або видаляє всі заражені файли, включаючи архівні. Єдине виключення становлять системні файли. Якщо це неможливо, користувачеві виводиться попередження із пропозицією виконати певну дію.

Розширення.

Розширенням називається частина імені файлу, відділена від основної частини крапкою. Звичайне розширення позначає тип файлу або його вміст. Цей розділ параметрів системи своєчасного виявлення дозволяє визначити типи файлів, що підлягають скануванню.

За замовчуванням скануються всі файли незалежно від їхнього розширення. Будь-яке розширення можна додати до списку виключень зі сканування. Якщо прапорець Перевіряти всі файли не встановлений, найменування списку змінюється на Список файлів, що скануються. Він містить попередньо певні налагодження для більшості типів файлів. За допомогою кнопок Додати і Вилучити можна змінювати вміст списку, забороняючи або дозволяючи сканування для тих або інших розширень.

Для того щоб включити сканування файлів без розширень, установіть прапорець Сканувати файли без розширень.

Виключення файлів призначене для тих випадків, коли сканування файлів певного типу приводить до помилок у роботі програм, які їх використовують. Наприклад, ця ситуація можлива для файлів з розширеннями EDB, EML і TMP, які використовуються сервером Microsoft Exchange.

Обмеження.

Нижче наведені параметри, що дозволяють задати максимальний розмір об'єктів і рівень вкладеності архівів, що підлягають скануванню.

Максимальний розмір об'єкта, у байтах. У це поле вводиться число, що задає максимальний розмір об'єктів. Після налагодження цього обмеження модуль захисту від вірусів буде перевіряти тільки об'єкти менше зазначеного розміру. Не рекомендується змінювати значення за замовчуванням, якщо для цього немає особою причини. Даний

параметр призначений для досвідчених користувачів, яким необхідно виключити більші об'єкти із процесу сканування.

Максимальний час сканування, у секундах. Визначає максимальний час сканування об'єкта. Якщо в цьому полі втримується задане користувачем значення, після закінчення зазначеного часу антивірусний модуль перериває сканування поточного об'єкта незалежно від того, чи завершене воно.

Рівень вкладеності архіву Визначає максимальну глибину перевірки архівів. Не рекомендується міняти значення за замовчуванням, рівне 10, якщо для цього немає особою причини. Якщо сканування передчасно переривається через перевищення значення даного параметра, архів залишається неперевіреним.

Максимальний розмір файлу в архіві, у байтах. Цей параметр дозволяє задати максимальне число файлів, що перевіряються, в архіві (при їхньому витягу). Якщо сканування передчасно переривається через перевищення значення даного параметра, архів залишається неперевіреним.

Інше.

Цей розділ призначений для налагодження різних параметрів модуля сканування Threatsense.

Реєструвати всі об'єкти. Включає занесення інформації про всі просканові об'єкти у журнал. Якщо включений захист файлової системи в режимі реального часу, записи в журнал підлягають просканові файли в архівах. Не рекомендується включати даний параметр, особливо при повному скануванні жорстких дисків.

Сканувати потоки даних ADS. Альтернативні потоки даних (ADS) використовуються файловою системою NTFS при роботі з файлами й каталогами, які не видимі для звичайного процесу сканування. Багато шкідливих програм використовують альтернативні потоки даних для того, щоб уникнути виявлення.

Запустити фонове сканування з низьким пріоритетом. Кожний процес сканування споживає деяку кількість системних ресурсів. Якщо користувач працює із програмами, що пред'являють високі вимоги до системних ресурсів, можна запустити сканування в режимі низького пріоритету й визволити ресурси для інших додатків.

Зберегти оцінку про час останнього доступу. Зберігає вихідну оцінку про час доступу до файлам, що скануються, не обновляючи її (наприклад, для правильного функціонування систем резервного копіювання).

Прокрутити журнал сканування. Якщо прокручування включене, нова інформація завжди відображається в нижній частині екрану.

Показувати повідомлення про завершення сканування в окремому вікні. Відкриває окреме вікно для відображення результатів сканування.

Виявлене зараження.

Система може одержати шкідливий код з різних джерел – веб-сайти, каталоги загального доступу, електронна пошта або змінні носії (USB, зовнішні диски, компакт-диски, диски DVD і т.д.).

Якщо на комп'ютері виникли ознаки зараження (наприклад, він став повільніше працювати, часто зависає й т.п.), рекомендується виконати наступне:

- Відкрийте ESET Smart Security Сканування комп'ютера;
- Натисніть кнопку Звичайне сканування;
- Після закінчення сканування подивіться журнал на предмет кількості перевірених, заражених і вилікуваних об'єктів.

Якщо необхідно перевірити тільки частину диска, виберіть Сканування з користувацькими налагодженнями, потім – Об'єкти для сканування.

Для прикладу того, що відбувається, коли система ESET Smart Security знаходить зараження, припустимо, що зараження виявлене модулем захисту файлів у режимі реального часу, який використовується в режимі очищення за замовчуванням. Модуль намагається очистити або вилучити файл. Якщо дія за замовчуванням для модуля захисту в режимі реального часу не визначена, запит відправляється користувачеві. Звичайно надається вибір з дій Очистити, Вилучити або Пропустити. Не рекомендується використовувати дію, Пропустити тому що заражений файл залишиться на комп'ютері. Цю дію слід використовувати тільки тоді, коли є повна впевненість у тому, що файл нешкідливий і потрапив під підозру помилково.

Очищення й видалення. Застосуєте очищення, якщо корисний файл був атакований вірусом, який додає шкідливих код до корисного. У в першу цьому випадку слід спробувати очистити файл, щоб відновити його первісний стан.

Видалення файлів з архівів. У звичайному режимі архів цілком видаляється, якщо містить тільки заражені файли. Архіви не віддаляються, якщо містять незаражені файли. Проте, при скануванні в режимі ретельного очищення архів віддаляється, якщо містить як мінімум один заражений файл, незалежно від стану інших файлів в архіві.

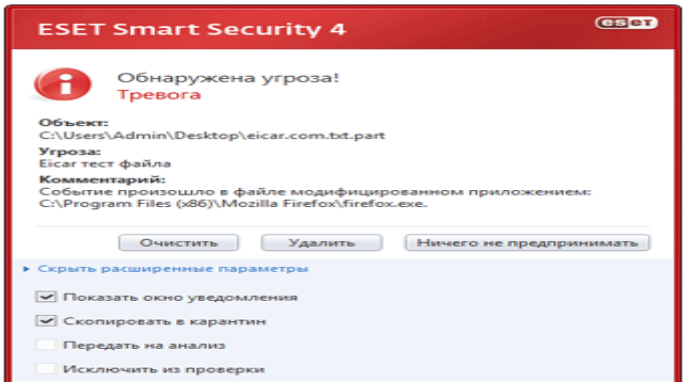


Рис. 13. Вікно погрози

Режими фільтрації

Персональний брандмауер ESET Smart Security підтримує 5 режимів фільтрації мережного трафіка. Рівень взаємодії з користувачем і поведінка персонального брандмауера засновані на обраному режимі.

- Автоматичний режим – це режим за замовчуванням, який призначений для випадку, коли не треба визначати правила. Автоматичний режим дозволяє сканувати весь вихідний трафік для комп'ютера користувача й блокує всі нові з'єднання ззовні.
- Автоматичний режим з виключеннями (правила, встановлені користувачем) – користувачеві дозволено додавати свої правила.
- Інтерактивний режим – допускаються користувацькі конфігурації. Коли виявляється з'єднання без відповідного правила, виводиться діалогове вікно із пропозицією дозволити або заборонити з'єднання. Також існує можливість створити нове правило, щоб завжди дозволяти або забороняти подібні з'єднання в майбутньому.
- Режим на основі політики – блокуються всі з'єднання, що не задовольняють жодному з раніше певних розв'язних правил. Цей режим призначений для досвідчених користувачів, які точно знають, які з'єднання їм необхідні.
- Режим навчання – автоматичне створення й збереження правил, призначений для первісного налагодження персонального брандмауера. Участь користувача не потрібно, тому що ESET Smart Security зберігає правила згідно з попередньо налагодженими параметрами. Режим навчання є небезпечним, тому

рекомендується використовувати його тільки до моменту створення правил для всіх необхідних з'єднань.

-

Профілі

Профілі дозволяють контролювати поведінку персонального файервола ESET Smart Security. При створенні або зміні правила персонального файервола (рис. 14) його можна призначити окремому профілю або застосувати до всіх профілів. При виборі певного профілю діють тільки глобальні правила (без вказівки профілю) і правила, призначені цьому профілю. Для легкої зміни поведінки персонального файервола можна створити кілька профілів з різними призначеними правилами.

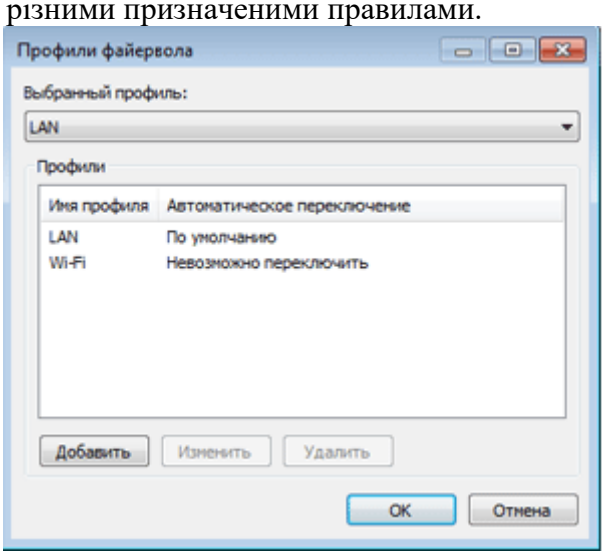


Рис.14. Профіль

Керування профілями

Для того щоб відкрити вікно Профілі файервола, у якому можна додавати, змінювати й видаляти профілі, натисніть кнопку Профілі.... Майте на увазі, що змінити або вилучити профіль, зазначений у меню, що розкривається, Обраний профіль, не можна. При додаванні або зміні профілю можна задати умови, при яких він запуститься. Доступні зазначені нижче параметри (рис. 15).

Не перемикатися автоматично – автоматичний запуск відключений (профіль повинен бути активований вручну).

Якщо ця зона аутентентифікована – цей профіль запуститься, коли певна зона буде аутентентифікована.

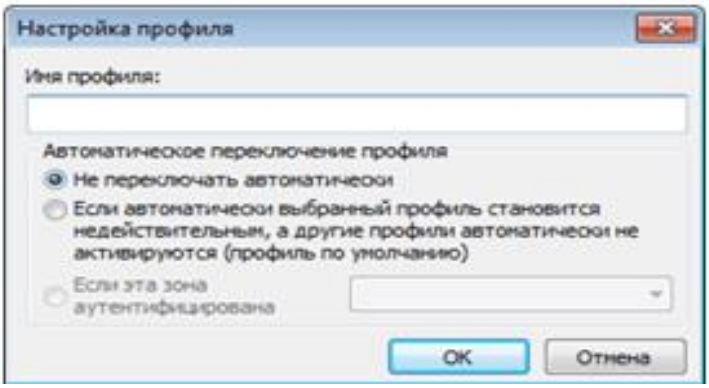


Рис. 15 Налагодження профілю

При перемиканні профілів персонального файервола в правому нижньому куті поруч із системним годинником з'являється відповідне повідомлення.

Блокувати весь трафік: відключити мережу

Заблокувати весь мережевий трафік можна тільки за допомогою функції Блокувати весь трафік: відключити мережу (рис. 16). Усі вхідні й вихідні з'єднання будуть заблоковані персональним брандмауером без попередження. Використовуйте цю функцію тільки в особливих випадках, коли виникає небезпечна критична ситуація, що вимагає негайного відключення від мережі.

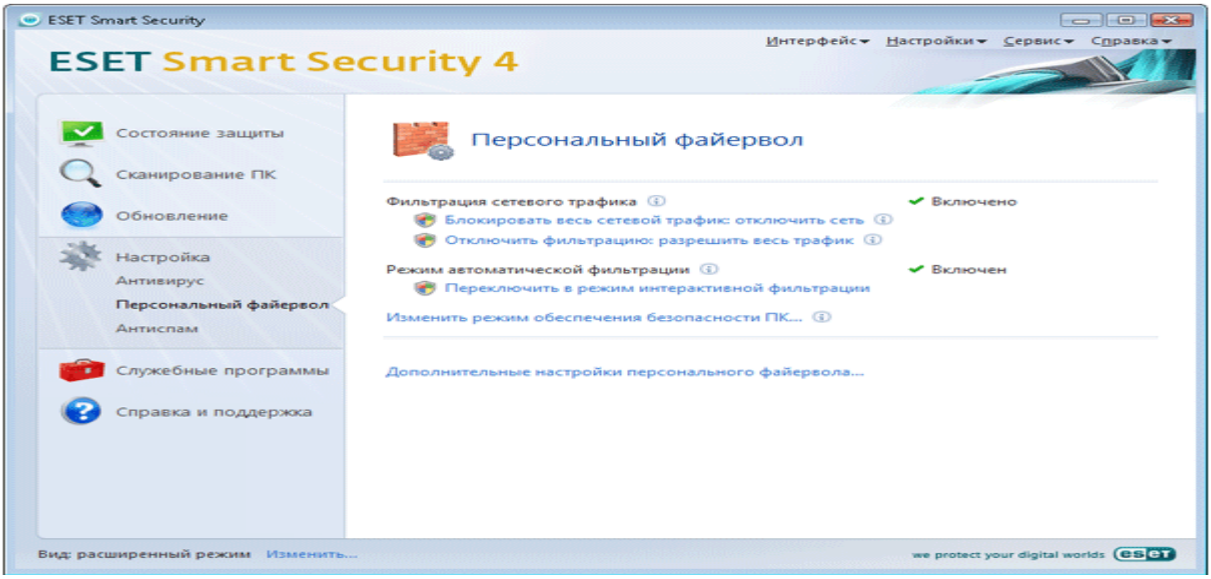


Рис. 16. Блокування трафіка

Відключити фільтрацію: дозволити весь трафік.

Заборона фільтрації є прямо протилежним режимом раніше згаданому режиму блокування всіх з'єднань. У цьому режимі персональний брандмауер відключає всі функції фільтрації й дозволяє всі вхідні й вихідні з'єднання. З погляду мережі це еквівалентно повній відсутності персонального брандмауера.

1.19 Створення нових правил

При установці нового додатка, який використовує доступ до мережі, або при зміні параметрів існуючого з'єднання (адреса вилученого комп'ютера, номер порту й т.п.) необхідне створення нового правила.

Для того щоб додати нове правило, у вікні Зони й правила натисніть кнопку Створити. У результаті відкриється діалогове вікно, у якому можна створити нове правило (рис. 17). Верхня частина діалогового вікна містить три вкладки:

- Загальні (рис. 18) – містить ім'я правила, напрямок з'єднання, дія й протокол. Напрямок може бути зазначений як у зовнішню мережу, так і з неї (або обоє напрямків). Дія має на увазі дозвіл або заборона відповідного з'єднання.
- Локальний комп'ютер – містить інформацію про локальну сторону з'єднання. Інформація містить номер порту або діапазон припустимих портів, а також назву додатка.
- Віддалений комп'ютер – містить інформацію про віддалений порт (або діапазоні портів). Крім того, на ній можна вказати список віддалених адрес і зон для відповідного правила.

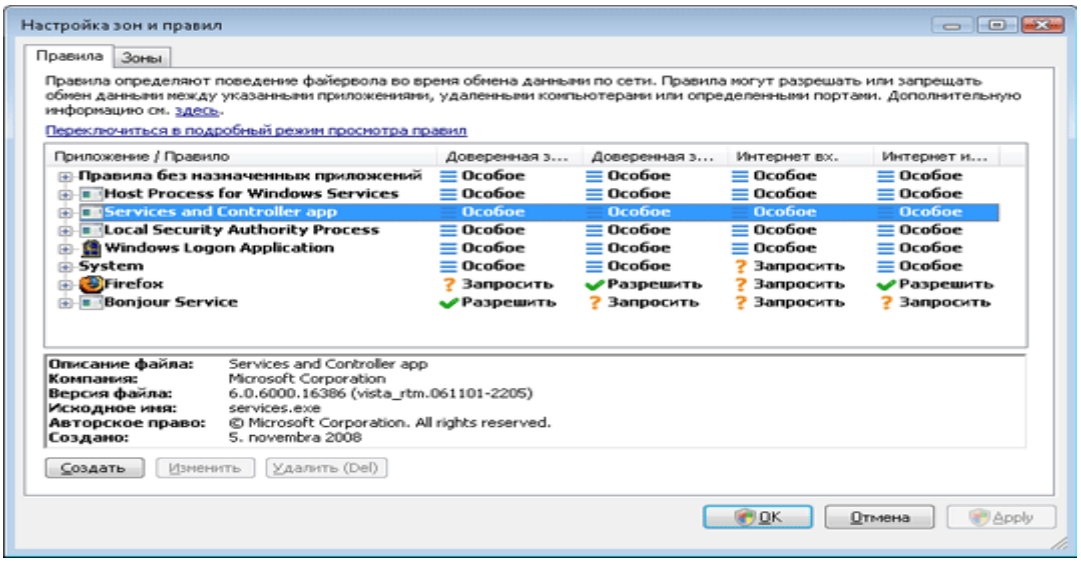


Рис. 17 Вікно правил

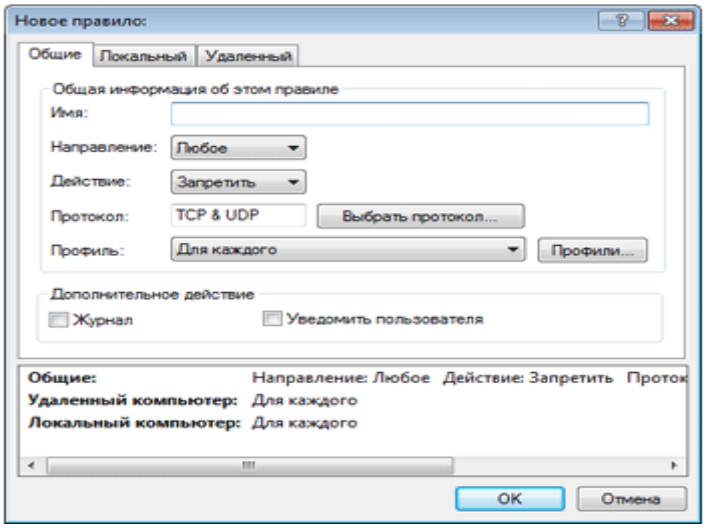


Рис. 18. Вкладка загальні

Гарним прикладом є створення правила доступу в Інтернет для веб-браузера. У цьому випадку необхідно виконати наступні налагодження:

- На вкладці Загальні дозволите обмін даними ПЗ за протоколами TCP і UDP.
- На вкладці Локальний комп'ютер укажіть ім'я процесу додатка веб-браузера (для браузера Internet Explorer – iexplore.exe).
- На вкладці Віддалений комп'ютер дозволите обмін даними через порт 80, якщо необхідно дозволити тільки стандартний порт для перегляду веб-сторінок.

Зміна правил.

Для того щоб змінити існуюче правило, натисніть кнопку Змінити потрібно при кожній зміні параметрів об'єкта спостереження. Якщо параметри об'єкта змінилися, то умови правила не виконуються й зазначену дію не проводиться. У результаті з'єднання може бути заблоковане, що викличе проблеми в роботі з додатком. Прикладом змінних параметрів може бути мережна адреса або номер порту віддаленого комп'ютера.

1.20 Аутентифікація зон: конфігурація клієнта

У вікні Налагодження зони створіть зону, використовуючи ім'я зони, що аутентифікована сервером. Для того щоб додати маску, що містить сервер аутентифікації,

натисніть кнопку **Додати адресу Ipv4** і виберіть параметр **Подсеть**. Відкрийте вкладку **Аутентыфикация** зони (рис. 19) і виберіть параметр **Ip-Адреси и подсети** цієї зони стануть дійсними після успішної аутентифікації в мережі. Коли цей параметр установлений, зона стає недійсною, якщо аутентифікація не виконана. Для того щоб вибрати профіль персонального файервола, який буде активуватися після аутентифікації, натисніть кнопку **Профили**.... Якщо обраний параметр Додати адреси й підмережі цієї зони в довірену зону (рекомендується), після аутентифікації адреси й підмережі зони будуть додані в довірену зону.

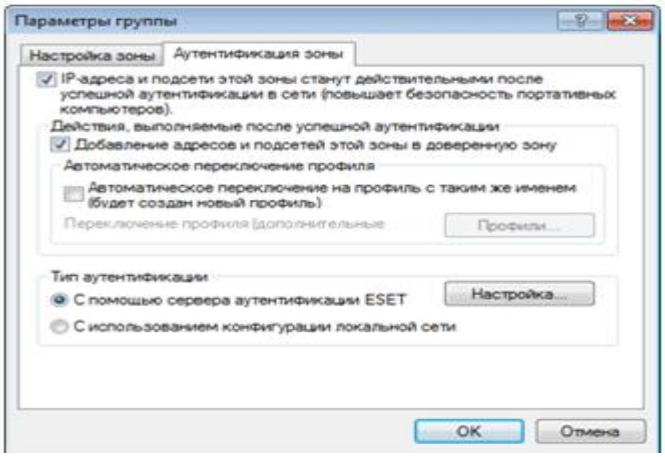


Рис. 19. Аутентифікація

Існує два типи аутентифікації.

1. За допомогою сервера аутентифікації ESET Натисніть кнопку Налагодження... і вкажіть ім'я сервера, його відкритий ключ, порт що прослуховує. Ім'я сервера можна ввести у формі Ip-Адреси або імені DNS або Netbios. Після імені сервера можна вказати шлях до файлу на сервері (наприклад, server_name_/directory1/directory2/authentication). На випадок неприступності першого сервера можна вказати додаткові сервери, відокремивши їх імена крапкою з комою. Відкритим ключем може бути файл одного із зазначених нижче типів.

- Зашифрований відкритий ключ у форматі PEM (його можна створити за допомогою додатка ESET Authentication Server)
- Закодований відкритий ключ
- Сертифікат відкритого ключа (CRT) (рис. 20).

Для того щоб перевірити свої налагодження, натисніть кнопку Перевірити. Якщо аутентифікація пройшла успішно, з'явиться відповідне повідомлення. Якщо аутентифікація не налагоджена належним чином, з'явиться одне із зазначених нижче повідомлень.

- Збій аутентифікації сервера. Максимальний час аутентифікації минув. Сервер аутентифікації недоступний. Перевірте ім'я сервера й Ip-Адресу або параметри персонального файервола клієнта, а також параметри сервера.
- При з'єднанні із сервером відбулася помилка. Сервер аутентифікації не працює. Запустіть службу сервера аутентифікації.
- Ім'я зони аутентифікації не відповідає імені зони сервера. Настроєне ім'я зони не відповідає зоні сервера аутентифікації. Переглянете обидві зони й задайте для них однакові імена.

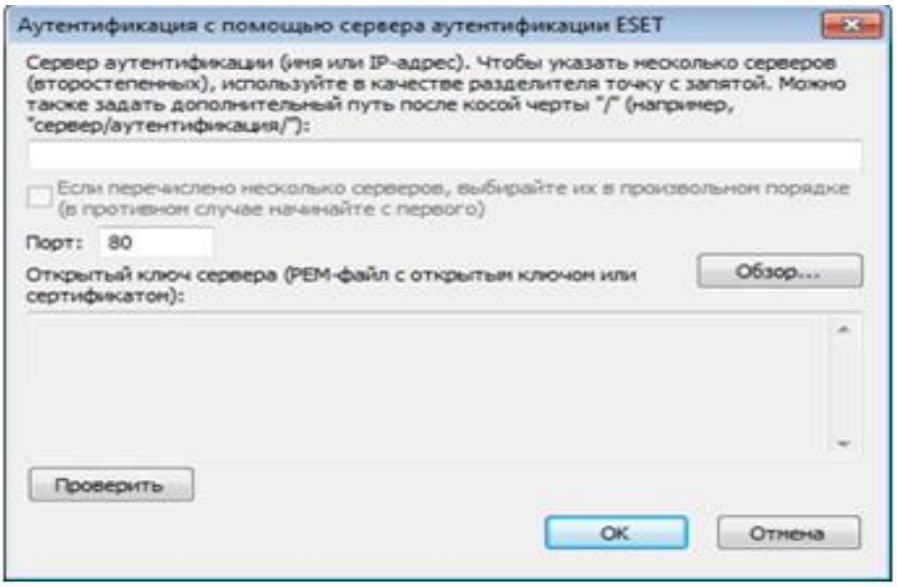


Рис. 20. Відкритий ключ

- Збій аутентифікації сервера. Адреса сервера не знайдена в списку адрес зазначеної зони. Ip-Адреса комп'ютера, на якій запущений сервер аутентифікації, перебуває поза заданим діапазоном Ip-Адрес у поточній конфігурації зони.
- Збій аутентифікації сервера. Можливо, уведений недійсний відкритий ключ. Переконайтеся в тому, що зазначений відкритий ключ відповідає закритому ключу сервера. Крім того, перевірте, чи ушкоджений файл відкритого ключа.

2. З використанням конфігурації локальної мережі (рис. 21)- аутентифікація виконується відповідно до параметрів адаптера локальної мережі. Вона вважається виконаною, якщо дійсні всі параметри, обрані для активного підключення.

Аутентифікація зон: конфігурація сервера

Аутентифікацію мережі можна виконати за допомогою будь-якого підключеного до неї комп'ютера або сервера. Для цього на комп'ютер або сервер, який завжди доступний для аутентифікації, коли клієнт намагається підключитися до мережі, потрібно встановити додаток ESET Authentication Server. Файл налагодження цього додатка можна завантажити із сайту http://www.eset.eu/download/registered.

Після налагодження ESET Authentication Server з'явиться діалогове вікно. (Додаток можна запустити в будь-який момент, нажавши кнопку Пуск і вибравши послідовно пункти Програми/ESET/ESET Authentication Server/ESET Authentication Server.) (рис. 22)

Для того щоб налагодити сервер аутентифікації, уведіть ім'я зони аутентифікації порт, що прослуховує, сервера (за замовчуванням 80) і створіть відкритий і закритий ключі, які будуть використовуватися при аутентифікації. Створені ключі будуть зберігатися в папці набору. Закритий ключ повинен використовуватися на сервері, а відкритий – на стороні клієнта, у конфігурації сервера аутентифікації в розв'язку ESET Smart Security.

Установка з'єднання – виявлення

Персональний брандмауер виявляє кожне зі знову створених мережних з'єднань. Активний режим персонального брандмауера (автоматичний, інтерактивний або на основі

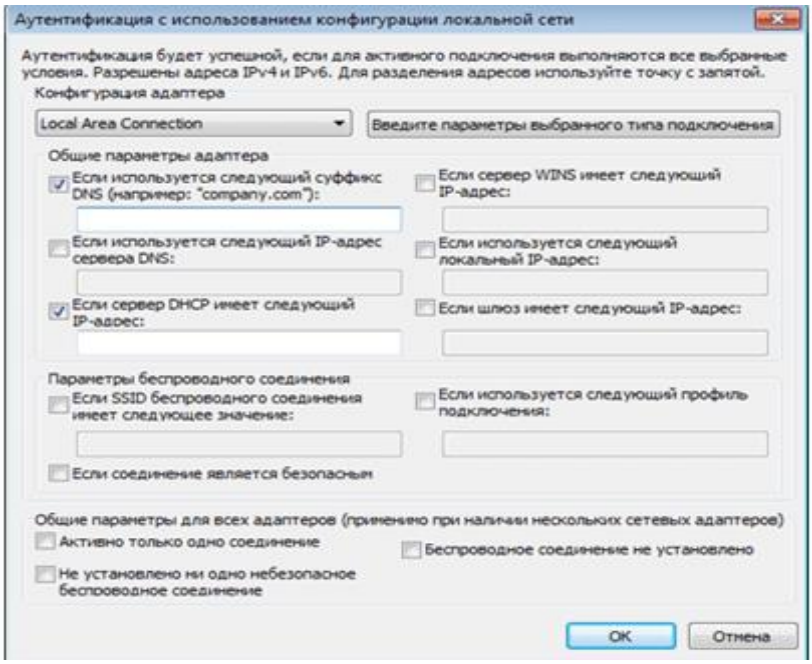


Рис. 21 Аутентифікація використанням конфігурації локальної мережі

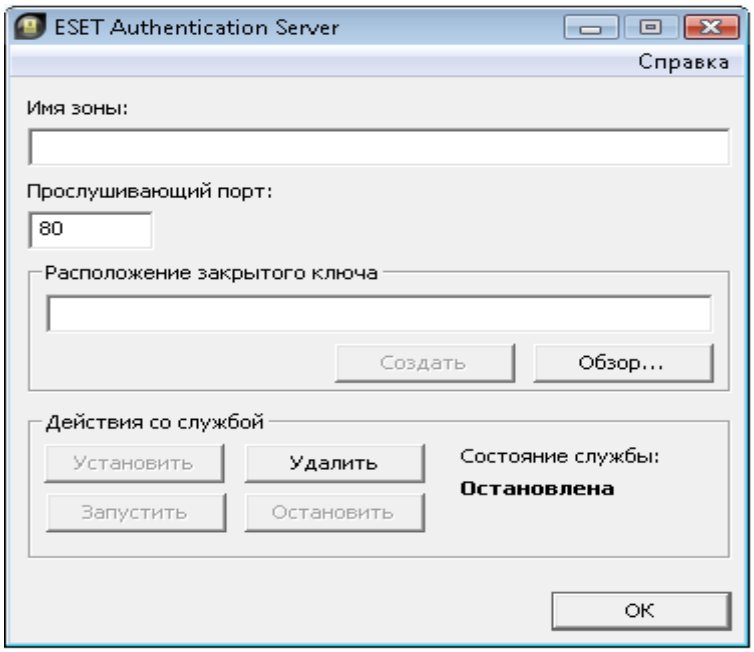


Рис. 22. Вікно програми

політики) визначає, які дії повинні виконуватися для нового з'єднання. При роботі в автоматичному режимі або режимі на основі політики персональний брандмауер виконує дії без втручання користувача. В інтерактивному режимі виводиться інформаційне вікно (рис. 23) з повідомленням про встановлення з'єднання. Воно містить інформацію про нове з'єднання. Користувач може дозволити або заборонити (заблокувати) з'єднання. Якщо з'єднання одного типу виникають регулярно, і їх доводиться дозволяти вручну, рекомендується створити для них правило. Для цього виберіть функцію Запам'ятати дію (створити правило)» і збережіть нове правило для персонального брандмауера. Якщо персональний брандмауер виявить таке з'єднання в майбутньому, він застосує це правило.

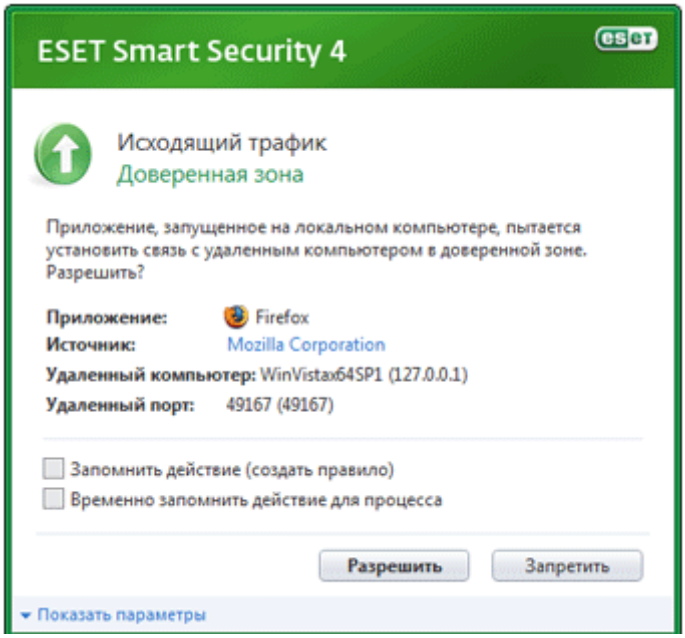


Рис. 23. Підключення з'єднання

Будьте уважні при створенні нових правил. Дозволяйте тільки безпечні з'єднання. Якщо дозволити всі з'єднання, персональний брандмауер не зможе забезпечувати захист. Нижче перераховані найбільш важливі параметри з'єднань:

- Віддалений комп'ютер: дозволити з'єднання тільки з довіреними й відомими адресами.
- Локальний додаток: не рекомендується дозволяти з'єднання з невідомими додатками й процесами.
- Порт: з'єднання на стандартних портах (наприклад, для перегляду веб-сторінок — порт номер 80) звичайно є безпечним.

Комп'ютерні віруси для розмноження часто використовують з'єднання з Інтернетом або сховані з'єднання, через які відбувається зараження інших комп'ютерів. Якщо правила налагоджені належним чином, персональний брандмауер є ефективним засобом протидії множинним зловмисним атакам

Ведення журналу

Персональний брандмауер у складі ESET Smart Security зберігає дані про важливі події у файлі журналу, який можна відкрити за допомогою головного меню програми. Виберіть Службові програми/Файли журналу, потім Журнал персонального файервола Eset. (рис. 24). Файли журналів є незамінним інструментом, який допомагає виявляти помилки й протидіяти зараженню. Журнали персонального брандмауера ESET містять наступну інформацію:

- дата й час події;
- подія;
- мережеві адреси джерела й об'єкта;
- мережевий протокол передачі даних;
- застосоване правило або ім'я хробака (якщо виявлене);
- задіяний додаток.

Ретельний аналіз інформації значно полегшує процес оптимізації системної безпеки. Багато факторів є індикаторами потенційних погроз і дозволяють користувачеві звести їхній вплив до мінімуму: занадто часті з'єднання від невідомих комп'ютерів,

множинні спроби встановити з'єднання, мережна активність невідомих додатків або з використанням невідомих номерів портів.

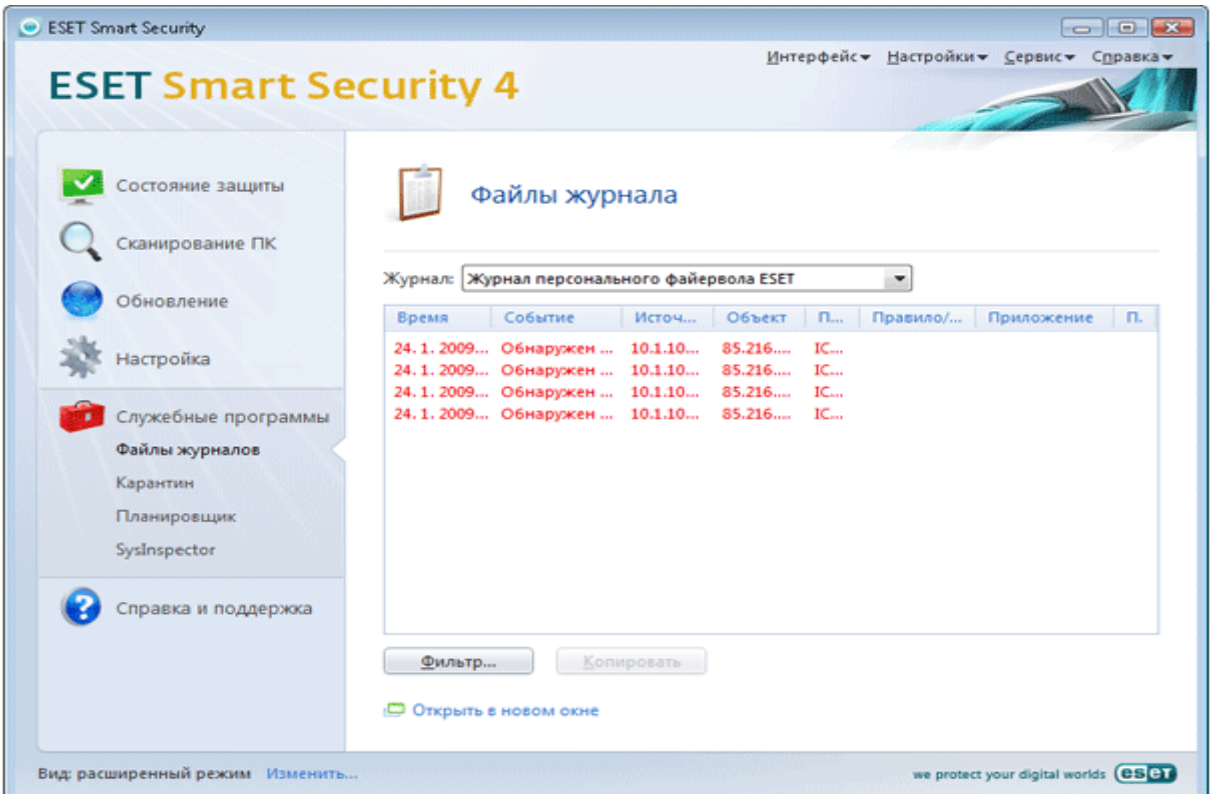


Рис. 24. Вікно журналу.

1.21 Спам

Додавання адрес в білий і чорний списки.

Адреси електронної пошти, що належать особам, з якими користувач часто спілкується, можуть бути занесені в список безпечних адрес – білий список. Цей захід запобігає отриманню повідомлень від адресатів білого списку в категорію небажаних. Для того щоб додати адреса в білий список, у контекстному меню відповідного повідомлення виберіть ESET Smart Security/Додати в білий список або виберіть Довірені адреси на панелі інструментів ESS, розташованої у верхній частині вікна поштової програми.

Цей процес може застосовуватися й до адрес небажаної пошти. Якщо адреса електронної пошти втримується в чорному списку, кожне повідомлення електронної пошти від цієї адреси буде класифіковано як небажане.

Оцінка повідомлень як небажаної пошти

Будь-яке повідомлення, що проглядається в поштовому клієнтові, може бути віднесене до категорії небажаних. Для цього необхідно використовувати команду контекстного меню (клацання правої клавіші миші ESET Smart Security – Класифікувати обрані повідомлення як спам) або вибрати параметр Спам на панелі інструментів ESS у поштовому клієнтові. При класифікації повідомлення автоматично поміщається в папку небажаної пошти, але адреса відправника не поміщається в чорний список. Подібним чином відбувається класифікація повідомлень як корисних. Якщо повідомлення з каталоги небажаної пошти класифікуються як корисні, вони переміщаються у вихідну папку. При цьому адреса відправника не поміщається автоматично в білий список.

Призначення запланованих завдань

Планувальник управляє й запускає завдання за розкладом з визначеними параметрами. Параметри містять інформацію, таку як дата й час виконання, а також профілі відновлення, які використовуються під час виконання завдання.

Створення нового завдання.

Для того щоб створити нове завдання в планувальнику, натисніть кнопку **Добавить** або виберіть пункт **Добавить** у контекстному меню. Доступні п'ять типів завдань (рис. 25):

- Запуск зовнішнього додатка;
- Обслуговування журналу;
- Перевірка файлів, що виконуються при запуску системи;
- Сканування комп'ютера на вимогу;
- Відновлення.

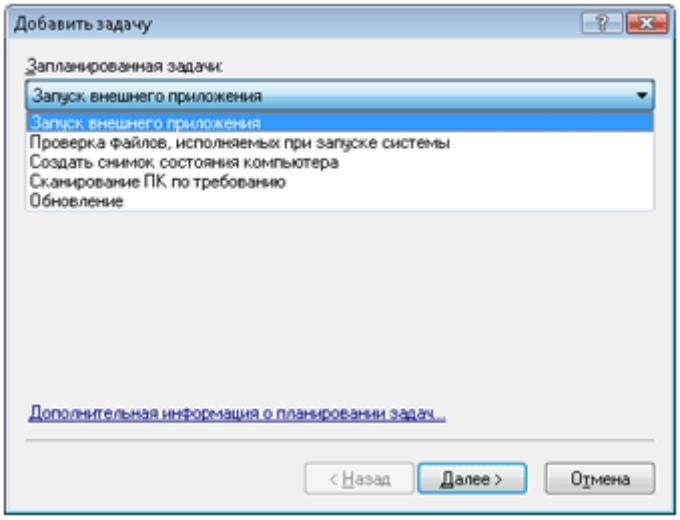


Рис. 25. Завдання

Тому що найбільше часто використовуваними завданнями є Сканування комп'ютера на вимогу і Відновлення, нижче описане створення завдання відновлення.

У меню планувальника, що містить усі типи завдань, виберіть Відновлення. Натисніть Далі і введіть ім'я завдання в поле Ім'я завдання. Виберіть частоту запуску завдання. Для цього параметра доступні значення: Одноразово, Багаторазово, Щодня, Щотижня і За певних умов. Цей параметр визначає й інші параметри. Далі вкажіть (якщо необхідно), яку дію слід почати, якщо завдання не виконане або не завершене успішно у встановлений час. Доступні наступні варіанти:

- Чекати до наступного наміченого моменту;
- Виконати завдання якомога швидше;
- Виконати завдання негайно, якщо час, з останнього запуску, перевищив зазначений інтервал (при виборі цього варіанта доступне налагодження інтервалу часу).

На наступному кроці відображається зведена інформація про поточне плановане завдання. Пункт Запустити завдання із зазначеними параметрами автоматично обраний. Натисніть кнопку Готово. У вікні, що відкрилося, виберіть профіль, використовуваний при виконанні завдання. Можна вибрати основний або альтернативний профіль, який буде використовуватися, якщо запуск завдання пройде невдало за допомогою основного профілю. Підтвердіть налагодження, нажавши кнопку ОК у вікні профілю відновлення. Нове завдання з'явиться в списку запланованих.

Переміщення файлів на карантин

Програма автоматично поміщає вилучені файли на карантин (якщо ця функція не відключена у вікні попередження). При необхідності користувач може самостійно помістити на карантин будь-який підозрілий файл за допомогою кнопки Додати. При цьому вихідна копія файлу не видаляється. Для цього також можна скористатися командою Додати контекстного меню у вікні карантину.

Відновлення з карантину

Ізольовані файли можуть бути відновлені у вихідне місце розташування в системі. Для цього призначена функція Відновити, доступна в контекстному меню вікна карантину. Крім того, контекстне меню містить функцію Відновити в, яка дозволяє відновлювати файли в інше місце розташування, відмінне від вихідного.

Передача файлу з карантину

Якщо на карантин поміщений файл, погроза в якому не розпізнана програмою, або файл невірно кваліфікований як заражений (наприклад, у результаті помилки евристичного методу) і ізольований, передайте файл у лабораторію ESET. Для того щоб передати файл із карантину, виберіть його й використовуйте пункт Передати на аналіз контекстного меню.

Обслуговування журналу

Налагодити ведення журналу ESET Smart Security можна в розділі Налагодження/Уведення всього дерева розширених параметрів/Службові програми/Файли журналу. Для файлів журналу можна задати наступні параметри (рис. 26).

- Автоматично видаляти записи – запису в журналі старше зазначеного часу (у днях) будуть автоматично видалятися.
- Автоматично оптимізувати файли журналів – файли журналу автоматично дефрагментируються, якщо перевищений зазначений відсоток невикористаних записів.
- Мінімальний ступінь деталізації журналу – визначає рівень деталізації журналу.

Доступні наступні варіанти.

Діагностичні записи – найдетальніший рівень, що включає дані, необхідні для точного налагодження програми, і всі описані нижче записи.

Інформаційні записи – інформаційні повідомлення, включаючи повідомлення про виконані відновлення, попередження й помилки.

Попередження – повідомлення з попередженнями й помилки.

Помилки – помилки класу Не вдалося завантажити файл і критичні помилки.

Критичні помилки – найнижчий рівень деталізації, що містить критичні системні помилки (наприклад, помилка запуску захисту від вірусів, персональний брандмауер не працює й т.п.)

Попередження й повідомлення.

У розділі Попередження й повідомлення можна набудовувати порядок повідомлення користувача про появу погроз.

Перший пункт – Вікно попередження. Якщо відповідний прапорець зняти попередження не відображаються. Виводяться попередження тільки для вузького кола особливих ситуацій. Для більшості користувачів рекомендується використовувати цю функцію (установити прапорець).

Для того щоб спливаючі вікна закривалися автоматично після закінчення певного періоду часу, установіть прапорець Закривати діалоги повідомлень автоматично після закінчення (сек.). Якщо вікно не закрите користувачем, воно закривається через зазначений проміжок часу.

Повідомлення на робочому столі й спливаючі підказки є інформаційними й не вимагають участі користувача. Вони відображаються на панелі завдань у правій нижній частині екрана. Для того щоб включити повідомлення на робочому столі, установіть прапорець Відображати повідомлення на робочому столі. Більш докладні параметри — час відображення й прозорість вікна — доступні за допомогою кнопки Конфігурація повідомлень. Для попереднього перегляду й оцінки поведінки натисніть кнопку Перегляд. Параметр Відображати підказки на панелі завдань протягом (сек.) призначений для налагодження часу відображення спливаючих підказок.

У нижній частині вікна Попередження й повідомлення розташований параметр Відображати повідомлення тільки при необхідності втручання. Цей параметр дозволяє включати або виключати відображення повідомлень, які не вимагають втручання з боку користувача. Останній параметр цього розділу призначений для визначення адресатів повідомлень у багатокористувацькім середовищі. У поле У багатокористувацьких системах відображати повідомлення для користувача можна вказати користувача, який буде одержувати важливу інформацію про роботу програми ESET Smart Security. Звичайно це системний або мережевий адміністратор. Ця функція особливо корисна для термінальних серверів, у яких усі повідомлення призначають адміністраторові.

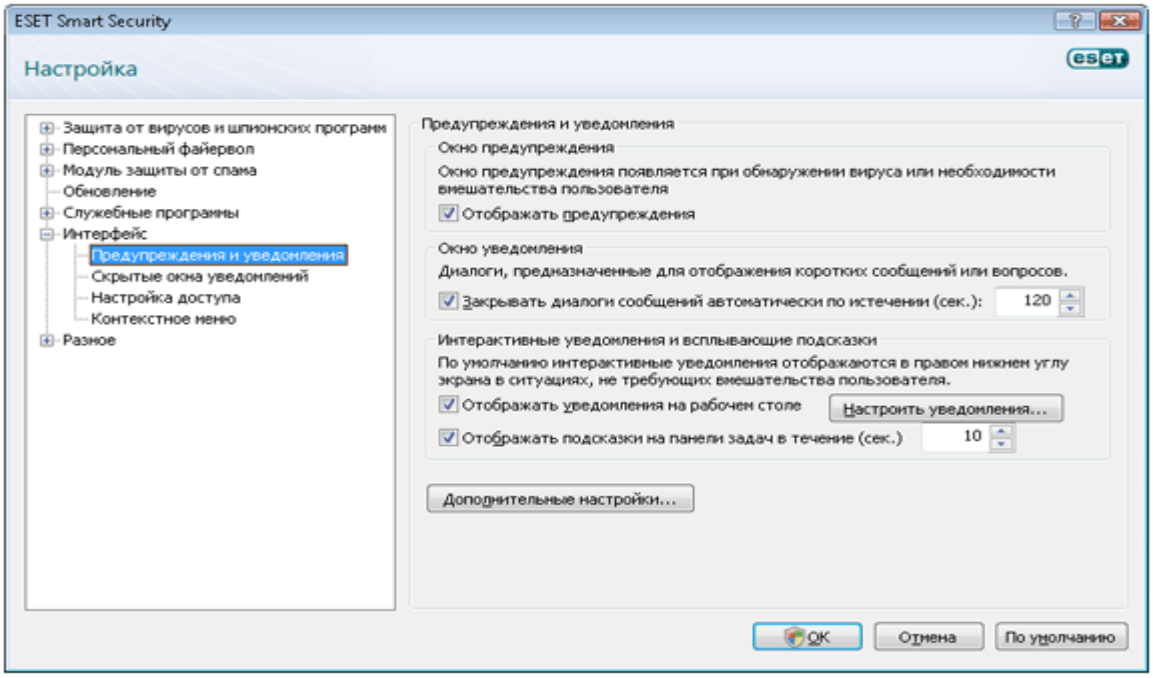


Рис. 26. Налагодження

Підозрілі файли.

Вкладка Підозрілі файли дозволяє користувачеві налагодити спосіб передачі шкідливого коду в лабораторію ESET для аналізу.

Якщо користувач виявив файл із підозрілою поведінкою, він може передати його в лабораторію компанії для подальшого аналізу. Якщо файл містить зловмисний код, інформація про нього буде включена в наступну версію бази даних сигнатур вірусів.

Передача файлів може виконуватися автоматично. Якщо обрана ця функція, підозрілі файли відправляються у фоновому режимі. Для того щоб знати, які файли відправляються для аналізу, і підтверджувати їхнє відправлення, виберіть функцію Запитати перед передачею.

Щоб заборонити передачу файлів, виберіть Не передавати на аналіз. Примітка: заборона на передачу файлів не впливає на передачу статистичної інформації в ESET.

Командний рядок.

Модуль захисту від вірусів ESET Smart Security може бути запущений з командного рядка, вручну (за допомогою команди ecls) або в пакетному режимі (за допомогою файлу bat).

Наступні параметри й аргументи можуть бути використані для запуску сканування на вимогу з командного рядка:

Загальні параметри:	Опис
--help	показати довідку й вийти
--version	показати версію й вийти
--base-dir=КАТАЛОГ	завантажити модулі з каталоги
--quar-dir=КАТАЛОГ	каталог карантину
--aind	показувати індикатор активності
--auto	сканувати всі жорсткі диски в режимі очищення
Об'єкти	
--files	сканувати файли (за замовчуванням)
--no-files	не сканувати файли
--boots	сканувати завантажувальні сектори (за замовчуванням)
--no-boots	не сканувати завантажувальні сектори
--arch	сканувати архіви (за замовчуванням)
--no-arch	не сканувати архіви
--max-archive-level=РІВНІ	максимальний рівень вкладеності архівів
--scan-timeout=ІНТЕРВАЛ	сканувати архіви не довше зазначеного інтервалу в секундах. Якщо час сканування перевищує цей інтервал, сканування архіву припиняється й переходить до наступного файлу
--max-arch-size=РОЗМІР	сканувати тільки першу частину файлу у байтах (за замовчуванням 0 = не обмежене)
--mail	сканувати файли електронної пошти
--no-mail	не сканувати файли електронної пошти
--sfx	сканувати архіви,
--no-sfx	не сканувати архіви,
--rtp	сканувати пакувальники в режимі реального часу
--no-rtp	не сканувати пакувальники в режимі реального часу
--exclude=КАТАЛОГ	виключити папку з перевірок (приклад виключення декількох каталогів: --exclude <перша>,<друга>,...)
--subdir	сканувати вкладені каталоги (за замовчуванням)
--no-subdir	не сканувати вкладені каталоги
--max-subdir-	максимальний рівень вкладеності каталогів (за

level=РІВНІ	замовчуванням 0 = не обмежене)
--symlink	випливати ПЗ символічних посиланнях (за замовчуванням)
--no-symlink	пропускати символічні посилання
--ext-remove=РОЗШИРЕННЯ	виключити файли з розширеннями (через двокрапки) зі сканування
--ext-exclude=РОЗШИРЕННЯ	виключити файли з розширеннями (через двокрапки) зі сканування

Методи	
--adware	сканувати на наявність рекламного/шпигунського/небезпечного ПЗ
--no-adware	не сканувати на наявність рекламного/шпигунського/небезпечного ПЗ
--unsafe	сканувати на наявність потенційно небезпечного ПЗ
--no-unsafe	не сканувати на наявність потенційно небезпечного ПЗ
--unwanted	сканувати на наявність потенційно небажаного ПЗ
--no-unwanted	не сканувати на наявність потенційно небажаного ПЗ
--pattern	використовувати сигнатури
--no-pattern	не використовувати сигнатури
--heur	включити евристику
--no-heur	відключити евристику
--adv-heur	включити розширену евристику
--no-adv-heur	відключити розширену евристику

Очищення	
--action=ДІЇ	виконати дію над зараженими об'єктами. Можливі дії: none (нічого), clean (очистити), prompt (запросити)
--quarantine	копіювати заражені файли в карантин (Додатково до дії)
--no-quarantine	не копіювати заражені файли в карантин

Журнали	
--log-file=ФАЙЛ	записувати інформацію про подію у файл
--log-rewrite	перезаписувати файл журналу (за замовчуванням — додавати)
--log-all	реєструвати інформацію про незаражені файли
--no-log-all	не реєструвати інформацію про незаражені файли (за замовчуванням)

Можливі коди завершення:

Примітка. Значення коду завершення більше 100 означає те, що файл не був сканований і може бути заражений. 0 – не знайдений потік 1 – вірус знайдений і вилучений 10 – не вдалося перевірити деякі файли 50 – деякі файли залишилися зараженими 100 – інша помилка

Клавіші швидкого доступу

В інтерфейсі користувача ESET Smart Security доступні наступні комбінації клавіш швидкого доступу.

Комбінація клавіш	Опис
Ctrl + G	перемикання між графічним і текстовим режимами
Ctrl + I	запуск ESET Sysinspector
Ctrl + L	виклик файлів журналу
Ctrl + M	перемикання між стандартним і розширеним режимами відображення
Ctrl + Q	каталог карантину
Ctrl + R	відновлення виду вікна за замовчуванням
Ctrl + S	виклик розкладу
Ctrl + U	вікно налагодження імені користувача й пароля
F1	виклик довідки
Ctrl + F1	виклик змісту довідки
Ctrl + Shift + F1	виклик пошуку ПЗ довідці
F5	виклик додаткових параметрів

Сценарій обслуговування

Сценарій обслуговування є допоміжним засобом для користувачів програми ESET Sysinspector. Він призначений для видалення із системи небажаних об'єктів.

Сценарій обслуговування дозволяє користувачам цілком або частково експортувати журнал Sysinspector. Після експорту користувач може вибрати й відзначити об'єкти для видалення. Потім можна запустити сценарій з відредагованим журналом для видалення відзначених об'єктів.

Сценарій обслуговування призначений для користувачів, що мають певний досвід у діагностиці комп'ютерних систем. Некваліфіковане використання даного засобу може привести до непрацездатності операційної системи.

Приклад. При наявності підозр на зараження комп'ютера вірусом, який не визначається антивірусною програмою, можна виконати наступну покрокову процедуру.

- Завантажите **ESET Sysinspector** і створіть новий знімок стану комп'ютера.
- Клацніть перший елемент у розділі ліворуч (у деревоподібній структурі), натисніть клавішу **CTRL**, а потім виберіть останній об'єкт, щоб відзначити всі елементи в списку. Відпустіть клавішу **CTRL**.
- Клацніть виділені об'єкти правою кнопкою й виберіть команду контекстного меню **Экспортировать в сценарии обслуживания**.
- Обрані об'єкти будуть експортовані в новий журнал.
- Далі випливає найбільш важливий крок усієї процедури: відкрийте створений журнал і змініть атрибут «-» на «+» для всіх об'єктів, що підлягають видаленню. Переконайтеся , що не відзначені об'єкти, життєво важливі для роботи операційної системи.
- Відкрийте **ESET Sysinspector**, клацніть **Файл/ Загрузить в сценарии обслуживания** і введіть шлях до свого сценарію.
- Натисніть **OK**, щоб запустити сценарій.

Клавіші швидкого доступу

Нижче представлений список клавіш швидкого доступу, які можна використовувати при роботі із програмою ESET Sysinspector.

Файл	Опис
Ctrl+O	відкриває існуючий журнал
Ctrl+S	зберігає створені журнали

Створення	
Ctrl+G	стандартна перевірка стану системи
Ctrl+H	виконує перевірку системи, яка може занести в журнал важливу інформацію (ім'я поточного користувача, ім'я комп'ютера, назва домену, права доступу поточного користувача, змінні оточення й усі Ip-Адреси, перетворені в доменні імена), а також усі адреси, перетворені в доменні імена

Фільтрація елементів	
1, O	докладні відомості, відображаються елементи з рівнем ризику 1—9
2	докладні відомості, відображаються елементи з рівнем ризику 2—9
3	докладні відомості, відображаються елементи з рівнем ризику 3—9
4, U	невідомі елементи, відображаються елементи з рівнем ризику 4—9
5	невідомі елементи, відображаються елементи з рівнем ризику 5—9
6	невідомі елементи, відображаються елементи з рівнем ризику 6—9
7, B	небезпечні елементи, відображаються елементи з рівнем ризику 7—9
8	небезпечні елементи, відображаються елементи з рівнем ризику 8—9
9	небезпечні елементи, відображаються елементи з рівнем ризику 9
-	підвищує рівень ризику
+	знижує рівень ризику

Вистава	
Ctrl+3	відображає повні відомості
Ctrl+2	відображає відомості середнього ступеня подробиці
Ctrl+1	основний вид
Backspace	перехід на один крок назад
Пробіл	перехід на один крок уперед
Ctrl+W	розвертає дерево
Ctrl+Q	звертає дерево

Інші елементи керування	
Ctrl+T	перехід до вихідного місця розташування елемента після його виділення в результатах пошуку
Ctrl+P	відображає базові відомості про об'єкт
Ctrl+A	відображає повні відомості про об'єкт
Ctrl+C	копіює елементи
Ctrl+X	копіює дерево поточного елемента
Ctrl+B	пошук відомостей про обрані файли в Інтернеті
Ctrl+L	відкриває папку, у якій перебуває обраний файл
Ctrl+R	відкриває відповідний запис у редакторі реєстру
Ctrl+Z	копіює шлях до файлу (якщо елемент пов'язаний з файлом)
Ctrl+F	перехід у поле пошуку
Ctrl+D	закриває результати пошуку

Порівняння	
Ctrl+Alt+O	відкриває вихідний або порівняльний журнал
Ctrl+Alt+R	скасовує порівняння
Ctrl+Alt+1	відображає всі елементи
Ctrl+Alt+2	відображає тільки додані елементи (відображаються тільки елементи з поточного журналу)
Ctrl+Alt+3	відображає тільки вилучені елементи (відображаються тільки елементи з попередньої версії журналу)
Ctrl+Alt+4	відображає тільки замінені елементи (включаючи файли)
Ctrl+Alt+5	відображає тільки відмінності між журналами
Ctrl+Alt+C	відображає результати порівняння
Ctrl+Alt+N	відображає поточний журнал
Ctrl+Alt+P	відображає попередню версію журналу

Різне	
F1	викликає довідку
Alt+F4	закриває програму
ALT+SHIFT+F4	закриває програму без висновку запиту

2. Хід роботи

1. Увести ім'я користувача й пароль
2. Налагодити відновлення
3. Налагодити параметри сканування комп'ютера
4. Провести сканування комп'ютера в різних припустимих режимах
5. Перевірити недавно створені й змінені файли
6. Перевірити захист електронної пошти

7. Провести вибіркове сканування електронної пошти
8. Створити профілі сканування
9. Перевірити різні режими фільтрації
10. Створити нові правила сканування
11. Перевірити журнал і його налагодження

3. Контрольні питання

1. Установка програми
2. Уведення імені користувача й пароля
3. Налагодження відновлень
4. Типи сканування комп'ютера
5. Налагодження довіреної зони
6. Налагодження прокси-сервера
7. Сканування носіїв
8. Перевірка недавно створених і змінених файлів
9. Поведінка модуля захисту від вірусів і втручання користувача
10. Рівні очищення
11. Термін зміни параметрів захисту в режимі реального часу
12. Вирішення проблем, що виникають при роботі модуля захисту в режимі реального часу
13. Захист електронної пошти
14. Видалення заражень
15. Керування адресами
16. Інтелектуальне сканування
17. Вибіркове сканування
18. Профілі сканування
19. Керування профілями
20. Режими фільтрації
21. Створення нових правил
22. Аутентифікація зон: конфігурація клієнта
23. Аутентифікація зон: конфігурація сервера
24. Установка з'єднання — виявлення
25. Ведення журналу
26. Боротьба зі спамом
27. Приміщення файлів на карантин
28. Обслуговування журналу
29. Сценарій обслуговування

Лабораторна робота 28
Ознайомлення з програмою захисту від вірусів Symantec AntiVirus

Мета роботи – Засвоїти принципи й елементи технології захисту інформації від вірусів та інших шкідливих програм. Ознайомитись з рівнями захисту комп'ютера, можливістю використання налагоджень та можливостей програми.

План

1. Теорія

1.1 Загальні відомості про програму Symantec AntiVirus

Систему захисту від вірусів і погроз безпеці Symantec AntiVirus™ можна встановити як в автономній конфігурації, так і в конфігурації, якою управляє адміністратор. У автономній конфігурації мережевий адміністратор не управляє програмним забезпеченням Symantec AntiVirus.

Якщо ви управляєте власним комп'ютером, це повинен бути комп'ютер один з наступних типів:

- автономний комп'ютер, не підключений до мережі, такий як домашній або портативний комп'ютер. Symantec AntiVirus повинен застосовувати параметри за умовчанням або зумовлені параметри, задані адміністратором.
- віддалений комп'ютер, який повинен задовольняти вимогам до безпеки для підключення до корпоративної мережі.

Задані за умовчанням параметри Symantec AntiVirus забезпечують достатній захист комп'ютера від вірусів і погроз безпеці. Проте ви можете змінити деякі параметри з урахуванням вимог своєї організації для підвищення продуктивності системи або відключення непотрібних параметрів.

Якщо конфігурацією управляє адміністратор, деякі параметри можуть бути заблоковані або недоступні, залежно від заданої адміністратором політики безпеки. Адміністратор може запускати процедури огляду вашого комп'ютера уручну або за розкладом.

Адміністратор повинен повідомити вас, які завдання потрібно буде виконувати за допомогою Symantec AntiVirus.

Автономні комп'ютери можуть бути підключені до Інтернету. Автономними комп'ютерами є комп'ютери, не підключені до сервера. Через це вони не отримують оновлення описів вірусів і погроз безпеці з сервера, і ними не можна управляти за допомогою програми Symantec System Center.

Якщо Symantec AntiVirus встановлений на автономному комп'ютері, відповідальність за оновлення файлів описів вірусів і погроз покладається на користувача. Нові файли описів поставляються фірмою виготовлювачем Symantec кілька разів в місяць. Коли виникає необхідність замінити файли описів, користувачам відправляється попередження.

Файли описів вірусів і погроз можна відновити за допомогою LiveUpdate™. Функція LiveUpdate автоматично знаходить нові файли описів на вузлі компанії Symantec, а потім замінює ними старі файли, що зберігаються в каталозі Symantec AntiVirus. Для цього потрібний модем або пряме підключення до Інтернету.

Віддалені комп'ютери, підключені до корпоративної мережі, можуть отримувати оновлення файлів описів вірусів і погроз. Для управління ними можна використовувати програму Symantec System Center.

На комп'ютери, що підключаються до корпоративної мережі|сіті|, можуть накладатися певні вимоги до захисту. Наприклад, для підключення до мережі|сіті| може потрібно завантажити найостанніші описи вірусів і погроз Symantec AntiVirus. Якщо ці вимоги не будуть виконані, доступ до мережі|сіті| для цього комп'ютера буде заборонений.

1.2 Відомості про погрози безпеки

Symantec AntiVirus виявляє, ізолює і усуває побічні ефекти погроз безпеці наступних категорій:

- Програми-шпигуни: Автономні програми, що відстежують операції системи, паролі, що вводяться, і іншу конфіденційну інформацію, яка потім відправляється на інший комп'ютер.

Користувачі можуть за незнанням завантажити програми-шпигуни з веб-вузлів (зазвичай у вигляді безкоштовних або умовно безкоштовних програм), у складі повідомлень електронної пошти і миттєвих повідомлень. Часто користувачі випадково завантажують програми-шпигуни, приймаючи ліцензійні угоди для інших програм.

- Реклама: Окремі або доповнюючі програми, які таємно збирають через Інтернет інформацію про користувача і відправляють її на інший комп'ютер. Такі

програми можуть відстежувати звички користувача при роботі в мережі Інтернет в цілях вибору найбільш відповідної реклами. Крім того, вони використовуються для розсилки реклами.

Користувачі можуть за незнанням завантажити програми показу реклами з веб-вузлів (зазвичай у вигляді безкоштовних або умовно безкоштовних програм), у складі повідомлень електронної пошти і миттєвих повідомлень. Часто користувачі випадково завантажують рекламні програми, приймаючи ліцензійні угоди для інших програм.

- Програми набору номера: Програми, які без дозволу користувача встановлюють через Інтернет телефонні з'єднання з номерами серії 900- або вузлами FTP для збору грошей.
- Засоби злому: Програми, вживані хакерами для діставання несанкціонованого доступу до комп'ютера користувача. Наприклад, одним із засобів злому є програма відстежування натиснень клавіш, яка реєструє окремі натиснення клавіш і відправляє цю інформацію хакерові. Потім хакер з її допомогою може виконати огляд портів або вторгнутися на комп'ютер іншим способом. Крім того, за допомогою засобів злому можна створювати віруси.
- Програми-жарти: Програми, які змінюють або переривають роботу комп'ютера способом, який їх творець визнав смішним або, навпаки, таким, що лякає. Наприклад, такі програми можна завантажити з веб-вузлів (зазвичай у вигляді безкоштовних або умовно безкоштовних програм), у складі повідомлень електронної пошти і миттєвих повідомлень. Після цього, наприклад, сміттєва корзина може почати «тікати» від користувача або дія кнопок миші поміняється на протилежну.
- Інші погрози: Погрози, що не відносяться ні до однієї з перерахованих вище категорій, але що потенційно представляють небезпеку для комп'ютера і його даних.
- Віддалений доступ: Програми, які дозволяють дістати доступ до комп'ютера ззовні за мережею Інтернет для збору інформації, атаки на комп'ютер користувача або внесення до нього змін. Наприклад, така програма може бути встановлена користувачем, або автоматично встановлена в прихованій формі іншим процесом. Програма може завдавати шкоди, зокрема, змінюючи початкову програму видаленого доступу.
- Стежачи програми: Автономні або додані застосування, що відстежують дії користувача в мережі Інтернет і що відправляють цю інформацію в цільову систему. Наприклад, такі застосування можуть бути завантажені з веб-вузла, з поштового або миттєвого повідомлення. Потім вони збирають конфіденційну інформацію про поведінку користувача.

За умовчанням всі типи операцій огляду Symantec AntiVirus, зокрема огляди, в рамках автоматичного захисту перевіряють комп'ютер на наявність вірусів, троянських коней, черв'яків і погроз безпеці всіх категорій.

1.3 Яким чином Symantec AntiVirus реагує на виявлення вірусів і погроз безпеці

Symantec AntiVirus захищає комп'ютер від вірусів і погроз безпеки, що поступають будь-яких джерел. До числа таких джерел входять жорсткі диски, дискети, а також мережі. Забезпечується захист комп'ютерів від вірусів і інших погроз, що розповсюджуються за допомогою вкладень електронної пошти і деякими іншими способами. Наприклад, загроза безпеці може бути встановлена на комп'ютері без вашого відома під час роботи в мережі Інтернет.

Всі файли, розташовані усередині стислих файлів, оглядаються і, при необхідності, виправляються. Для виявлення вірусів, що розповсюджуються за мережею Інтернет, не

потрібно змінювати ніяких параметрів і програм. Функція автоматичного захисту оглядає всі нестислі файли програм і документів під час їх завантаження.

При виявленні вірусу або загрози у файлі Symantec AntiVirus виконує першу і другу дії.

У разі виявлення вірусу Symantec AntiVirus за умовчанням намагається видалити його з файлу і усунути його побічні ефекти. Файл вважається виправленим, якщо з нього вдається повністю видалити вірус. Якщо за якими-небудь причинами Symantec AntiVirus не вдалося видалити вірус, то Symantec AntiVirus виконує другу дію, тобто переміщає заражений файл в Ізолятор, щоб запобігти розповсюдженню вірусу.

При оновленні захисту від вірусів Symantec AntiVirus автоматично перевіряє наявність файлів в Ізоляторі і пропонує оглянути їх з урахуванням нової інформації.

Примітка: Адміністратор може включити автоматичний огляд файлів в Ізоляторі.

При виявленні загрози безпеці Symantec AntiVirus за умовчанням ізолює заражені файли і відновлює системну інформацію, яка була змінена загрозою. Деякі погрози безпеці не можна видалити повністю, оскільки це може привести до збою іншої програми, наприклад веб-сервер-оглядач. Якщо програма Symantec AntiVirus не настроєна для автоматичної обробки погроз, вона попереджає користувача перед завершенням процесу і перезапуском комп'ютера. Крім того, Symantec AntiVirus можна налагодити так, щоб при виявленні погроз інформація про них заносилася в журнал, а інші дії не виконувалися.

Крім того, при цьому може відправлятися повідомлення, адміністратором.

1.4 Що робить Symantec AntiVirus для захисту комп'ютера

Зараження вірусом можна уникнути. Вчасно виявлені і видалені з комп'ютера віруси не зможуть розповсюдитися за файлами і завдати значного збитку. Всі побічні ефекти від наявності вірусів і погроз безпеці можна усунути. При виявленні вірусу або загрози безпеці Symantec AntiVirus за умовчанням попереджає користувача про зараження одного або декількох файлів. Якщо ви не хочете отримувати такі попередження, налагодьте Symantec AntiVirus для автоматичної обробки погроз.

Symantec AntiVirus забезпечує захист наступних типів:

- Автоматичний захист: Постійно відстежує роботу комп'ютера шляхом огляду всіх файлів при їх відкритті, запуску, внесенні змін, збереженні, переміщенні і копіюванні.
- Пошук сигнатур атак: Виконує пошук сигнатур вірусів в заражених файлах, а також сигнатур погроз безпеці в заражених файлах і системній інформації. Такий пошук називається оглядом. Залежно від конфігурації, користувачі і адміністратори можуть запускати огляди для систематичної перевірки файлів комп'ютера на наявність вірусів і погроз безпеці, таких як рекламні і шпигунські програми, з використанням сигнатур і шаблонів. Огляди можуть виконуватися на вимогу, автоматично за розкладом або при запуску системи.
- Додаткова евристика: Аналізує структуру програми, її поведінку і інші атрибути, порівнюючи їх з характеристиками вірусів. У багатьох випадках це дозволяє забезпечити захист від погроз (таких як поштові черв'яки і макровіруси) ще до створення опису загрози і оновлення програми. Додаткова евристика дозволяє розпізнати загрозу з боку сценаріїв у файлах HTML, VBScript і JavaScript.

1.5 Відкриття вікна програми Symantec AntiVirus

Виконаєте одну з наступних дій:

- Двічі клацніть на значку **Symantec AntiVirus** на панелі задач Windows, або використайте праву клавішу миші (рис. 1).

Наявність цього значка на панелі завдань залежить від параметрів, настроєних адміністратором.

- На панелі завдань Windows або Windows XP виберіть **Пуск / Программы(Symantec Client Security Symantec AntiVirus** (рис. 2), або **Пуск Дополнительные программы/ Symantec Client Security / Symantec AntiVirus.**

Головне вікно Symantec AntiVirus містить дві панелі (рис. 3). У лівій панелі доступні дії об'єднані в категорії. Наприклад, завдання огляду дискет, вибіркового огляду, швидкого огляду і повного огляду відносяться до категорії Огляд. Кожна категорія в лівій панелі показана у вигляді окремого значка. При виборі в лівій панелі категорій і інших елементів в правій панелі буде показана інформація, необхідна для виконання відповідного завдання.

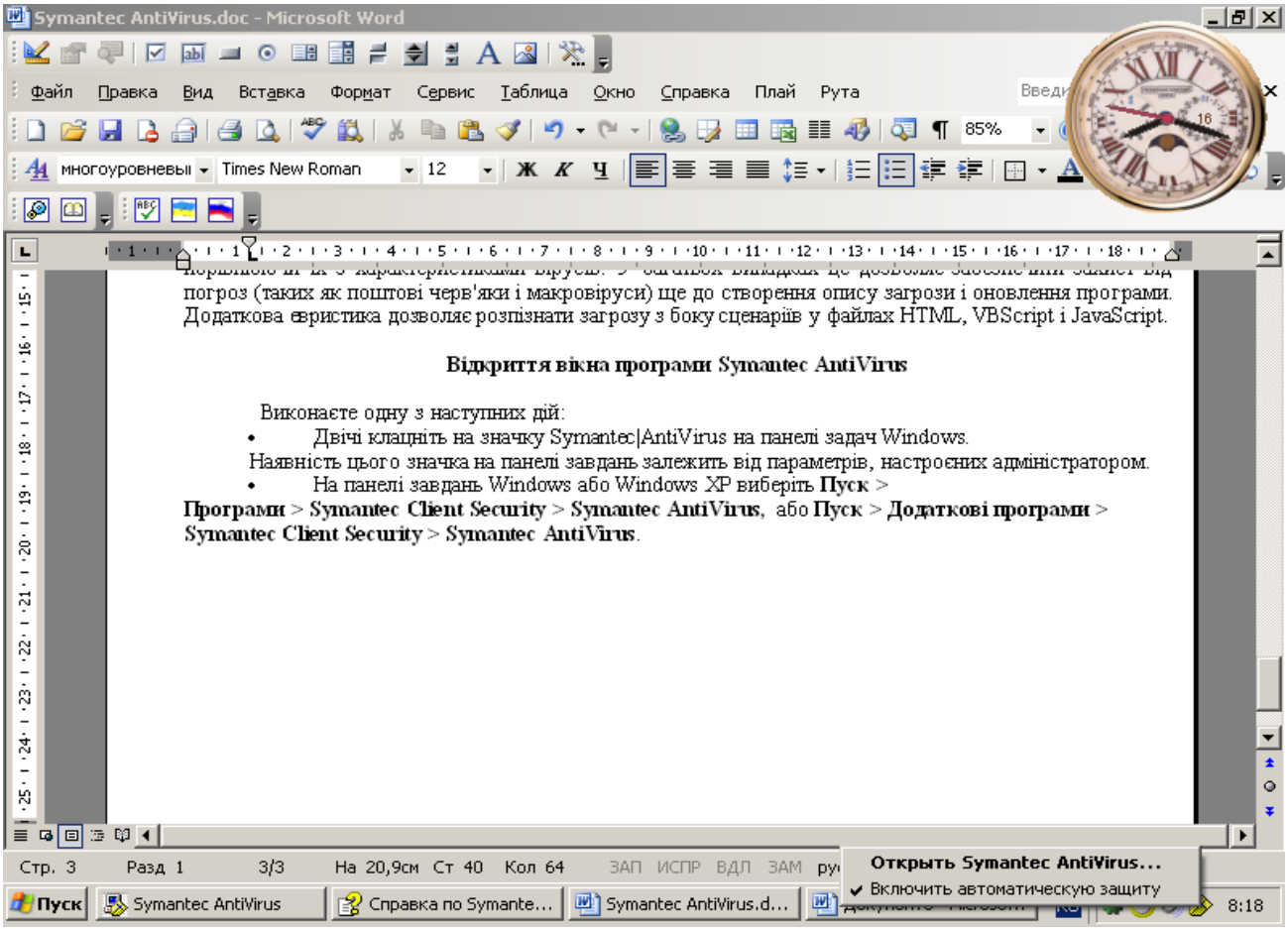


Рис.1 Вікно запуску програми

1.6 Категорія Перегляд

Категорія **Перегляд** призначена для відстежування дій із захисту від вірусів і інших погроз безпеці.

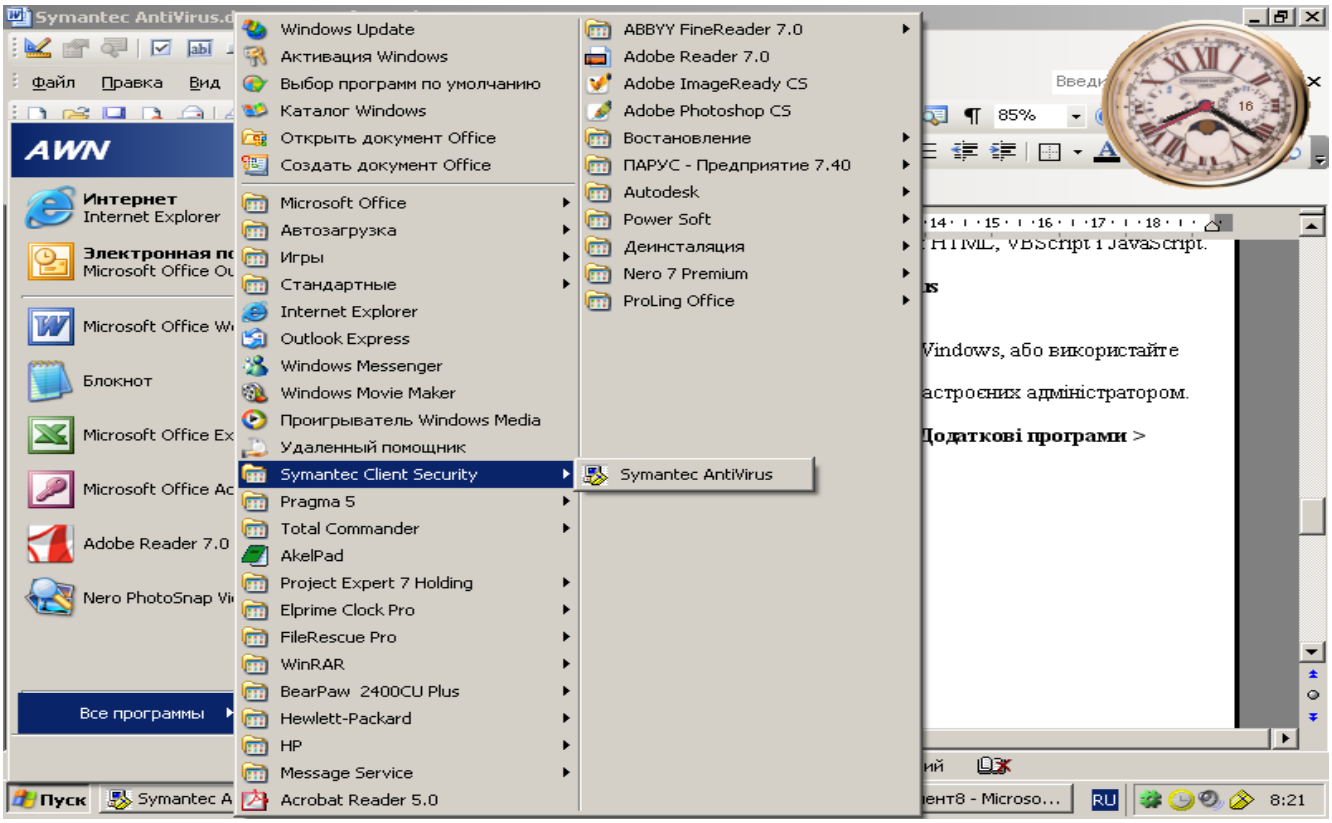


Рис. 2 Вікно запуску програми

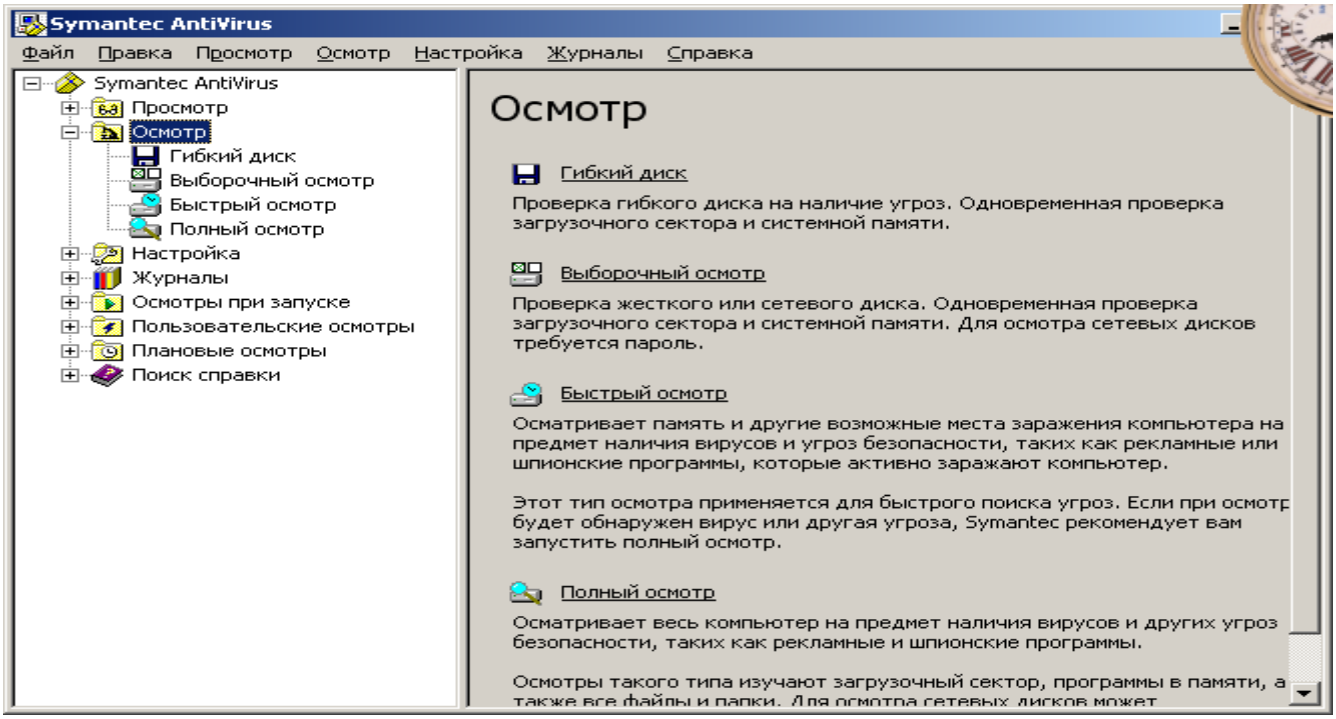


Рис. 3 Вікно програми

Таблиця 1

Опис категорії перегляд

Параметр	Опис
Статистика огляду в рамках автоматичного захисту	Показує статистику автоматичного захисту файлової системи, включаючи останній перевірений файл (навіть якщо він не був заражений
Планові огляди	Показує список всіх планових оглядів, що запускаються в системі, включаючи ім'я кожного огляду, час його запуску і ім'я користувача, що створив огляд. Плановий огляд може бути створений користувачем або адміністратором.
Ізолятор	Робота із зараженими файлами, ізольованими для запобігання розповсюдженню вірусів або побічних дій погроз безпеці.
Копії заражених файлів	Дозволяє видалити збережені копії заражених файлів. Як запобіжний засіб Symantec AntiVirus створює резервну копію заражених об'єктів перед спробою їх виправлення. Переконавшись, що Symantec AntiVirus виправив заражений файл, слід видалити резервну копію цього файлу. Symantec AntiVirus створює копію файлів, що містять погрози безпеці, при їх приміщенні в ізолятор. Крім того, він зберігає копії параметрів реєстру і системних точок завантаження, що містять погрози безпеці, такі як програми-шпигуни і програми показу реклами. Системні крапки завантаження - це найуразливіші фрагменти програмного забезпечення. Примітка: В деяких випадках видалення загрози безпеці може привести до того, що перестануть працювати деякі функції додатків. Перед видаленням файлу із загрозою безпеці переконаєтеся в тому, що він не потрібний для роботи додатків
Виправлені файли	. Виправлені файли, початкове розташування яких (таке як мережевий диск) більше не доступно. Наприклад, в Ізолятор могло бути поміщено вирізане з повідомлення електронної пошти заражене вкладення. Після того, як об'єкт виправлений в Ізоляторі і поміщений в теку «Виправлені файли», його слід перемістити

	в той каталог, в якому він повинен знаходитися доступний тільки у разі застосування ліцензій на вміст..
Ліцензія	Не відображається в меню, якщо застосовується корпоративна ліцензія Показує інформацію про поточну ліцензію. Інформація про поточну ліцензію включає стан ліцензії, серійний номер, а також початкову і кінцеву дати. При необхідності можна викликати Майстер установки ліцензій

1.7 Переглядання файлів і відомостей про них в Ізоляторі

1. У меню «Вид» програми Symantec AntiVirus виберіть команду Ізолятор.
2. Клацніть на потрібному файлі правою кнопкою миші і виберіть команду Властивості.

Як повторно оглянути ізольовані файли за допомогою Майстра лікування

1. Якщо був запущений Майстер лікування, натисніть кнопку Так.
2. Натисніть кнопку Далі і виконуйте вказівки, що з'являються на екрані, для повторного огляду вмісту Ізолятора.

1.8 Очистка уручну теки Копії заражених файлів

1. На лівій панелі вікна Symantec AntiVirus виберіть **Вид**.
2. На правій панелі виберіть **Копии зараженых файлов**.
3. Виберіть один або декілька файлів в списку **Копии зараженых файлов**.
4. Виконаєте одну з наступних дій:
   - Клацніть на файлі правою кнопкою миші і виберіть команду **Удалить**.
   - На правій панелі виберіть **Удалить**.
5. У вікні дії виберіть **Удалить**.

1.9 Налагодження автоматичного видалення файлів

1. На лівій панелі вікна Symantec AntiVirus виберіть **Вид**.
2. На правій панелі виберіть один з наступних елементів:
   - Ізолятор
   - Копії заражених файлів
   - Виправлені файли
3. Клацніть на значку **Очистить**, розташованому на правому кінці панелі інструментів.
4. У вікні **Параметры очистки** виберіть **Включить автоматическую очистку**.
5. У полі **Выполнять очистку** введіть число або виберіть його за допомогою кнопок із стрілками.

1.11 Вибір типів файлів для огляду

1. На лівій панелі Symantec AntiVirus виберіть огляд, який необхідно змінити.
   - Якщо огляд був вибраний в категорії **Осмотр** (рис. 4), то натисніть **Параметры** (рис. 5).

- Якщо був вибраний огляд при запуску, плановий або призначений для користувача огляд, то виберіть конкретний огляд, натисніть **Изменить**, а потім натисніть **Параметры**.

Зміни будуть застосовані тільки для вибраного огляду.

.

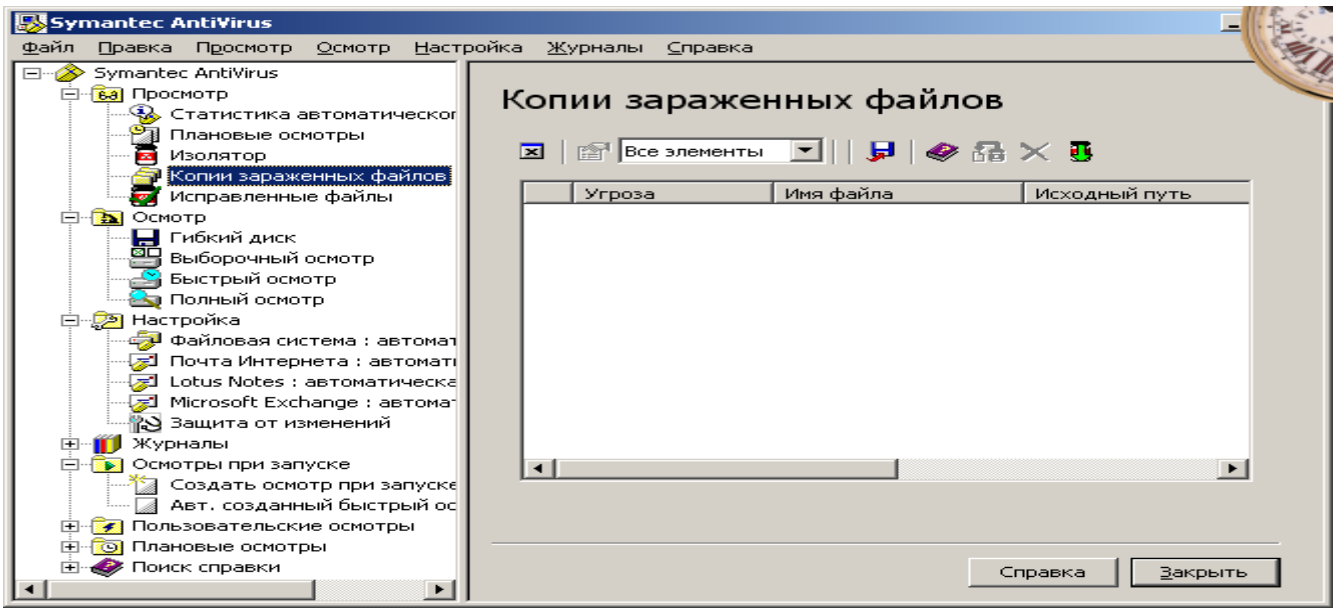


Рис. 4 Вікно наявності заражених файлів

6. Задайте інтервал часу.
7. Натисніть кнопку **ОК**.

1.10 Категорія Огляд

Категорія Огляд дозволяє виконати огляд системи уручну.

Таблиця 2

Категорія Огляд

Параметр	Опис
Гнучкий диск	Огляд дискет і інших змінних носіїв.
Швидкий огляд .	Дуже швидкий огляд оперативної пам'яті системи і всіх розташувань, які найбільш схильні до зараження.
Вибірковий огляд	Огляд файлу, теки, диска або всього комп'ютера, який можна виконати уручну у будь-який час..
Повний огляд	Огляд всієї системи, зокрема завантажувального сектора і оперативної пам'яті. Для огляду мережевих дисків інколи потрібно ввести пароль

2. Відзначте пункт **Избранные типы файлов** і натисніть кнопку **Типы**.
3. Виберіть будь-які з наступних типів файлів:

- Файли документів: Документи Word і Excel, а також файли шаблонів, пов'язаних з цими документами.
- Програмні файли: Включають динамічно компоновані бібліотеки (.dll), командні файли (.com), виконувані файли (.exe) і інші програмні файли.

4. Якщо настроєні дії повинні застосовуватися у всіх подальших оглядах, натисніть кнопку **Сохранить настройки**.
5. Натисніть кнопку **ОК**.

Як додати розширення в список для огляду

1. На лівій панелі Symantec AntiVirus виберіть огляд, який необхідно змінити.

- Якщо огляд був вибраний в категорії **Осмотр**, то натисніть **Параметры**.
- Якщо вибраний огляд при запуску, плановий або призначений для користувача огляд, то виберіть ім'я огляду, підмета зміні, натисніть кнопку **Изменить**, а потім натисніть кнопку **Параметры**.

Зміни будуть застосовані тільки для вибраного огляду.

- Якщо був вибраний автоматичний захист, перейдіть до кроку 2.

2. Відзначте пункт **Избранные расширения файлов** і натисніть кнопку **Расширения** (рис. 6).

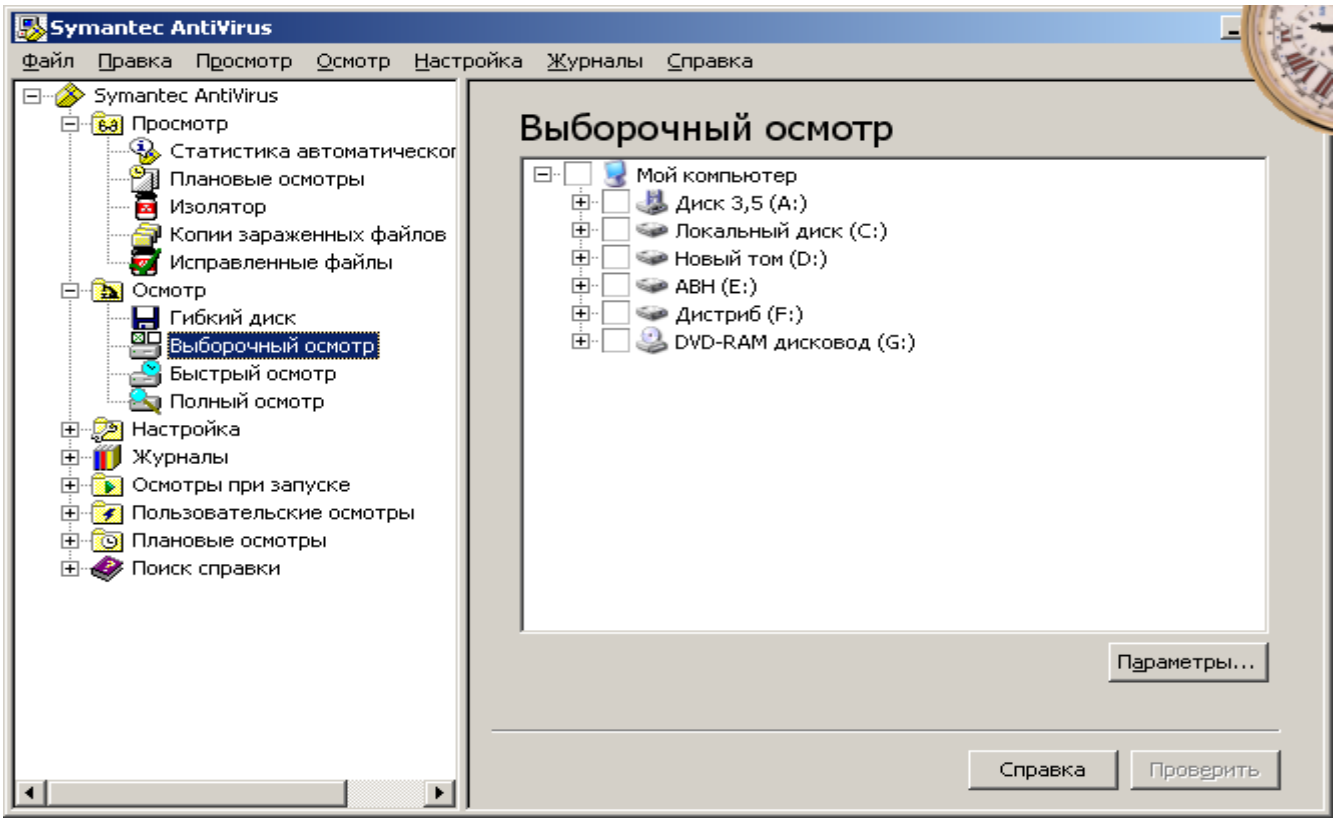


Рис. 4 Вікно огляду

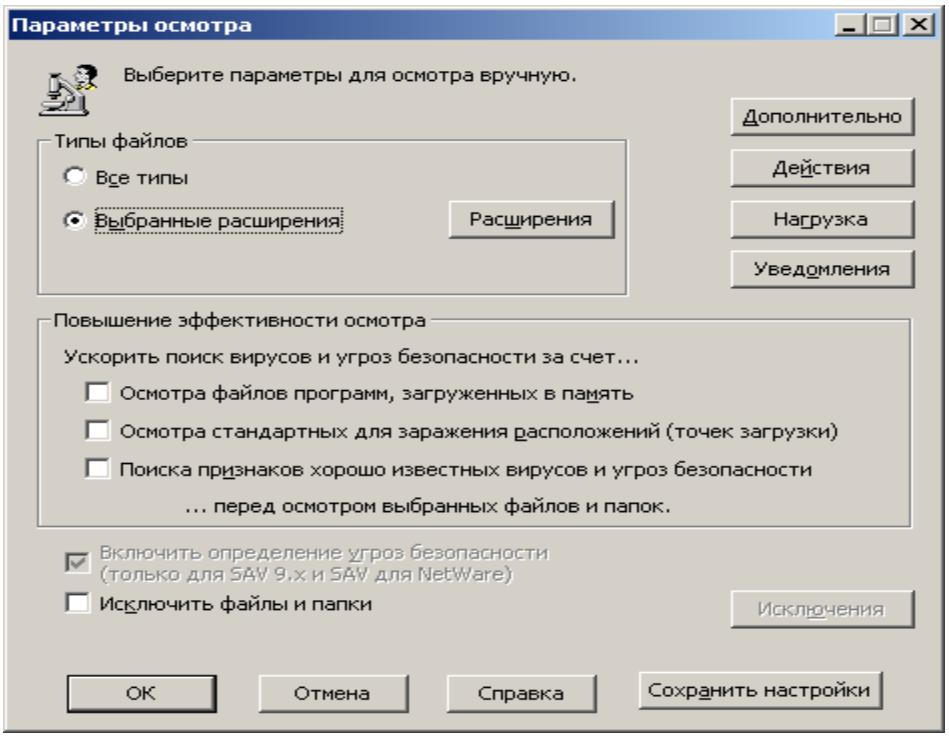


Рис. 5 Вікно параметрів

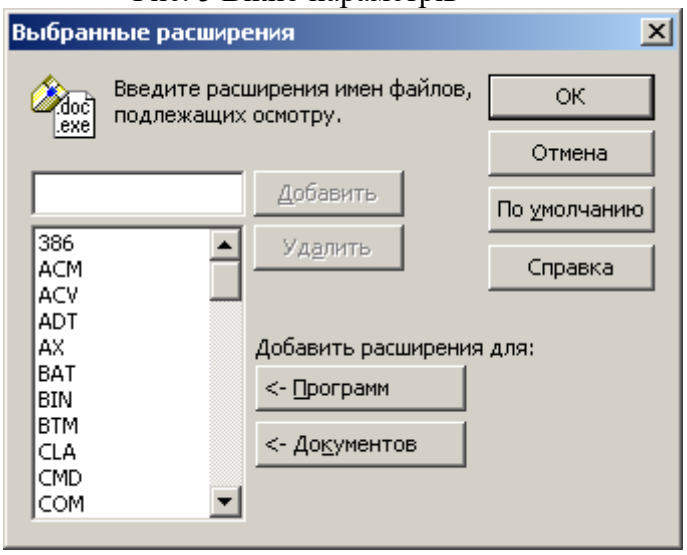


Рис. 6 Вікно вибору файлів за розширеннями

3. Введіть розширення, яке необхідно додати, і натисніть кнопку **Добавить**.
4. Повторіть крок 3 необхідне число разів.
5. Натисніть кнопку **ОК**.

1.12 Запуск огляду уручну в Symantec AntiVirus

1. На лівій панелі вікна Symantec AntiVirus виберіть **Осмотр**.
2. На лівій панелі виберіть один з наступних елементів:
   - Гнучкий диск

   Цей варіант доступний тільки за наявності дисковода.
   - Вибірковий огляд
   - Швидкий огляд
   - Повний огляд

3. Якщо був вибраний огляд гнучкого диска або вибірковий огляд, то виконайте наступні дії на правій панелі:

- Двічі клацніть на пристрої або теці, щоб відкрити або закрити її.
- Виберіть диски, що підлягають огляду.

4. Якщо був вибраний огляд уручну, натисніть кнопку **Параметры** і вкажіть, які об'єкти повинні оглядатися і які дії повинні виконуватися при виявленні вірусу або загрози безпеці.

За умовчанням задані наступні параметри:

- Оглядаються всі файли.
- При виявленні вірусу за умовчанням робиться спроба видалити вірус із зараженого файлу і усунути його побічні ефекти. Якщо це не вдається зробити, то заражений файл ізолюється.
- При виявленні загрози за умовчанням загроза ізолюється, а її побічні ефекти усуваються. Якщо це не вдається зробити, то інформація про загрозу заноситься в журнал.

Для того, щоб застосувати змінені параметри тільки до поточного огляду, натисніть OK. Для того, щоб задані параметри діяли для всіх подальших оглядів, натисніть кнопку Зберегти налагодження.

5. Натисніть кнопку **Дополнительно**, щоб задати параметри відображення вікна стану огляду під час планового огляду.

6. У вікні **Дополнительные параметры осмотра** знайдіть розділ параметрів вікна діалогу, виберіть у випадному списку пункт **Показать состояние осмотра** і натисніть кнопку **OK**.

7. У вікні параметрів огляду натисніть кнопку **OK**.

8. У головному вікні Symantec AntiVirus виберіть **Осмотр**.

Symantec AntiVirus запустить огляд і покаже його результати (рис. 7).

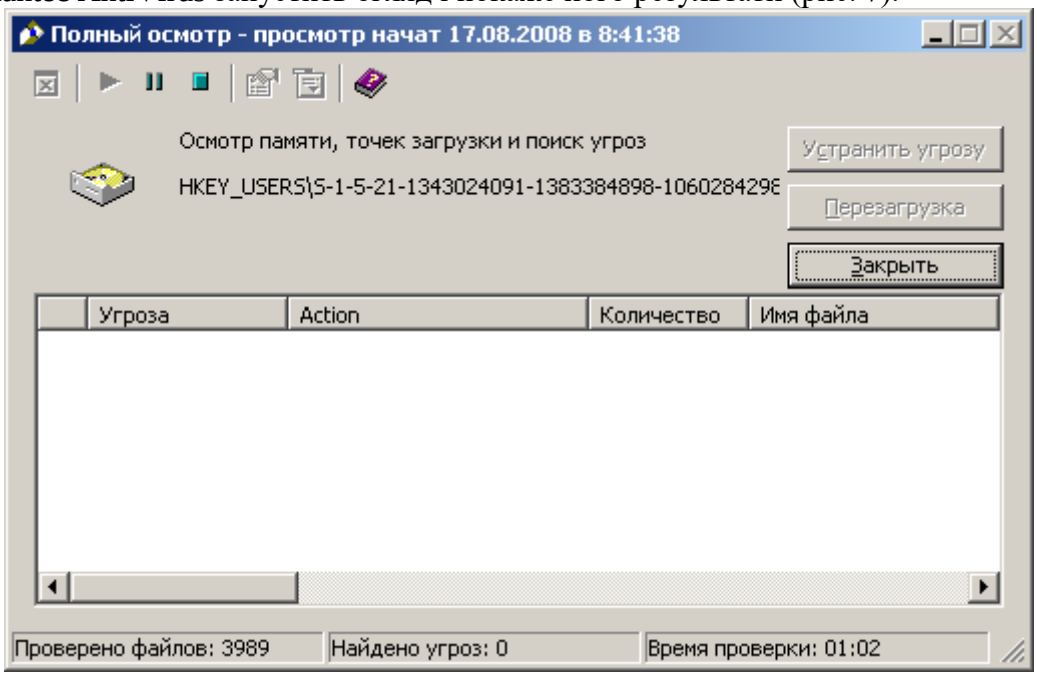


Рис. 7 Вікно огляду

1.13 Категорія Налагодження

За допомогою категорії Налагодження можна налагодити функцію автоматичного захисту для перевірки файлів і вкладень електронної пошти (у підтримуваних поштових

клієнтах), а також налагодити захист від змін, для того, щоб запобігти зміні додатків Symantec.

Таблиця 3

Опис категорії налагодження

Параметр	Опис
Автоматичний захист файлової системи	Файли перевіряються на наявність вірусів і погроз безпеці при кожному копіюванні, переміщенні, відкритті і зверненні до них. До складу автоматичного захисту входить функція SmartScan, що дозволяє визначити тип файлу навіть в тому випадку, якщо розширення файлу змінене вірусом
Автоматичний захист пошти Інтернета, Lotus Notes®, Microsoft® Exchange .	. Symantec AntiVirus забезпечує додатковий захист для клієнтів електронної пошти робочих груп (Lotus Notes і Microsoft Exchange/Microsoft Outlook®) . У клієнтах пошти Інтернету Symantec AntiVirus забезпечує захист вхідних і витікаючих поштових повідомлень, що застосовують протокол POP3 або SMTP.
Захист від змін	Захист від змін запобігає несанкціонованій зміні додатків Symantec.

1.14 Створення огляду при запуску

1. На лівій панелі вікна Symantec AntiVirus виберіть **Осмотры при запуске** (рис. 8)
2. На правій панелі виберіть **Создать осмотры при запуске** (рис. 9)
3. Виберіть один з наступних типів оглядів:
    - Швидкий огляд
    - Повний огляд
    - Вибірковий огляд
4. Натисніть кнопку **Далее** (рис. 10).
5. Введіть ім'я і опис огляду.
6. Натисніть кнопку **Далее**.
7. У разі вибіркового огляду відзначте на правій панелі ті елементи, в яких повинен виконуватися огляд. Ви можете виконати огляд як всього комп'ютера, так і окремого файлу.
8. Виберіть **Параметры** (рис.11) для зміни параметрів огляду за умовчання.

За умовчанням задані наступні параметри:

- Оглядаються всі файли.
- При виявленні вірусу за умовчанням робиться спроба видалити вірус із зараженого файлу і усунути його побічні ефекти. Якщо це не вдається зробити, то заражений файл ізолюється.
- При виявленні загрози за умовчанням загроза ізолюється, а її побічні ефекти усуваються. Якщо це не вдається зробити, то інформацію про загрозу заноситься в журнал.

Для того, щоб застосувати змінені параметри тільки до поточного огляду, натисніть **OK**. Для того, щоб задані параметри діяли для всіх подальших оглядів, натисніть кнопку **Сохранить настройку**.

9. Натисніть кнопку **Дополнительно**, щоб задати параметри відображення вікна стану огляду під час огляду при запуску.
10. У вікні **Дополнительные параметры осмотра** знайдіть розділ параметрів вікна діалогу, виберіть у випадному списку пункт **Показатьсостояние осмотра** і натисніть кнопку **OK**.

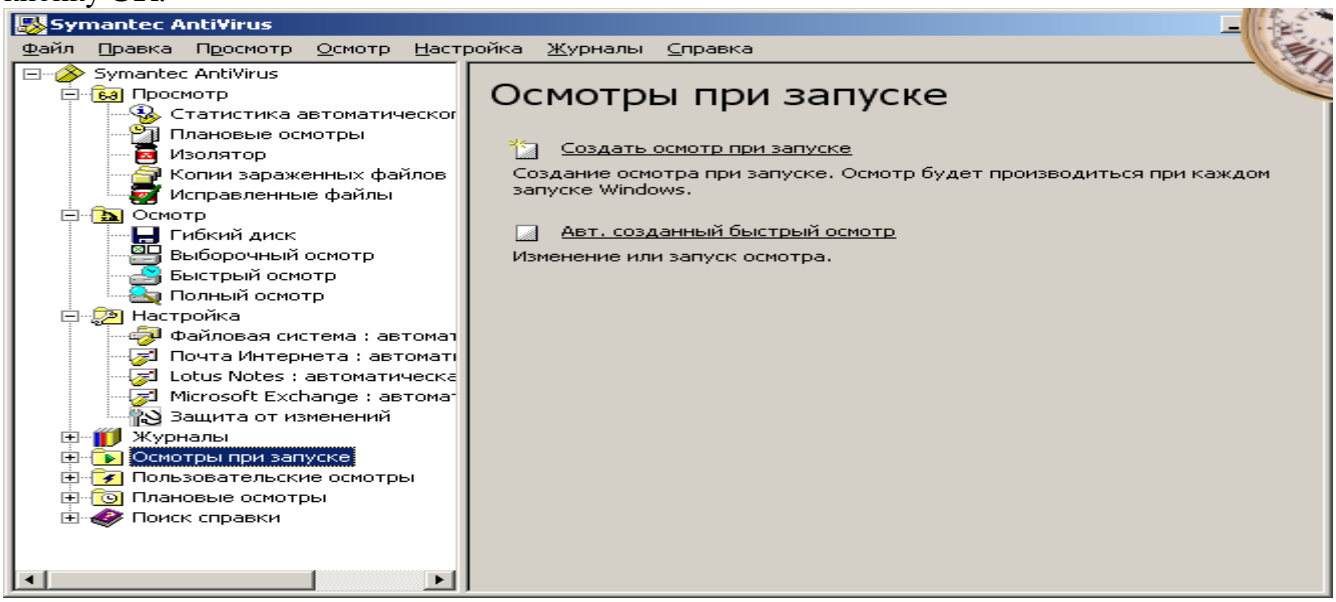


Рис. 8 Вікно відбору параметру Огляди при запуску

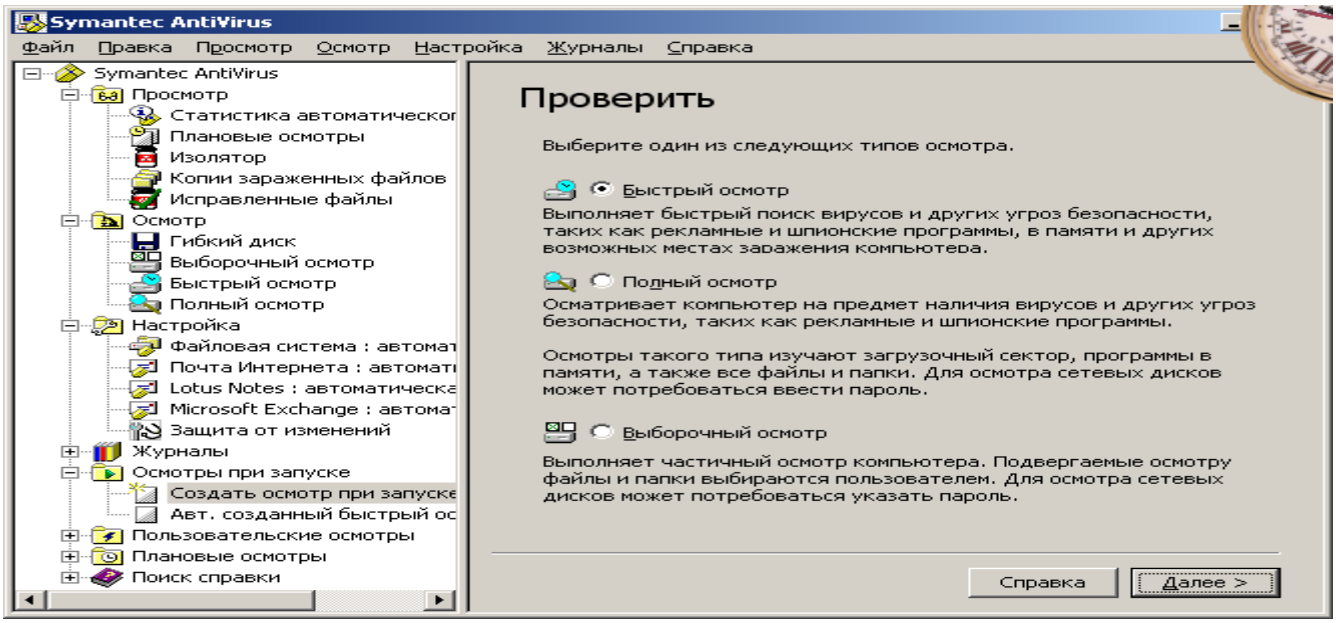


Рис. 9 Відбір типу огляду

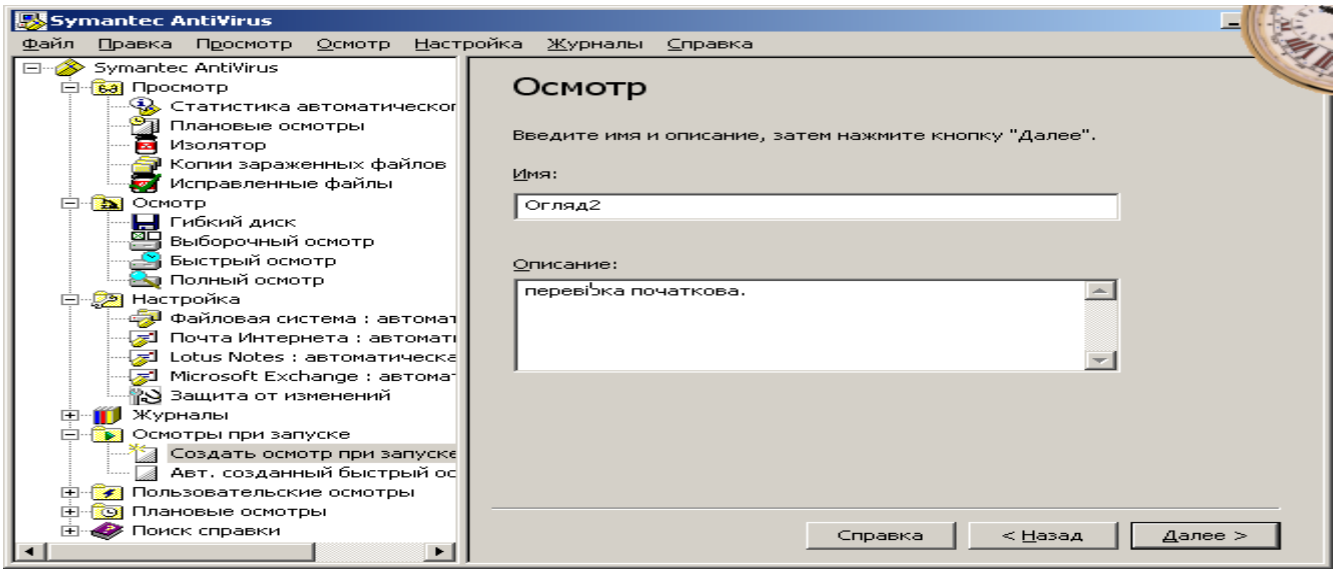


Рис. 10 Вікно назви огляду

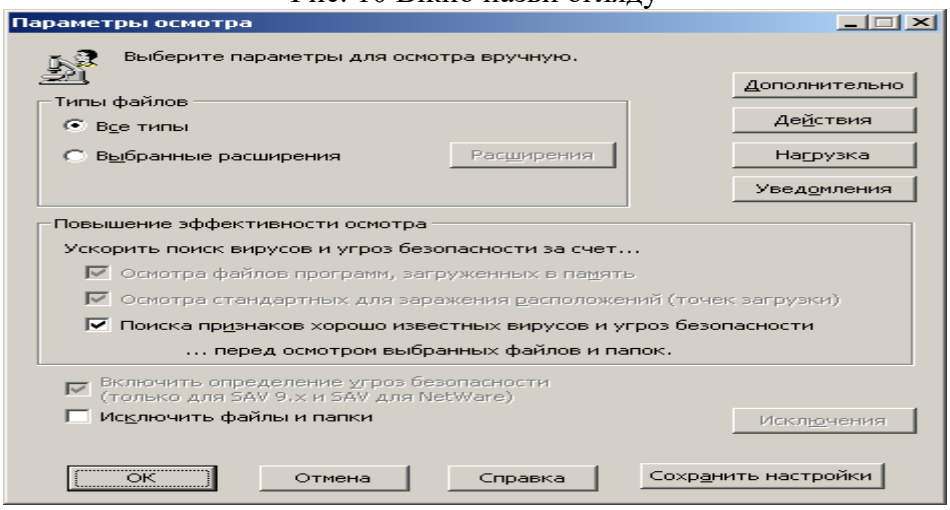


Рис. 11 Вікно параметрів

11. У вікні параметрів огляду натисніть кнопку **OK**.
12. У головному вікні Symantec AntiVirus натисніть кнопку **Сохранить**.

Огляд запускатиметься при кожному завантаженні Windows.

1.15 Як включити або вимкнути огляд на наявність погроз в налагодженнях автоматичного захисту?

1. На лівій панелі вікна Symantec AntiVirus виберіть **Настройка**
2. На правій панелі виберіть **Автоматическая защита файловой системи** (рис. 12).
3. У розділі параметрів виберіть або відміните вибір пункту **Включить автомати ческую защиту.**
4. Натисніть кнопку **ОК**.

1.16 Налагодження захисту від змін

1. На лівій панелі вікна Symantec AntiVirus виберіть **Защита от изменений**.
2. На правій панелі виберіть або відміните вибір пункту **Включить защиту от изменений** (рис. 13).
3. Після включення захисту від змін перейдіть до розділу **Защита** і виберіть один з наступних варіантів у випадному списку:

- Для того, щоб несанкціоновані дії блокувалися, виберіть значення **Блокировать**.
- Для того, щоб несанкціоновані операції реєструвалися в журналі, але не блокувалися, виберіть значення **Только заносить в журнал**.

4. Виберіть або відміните вибір пункту **Не отключать защиту от изменений** при завершенні роботи Symantec AntiVirus.
5. У розділі **Сообщения** виберіть або відміните вибір пункту **Показывать сообщения на атакованом компьютере**.
6. Натисніть кнопку **ОК**.

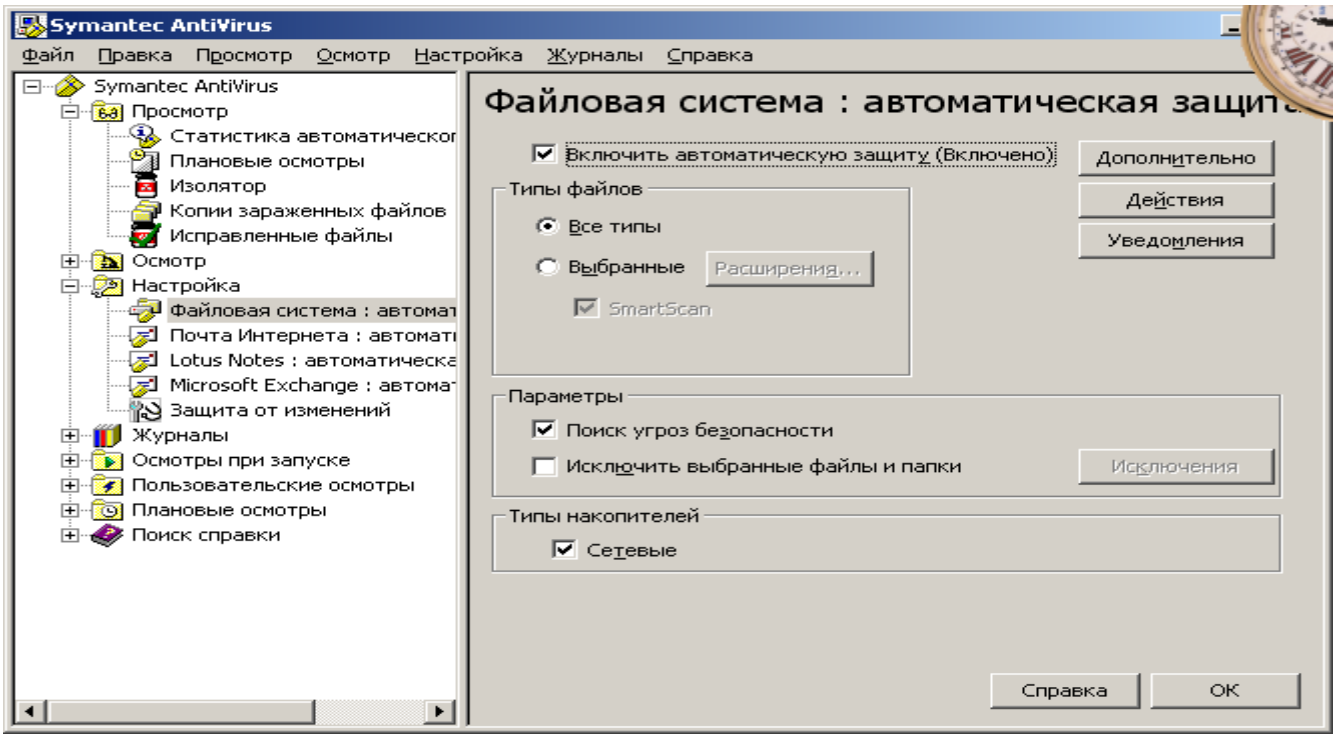


Рис. 12 Вікно автоматичного захисту

1.17 Налагодження повідомлень про віруси і погрози безпеці

При виявленні вірусу або загрози в ході огляду Symantec AntiVirus за умовчанням повідомляє про це користувача. Крім того, Symantec AntiVirus повідомляє користувача про необхідність завершити службу або зупинити процес для усунення побічних ефектів вірусу або загрози.

У огляді будь-якого типу можна налагодити наступні повідомлення:

Ви можете задати текст повідомлення з повідомленням. Для цього введіть текст в поле повідомлення або клацніть правою кнопкою миші в полі для вибору змінних.

Як приклад нижче розглянута процедура налагодження повного огляду, проте повідомлення можна аналогічним чином налагодити і для інших типів огляду.

Як налагодити повідомлення для вірусів і погроз безпеці

1. На лівій панелі розверніть пункт **Осмотр** і виберіть **Полный осмотр**.
2. На правій панелі виберіть **Параметры**.
3. У вікні параметрів огляду натисніть кнопку **Сообщения**.
4. У вікні параметрів повідомлень знайдіть розділ параметрів виявлення і відзначте пункт **Показывать сообщения на атакованом компьютере**.

Якщо при виявленні вірусу або загрози на комп'ютері слід показувати повідомлення.

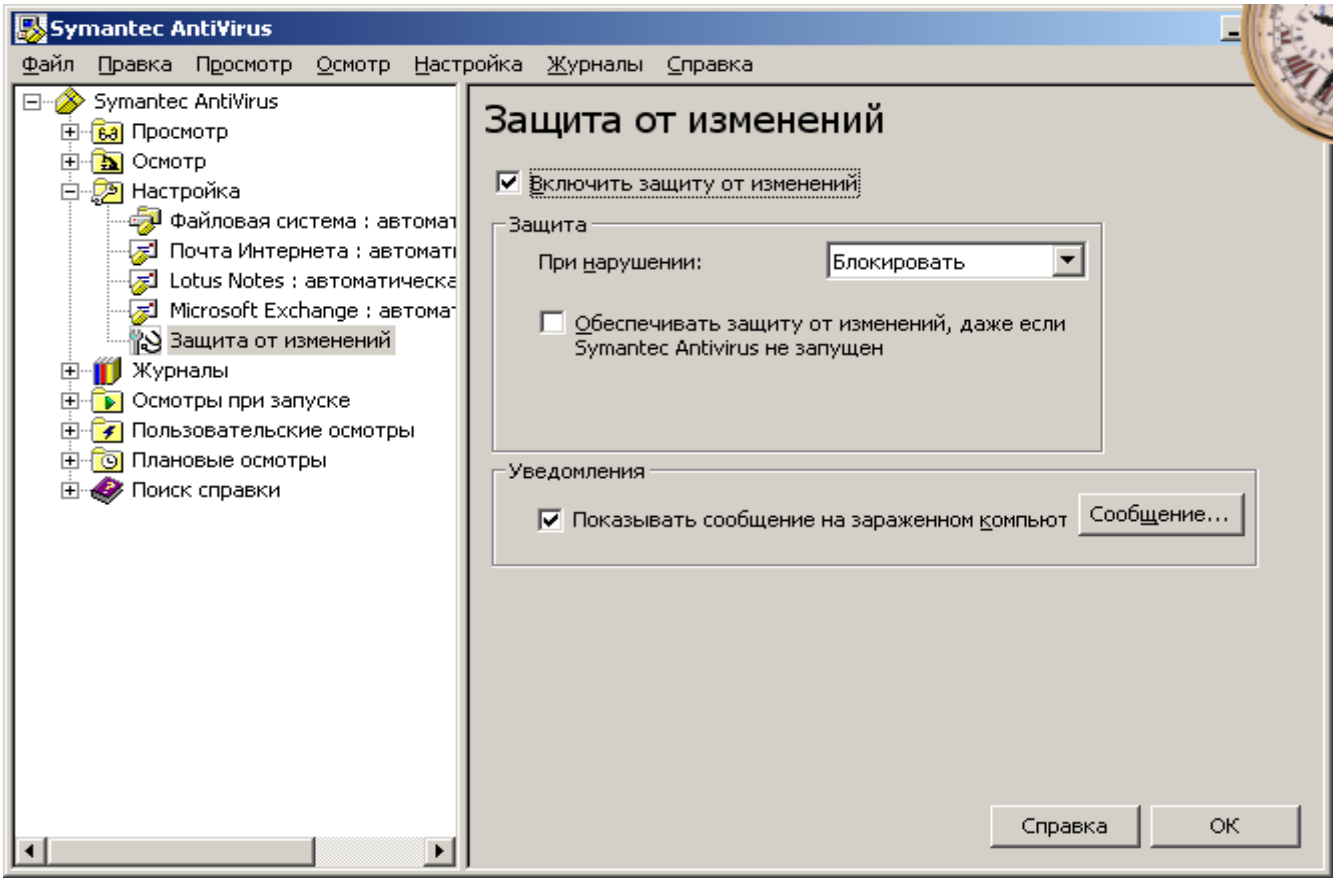


Рис. 13 Вікно вибору параметра захисту від змін

Таблиця 4

Опис полів повідомлення функції захисту від змін

Поле	**Опис**
Ім'я файлу	Ім'я файлу, що атакував захищений процес.
Шлях	Повне ім'я файлу, що атакував захищений процес.
Розташування	Апаратне або програмне забезпечення комп'ютера, захищене від змін. У разі повідомлень функцій захисту від змін це додатки Symantec.
Комп'ютер	Ім'я атакованого комп'ютера.
Користувач	Ім'я користувача, що працював в системі у момент виявлення атаки.
Дата виявлення	Дата виявлення атаки.
Виконана дія	Дія, виконана функцією захисту від змін у відповідь на атаку.
Подія системи	Тип виявленої спроби зміни.
Тип об'єкту	Тип цільового об'єкту атаки.
ID процесу-ініціатора	Ідентифікатор процесу, що атакував додаток Symantec.
Ім'я процесу ініціатора	Ім'я процесу, що атакував додаток Symantec.
Шлях до цільового об'єкту	Розташування цільового об'єкту атаки.

ID цільового процесу	Ідентифікатор цільового процесу, який був атакований.
ID цільового сеансу терміналу	Ідентифікатор сеансу терміналу, в якому виникла подія.

Таблиця 5

Параметри налагодження повідомлень

Параметри виявлення	Ви можете створити повідомлення, яке слід показувати на комп'ютері при виявленні вірусу або загрози за допомогою програми Symantec AntiVirus. Під час налагодження автоматичного захисту файлової системи можна вибрати додатковий параметр, що включає відображення вікна діалогу з результатами огляду при виявленні вірусу або загрози в ході автоматичного огляду.
Параметри виправлення	Вкажіть, чи хочете ви отримувати повідомлення про виявлення вірусів і погроз, а також необхідності завершити процес або зупинити службу для усунення загрози.

У табл. 6 описані поля змінних, які можна використовувати в повідомленнях з повідомленнями.

Таблиця 6

Поля змінних повідомлень з повідомленнями

Поле	**Опис**
Ім'я вірусу	Ім'я виявленого вірусу або загрози безпеці.
Дія	Дія, виконана при виявленні вірусу або загрози. Це може бути перша настроєна дія або друга настроєна дія.
Стан	Стан файлу: «Заражений», «Не заражений» або «Видалений». Ця змінна не використовується за умовчанням. Для проглядання цієї інформації уручну додайте змінну в повідомлення.
Ім'я файлу	Ім'я зараженого файлу.
Шлях	Повне ім'я файлу, що містить вірус або загрозу.
Розташування	Диск комп'ютера, що містить вірус або загрозу.
Комп'ютер	Ім'я комп'ютера, на якому був виявлений вірус або загроза.
Користувач	Ім'я користувача, що працював в системі у момент виявлення вірусу або загрози.
Подія	Тип події, наприклад «Виявлена загроза».
Тип огляду	Тип огляду (огляд уручну, плановий огляд і так далі), в ході якого був виявлений вірус або загроза.
Дата виявлення	Дата виявлення вірусу або загрози безпеці.
Ім'я	Область додатку, наприклад, автоматичний захист файлової

сховища	системи або автоматичний захист Lotus Notes.
Опис дії	Докладний опис дій, виконаних при виявленні вірусу або загрози.

5. Для створення повідомлення виконаєте наступні дії в полі повідомлення:
   - Клацніть, щоб ввести або змінити текст повідомлення.
   - Клацніть правою кнопкою миші, виберіть пункт **Вставить поле** і виберіть поле змінної, яке необхідно вставити.
   - Клацніть правою кнопкою миші і виберіть пункт **Вырезать**, **Скопировать**, **Вставить**, **Очистить** або **Отменить**.
6. При налагодженні повідомлень для автоматичного захисту файлової системи під полем повідомлення доступний додатковий параметр. Відмініть вибір пункту **Показывать сообщения на зараженням компьютере** , щоб на зараженому комп'ютері не з'являлося вікно результатів, коли автоматичний захист виявляє віруси і погрози безпеці.
7. У розділі параметрів виправлення відзначте необхідні пункти. Передбачені наступні варіанти:

Автоматично завершувати процеси

Якщо вибраний цей пункт, то Symantec AntiVirus автоматично завершує процеси, коли це необхідно для усунення вірусу або загрози безпеці. Symantec AntiVirus не пропонуватиме користувачам зберегти дані перед завершенням процесів.

Автоматично зупиняти служби

Якщо вибраний цей пункт, то Symantec AntiVirus автоматично зупиняє служби, коли це необхідно для усунення вірусу або загрози безпеці. Symantec AntiVirus не пропонуватиме користувачам зберегти дані перед завершенням служб.

8. Натисніть кнопку **ОК** стільки раз, скільки необхідно для повернення в головне вікно Symantec AntiVirus. Після цього виберіть **Осмотр**.

Дії при отриманні повідомлень

За умовчанням Symantec AntiVirus повідомляє користувача при виявленні вірусу або загрози безпеці. З'являється наступне вікно результатами автоматичного захисту:

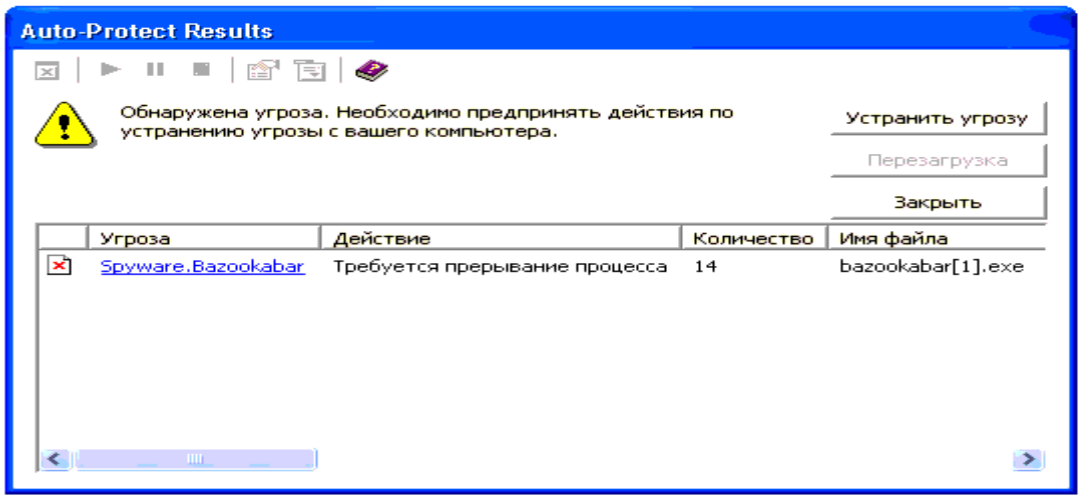


Рис. 14 Вікно повідомлення результатами автоматичного захисту

Якщо Symantec AntiVirus необхідно завершити процес або додаток, або зупинити службу, то у вікні буде доступна кнопка **Устранить угрозу**. Якщо користувач натисне цю кнопку, то з'явиться наступне повідомлення:

Воно дає можливість зберегти дані і закрити відкриті застосування, якщо ви ще не зробили цього. Після збереження даних можна повернутися до вікна повідомлення і натиснути кнопку **Да** для завершення процедури видалення.

Якщо Symantec AntiVirus необхідно перезапустити комп'ютер для завершення операції видалення загрози, то у вікні буде активна кнопка **Перезагрузка**. Якщо користувач натисне цю кнопку, то з'явиться наступне повідомлення:

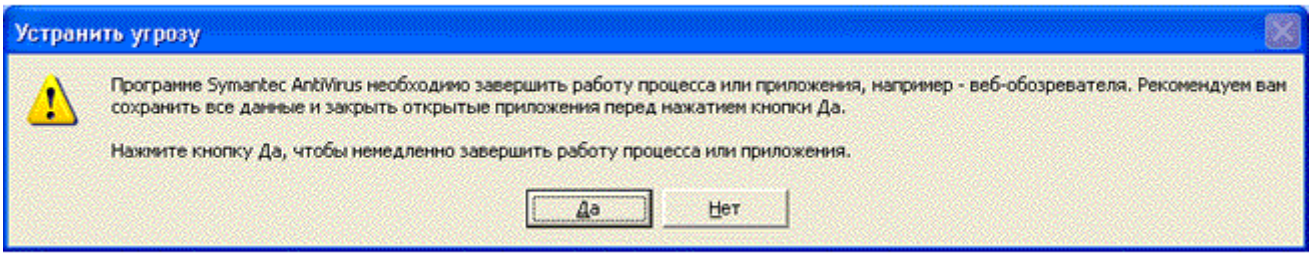


Рис.15 Вікно завершення процесу

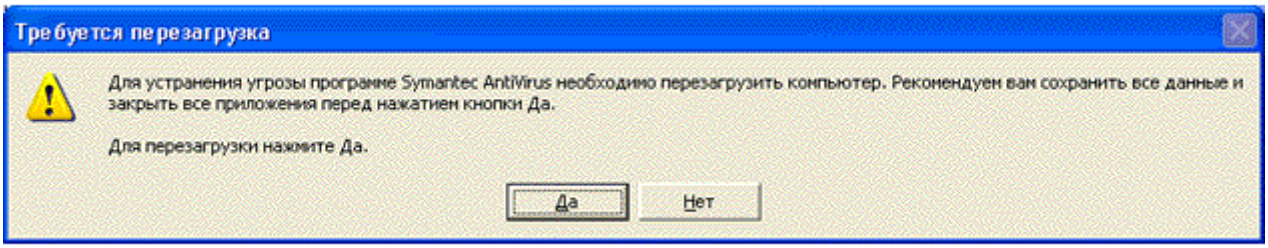


Рис. 16 Вікно спроби перезавантаження комп'ютера

Воно дає можливість зберегти дані і закрити відкриті застосування, якщо ви ще не зробили цього. Після збереження даних можна повернутися до вікна повідомлення і натиснути кнопку **Да** для перезапуску комп'ютера. Якщо ви натиснете кнопку **Нет** і закриєте вікно, не перезавантажуючи комп'ютер, то операція видалення буде повністю завершена тільки після наступного перезапуску системи.

Якщо ви спробуєте закрити вікно повідомлення, не завершивши усунення загрози, то з'явиться наступне повідомлення:

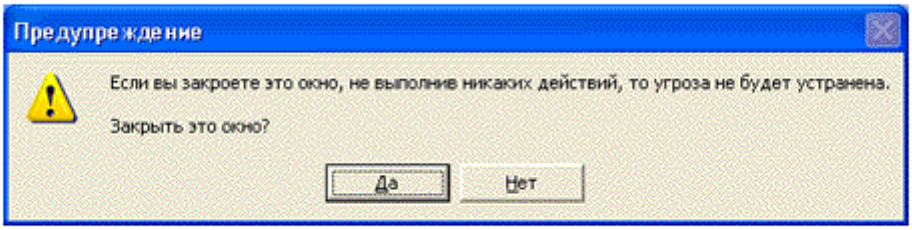


Рис. 17 Вікно нагадування про наявну загрозу

Якщо ви натиснете кнопку **Да** і закриєте вікно діалогу, не виконавши ніякої дії, то загрозу можна буде усунути пізніше наступними способами:

- Відкрийте журнал погроз, клацніть правою кнопкою миші на записі про загрозу і виконаєте необхідну дію.

- Запустіть огляд для повторного виявлення загрози. При цьому знову з'явиться вікно результатів.

Можливі дії залежать від дій, настроєних для виявленого вірусу або загрози безпеці.

Якщо ви натиснете кнопку **Нет** то знову з'явиться вікно результатів, щоб ви могли виконати необхідну дію.

1.18 Категорія Журнали

Категорія **Журнали** дозволяє відстежувати інформацію про виконані в системі огляди, а також виявлені віруси і погрози безпеці.

Таблиця 7

Опис категорія журнали

Параметр	Опис
Журнал погроз	Показує список наступних об'єктів: Список вірусів, виявлених в системі, і додаткову інформацію про зараження. Список погроз безпеці, таких як програми показу реклами і програми-шпигуни, які були виявлені програмою Symantec AntiVirus і зареєстровані в журналі, ізольовані і виправлені, або видалені.
Журнали оглядів	Містять інформацію про огляди, виконані на комп'ютері. Для кожного огляду показана додаткова інформація.
Журнал подій	Журнал виконаних в системі операцій, пов'язаних з вірусами і погрозами безпеці. Зокрема, журнал містить зведення про зміни конфігурації, помилки і файл описів.
Журнал змін	Список спроб змінити додатки Symantec на локальному комп'ютері.

1.19 Відбір записів за датою

1. У меню **Журналы** виберіть **Журнал событий** (рис. 18)
2. Розверніть випадаючий список **Все элементы** (або діапазон дат).
3. Виберіть **Фильтр** (рис. 19)
4. Якщо був вибраний діапазон, виберіть початкову і кінцеву дати і натисніть кнопку **ОК**.

1.20 Відбір записів за категорією подій

1. У меню **Журналы** виберіть **Журнал событий**.
2. Виберіть **Фильтр** журналу подій.
3. Виберіть одну або декілька категорій подій.
4. Натисніть кнопку **ОК**.

1.21 Видалення записів з журналу подій

Записи журналу подій не можна видалити засобами програми Symantec AntiVirus.

Для того, щоб видалити записи журналу подій, необхідно видалити файли .log, що містять ці записи. Події за кожен день тижня зберігаються в окремому файлі .log із каталога Logs програми Symantec AntiVirus. Імена цим файлам привласнюються відповідно до дня їх створення. Файли .log видаляти не рекомендується, оскільки це приведе до втрати тих, що містяться в них даних антивірусного захисту.

1.22 Експорт даних у файл .csv

1. Переконаєтеся, що дані, які потрібно зберегти, показані у вікні журналу погроз, журналу огляду або журналу подій.
2. Натисніть кнопку **Экспортировать**.
3. У вікні збереження файлу виберіть теку для збереження файлу і введіть його ім'я.
4. Натисніть кнопку **Сохранить**.

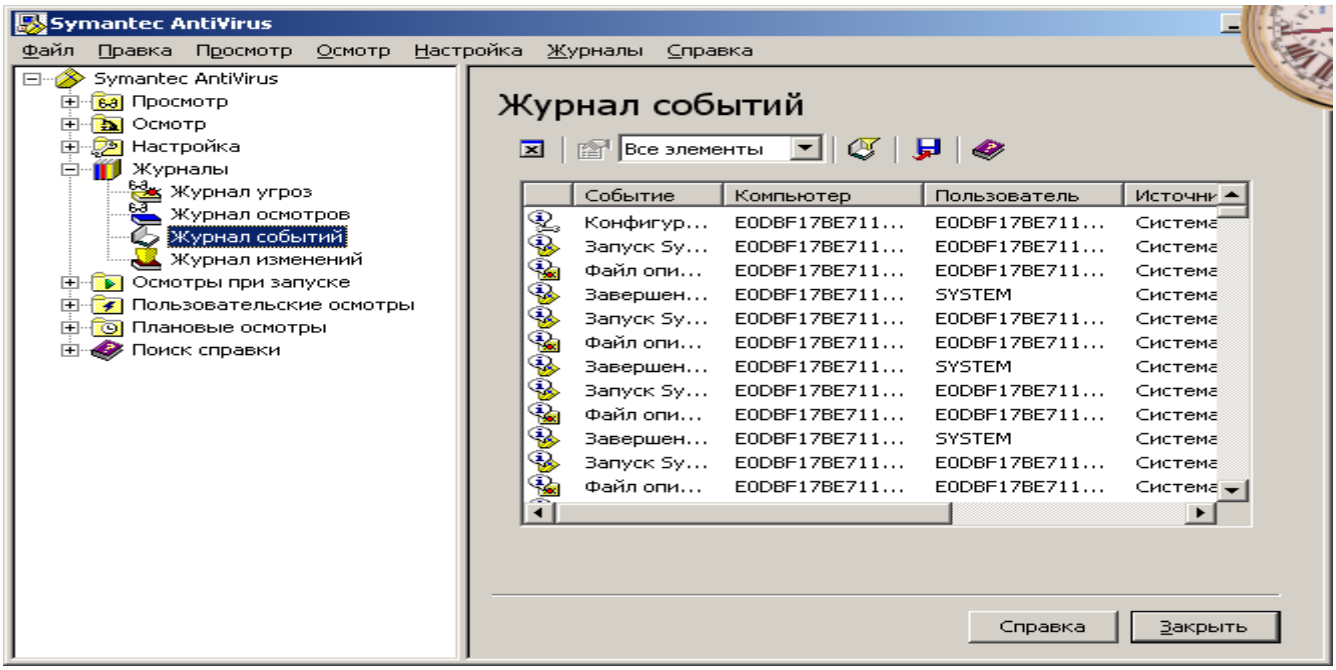


Рис. 18 Журнал подій

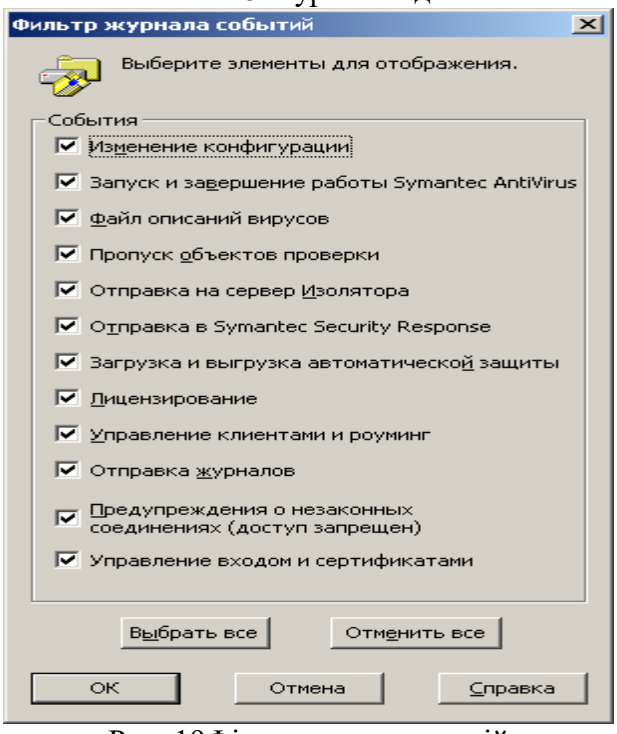


Рис. 19Фільтр журналу подій

1.23 Категорія Огляди при запуску

Категорія Огляди при запуску дозволяє створювати і настроювати огляди, що запускаються разом з системою.

Таблиця 8

Опис категорії огляди при запуску

Параметр	Опис
Створити огляд при запуску	Деякі користувачі доповнюють планові огляди автоматичними оглядами при запуску системи. Часто огляди при запуску обмежуються найбільш важливими теками, такими як тека Windows і теки шаблонами Microsoft Word і Microsoft Excel.
Автоматично створений швидкий огляд	Цей тип огляду перевіряє на наявність вірусів і погроз файли, завантажені в оперативну пам'ять, і інші стандартні для зараження розташування при кожному вході користувача в систему. Такий огляд можна настроювати так само, як і огляди уручну, за винятком того, що в його параметрах не можна відключити огляд завантажених в пам'ять файлів і інших стандартних для зараження розташувань комп'ютера. Примітка: Цей тип огляду доступний тільки на некерованих клієнтах.

1.24 Категорія Призначені для користувача огляди

За допомогою категорії призначені для користувача огляди можна заздалегідь налагодити операції огляду, які надалі виконуватимуться уручну.

Таблиця 9

Опис категорії призначені для користувача огляди

Параметр	Опис
Створити призначений для користувача огляд	Якщо ви часто оглядаєте один і той же набір файлів і тек, рекомендується створити призначений для користувача огляд, в якому будуть перераховані елементи, що оглядаються. Цей тип огляду дозволяє швидко перевірити заданий набір файлів і тек на наявність вірусів і інших погроз

1.25 Категорія Планові огляди

Категорія Планові огляди дозволяє створювати огляди, що автоматично запускаються в указаний час.

Таблиця 10

Опис категорії категорія планові огляди

Параметр	Опис
Створити плановий огляд	Заплануйте огляд жорстких дисків, що виконується не рідше за один раз на тиждень. Плановий огляд дозволяє переконатися, що на комп'ютері немає вірусів і інших погроз безпеці.

Включення і виключення автоматичного захисту

За умовчанням автоматичний захист від вірусів і інших погроз безпеці завантажується при запуску системи. Він перевіряє програми на наявність вірусів і погроз

безпеці, а також відстежує виконання тих операцій, які можуть указувати на наявність вірусу або загрози. При виявленні вірусу, вірусоподібних дій (подій, які можуть бути результатом наявності вірусу) або загрози безпеці, функція автоматичного захисту попереджає про це користувача.

В деяких випадках функція автоматичного захисту може попереджати про дії, вказуючи на наявність вірусу, хоча відомо, що ці дії не є наслідком роботи вірусу. Наприклад, це може відбутися при установці нових програм. При виконанні подібних дій, для того, щоб уникнути виведення попереджень, рекомендується тимчасово відключити автоматичний захист. Обов'язково включіть автоматичний захист відразу після завершення завдання, щоб комп'ютер залишався захищеним від вірусів.

Відключення автоматичного захисту може бути заблоковане системним адміністратором; крім того, автоматичний захист можна відключити тимчасово, щоб він автоматично включався через вказаний проміжок часу.

1.26 Застосування Symantec AntiVirus разом з Windows Security Center

Якщо для відстежування рівня безпеки в системі Windows XP із пакетом оновлення 2 застосовується програма Windows Security Center (WSC), то в її вікні буде показано стан Symantec AntiVirus.

Таблиця 11

Стан системи захисту, яке може бути показане в WSC.

Стан продукту Symantec	Стан системи захисту
Symantec AntiVirus не встановлений	Не знайдено (відмічено червоним кольором)
Програма Symantec AntiVirus встановлена з повним набором функцій захисту	Включена (відмічено зеленим кольором)
Програма Symantec AntiVirus встановлена, але описи вірусів і погроз застаріли	Застаріла (відмічено червоним кольором)
Програма Symantec AntiVirus встановлена, і в ній включений автоматичний захист файлової системи	Вимкнена (відмічено червоним кольором)
Програма Symantec AntiVirus встановлена, автоматичний захист файлової системи не включений, а описи вірусів і погроз застаріли	Вимкнена (відмічено червоним кольором)
Програма Symantec AntiVirus встановлена, і функція Rtvscan уручну вимкнена	Вимкнена (відмічено червоним кольором)

1.27 Зміна і видалення оглядів

При необхідності ви можете внести зміни до оглядів при запуску, призначені для користувача і планові огляди, а також видалити їх. Ті параметри, які не можна налагодити для вибраного типу огляду, будуть недоступні для зміни.

Зміна огляду

1. На лівій панелі Symantec AntiVirus виберіть огляд для зміни.
2. Натисніть кнопку **Изменить**.
3. У вікні, що з'явилося, можна виконати наступні дії:

- У разі призначеного для користувача огляду відкрийте вкладку **Файлы** і виберіть ті файли, теки і диски, які повинні оглядатися.
- У разі планового огляду відкрийте вкладку **Расписание** і змініть періодичність виконання огляду, а також дату і час запуску огляду.

- На вкладці **Имя /Описание** змініть ім'я і опис огляду.

4. При необхідності натисніть кнопку **Параметры** для зміни наступних параметрів огляду:

- Типи файлів: Огляд може виконуватися за типом або розширенням файлів
- Підвищення ефективності огляду: Можна включити огляд програмних файлів, завантажених в пам'ять, огляд найбільш схильних до зараження розташувань, а також пошук ознак відомих вірусів і погроз перед оглядом вибраних файлів і тек.
- Файли, що виключаються, і теки
- Додаткові параметри огляду: Параметри стислих файлів, перенесення з пам'яті і так далі.
- Дії, що виконуються при виявленні вірусу або іншої загрози безпеці
- Параметри навантаження
- Повідомлення: У параметрах виявлення можна задати повідомлення, яке повинне з'являтися при виявленні вірусу або загрози. У параметрах виправлення можна вказати, чи слід повідомляти користувача про майбутнє виконання таких дій з виправлення, як завершення служби.

5. Натисніть кнопку **ОК** стільки раз, скільки необхідно для повернення в головне вікно Symantec AntiVirus.

Видалення огляду

- На лівій панелі Symantec AntiVirus клацніть правою кнопкою миші на огляді, який потрібно видалити, потім виберіть команду **Удалить**.

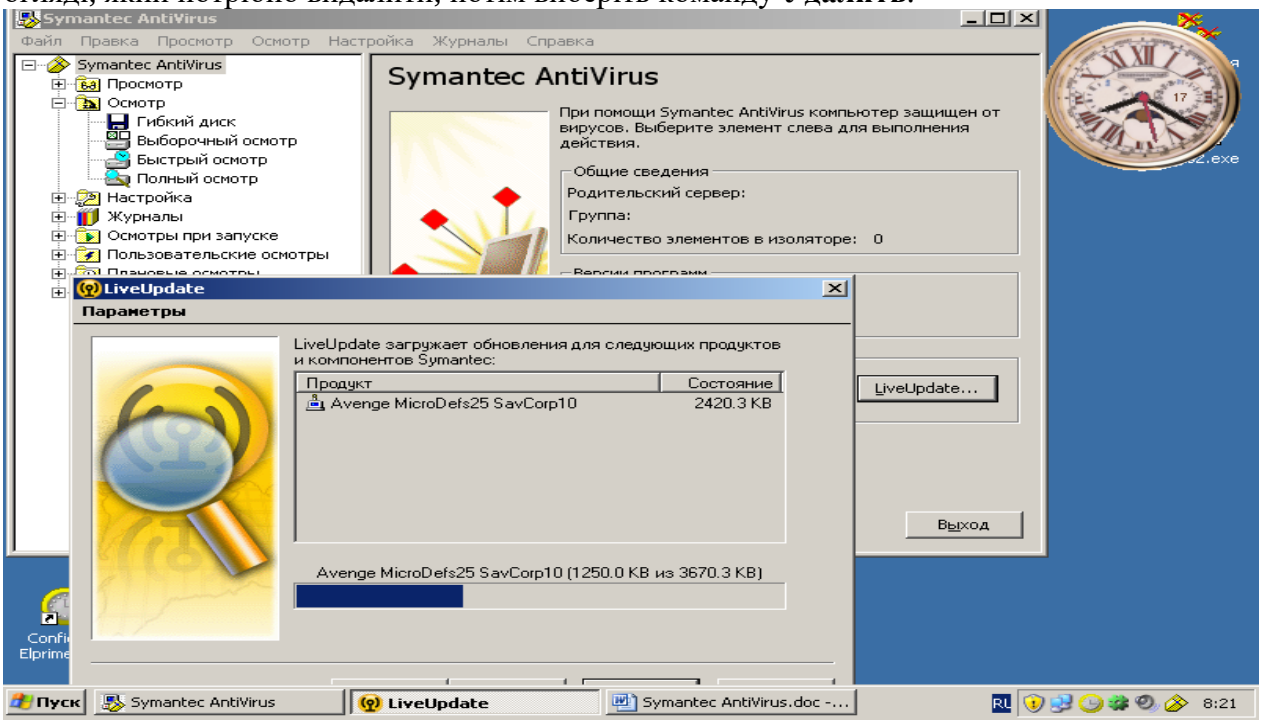


Рис. 20 Вікно оновлення баз

1.28 Оновлення баз даних програми вручну

1. Необхідно запустити програму.
2. В вікні програми подати команду **LiveUpdate,** з'явиться вікно оновлення (рис. 20), яке автоматично дозволить отримати нові оновлення.
3. За закінченням оновлення з'явиться вікно (рис. 21).
4. Подати команду **Готово**. Далі почнеться оновлення баз програми (рис. 22).

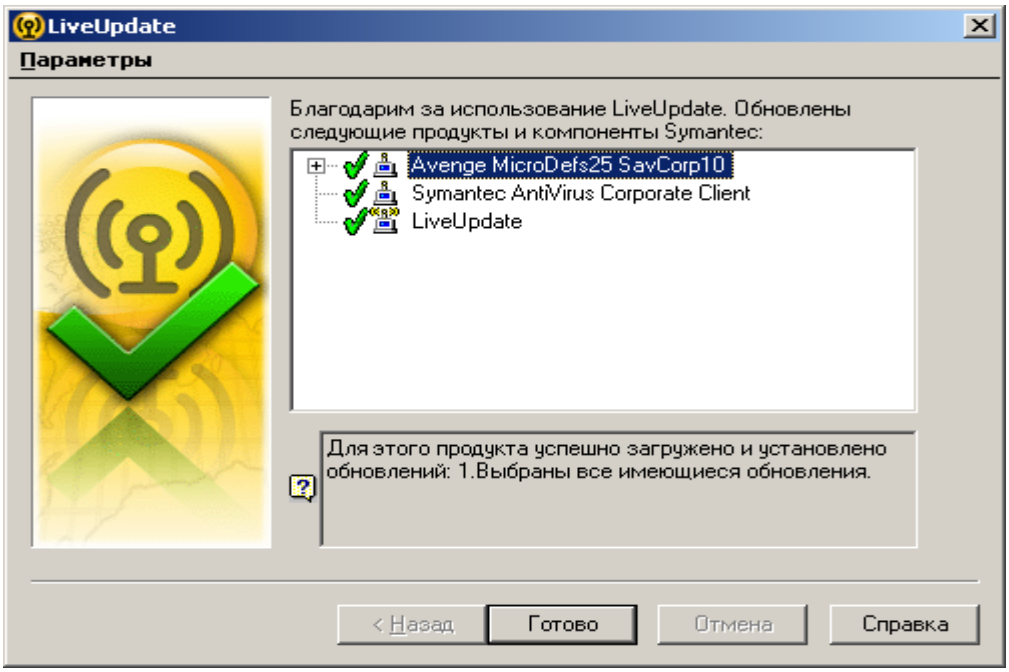


Рис.21 Вікно закінчення оновлення баз

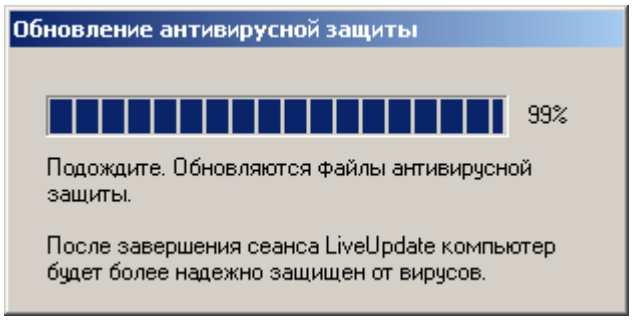


Рис. 22 Вікно оновлення баз в програмі

2. Хід роботи

1. Відкрийте вікно програми Symantec AntiVirus.
2. Перегляньте файли і відомості про них в Ізоляторі
3. Проведіть очистку уручну теки Копії заражених файлів.
4. Проведіть налагодження автоматичного видалення файлів
5. Встановіть для огляду типи файлів Microsoft Word, Excel та Access.
6. Встановіть для огляду файли за розширенням exe, bat, com.
7. Проведіть Налагодження повідомлень про віруси і погрози безпеці.
8. Проведіть налагодження журналу подій відбір записів за датою.
9. Проведіть налагодження журналу подій відбір записів за категорією подій.
10. Запустіть огляду уручну в Symantec AntiVirus.
11. Створіть огляд при запуску категорії швидкий.
12. Перевірте наявність огляду при запуску.
13. Встановіть налагодження захисту від змін.
14. Перевірте Застосування Symantec AntiVirus разом з Windows Security Center
15. Проведіть видалення оглядів.
16. Проведіть оновлення баз даних програми вручну.

3. Контрольні питання

1. Загальні відомості про програму Symantec AntiVirus
2. Які категорії погрозі безпеці ізолює програма?
3. Реакція програми на погрози безпеці.
4. Типи захисту програм.
5. Можливості категорії перегляд.
6. Як повторно оглянути ізольовані файли за допомогою Майстра лікування?
7. Як очистити уручну теку «Копії заражених файлів»?
8. Можливості категорії огляд.
9. Як вибрати для огляду типи файлів?
10. Як запустити огляду уручну в Symantec AntiVirus?
11. Можливості категорії налагодження
12. Як створити огляд при запуску та відібрати потрібні параметри?
13. Як включити або вимкнути огляд на наявність погроз в налагодженнях автоматичного захисту?
14. Як провести налагодження захисту від змін?
15. Як провести налагодження повідомлень про віруси і погрози безпеці?
16. Можливості категорії журнали.
17. Як провести налагодження журналу подій на відбір записів за датою та категорією подій?
18. Як провести видалення записів з журналу подій?
19. Призначення категорії «Огляди при запуску».
20. Призначення категорії «Планові огляди».
21. Як проводиться застосування Symantec AntiVirus разом з Windows Security Center?
22. Як проводиться Зміна і видалення оглядів?
23. Як проводиться оновлення баз даних програми вручну?

СПИСОК ВИКОРИСТОВАННОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

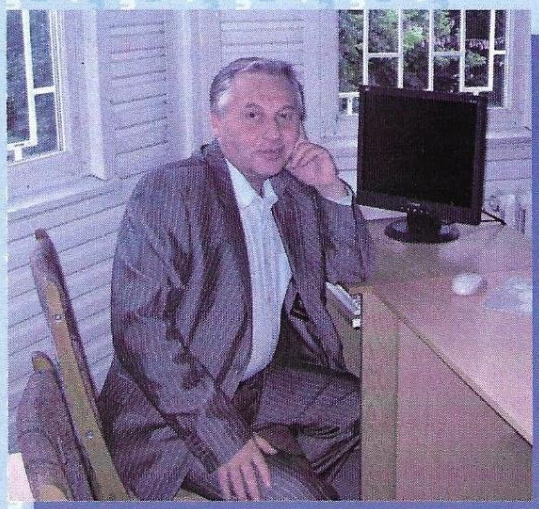
ОСНОВНА ЛІТЕРАТУРА

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с.
2. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с., іл.
3. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
4. Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.
5. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
6. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защити информации. Т. 1 : Несанкционированное получение информации. – К.: Арий, 2008. – 464 с.

ДОДАТКОВА ЛІТЕРАТУРА

7. Ахрамович. В.М. Ідентифікація й аутентифікація, керування доступом Сучасний захист інформації.К. ДУТ:-2016 .-№4.- с. 47-51
8. Ахрамович В.М. Захист інформації під час застосування операційної системи Windows 7 Науковий Вісник ДАСОА, 2012, №2.-с.96-116
9. Ахрамович. В.М., Чегренець В.М. Уразливості та способи захисту бездротових мереж. Тези доповідей *II Міждународної науково-практичної конференції. «Тенденції розвитку конвергентних мереж: рішення* **пост** - *NGN, 4G и 5G»*, **1**7 - 18 листопада 2016 року с. 163-166.
10. Ахрамович В.М. Захист інформації під час застосування особистої системи мережевого захисту McAfee Personal Firewall Plus. Науковий Вісник ДАСОА 2006, №2.-с.87-96.
11. Ахрамович В.М. Захист інформації під час застосування операційної системи Windows XP. Науковий Вісник ДАСОА 2007, №2.-с.92-105.
12. Ахрамович В.М. Резервування систем інформації в Norton Ghost. Науковий Вісник ДАСОА 2007, №4.-с.90-104
13. Ахрамович В.М. Програми захисту інформації приховуванням її та шифруванням. Науковий Вісник ДАСОА 2008, №4.-с.100-109
14. Алферов, А. П. Основы криптографии [Текст] : учебное пособие для вузов / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин. - М.: Гелиос АРВ 2005 (Гриф МО).
15. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации: учебное пособие / – Тамбов: Изд-во Тамб. гос. техн. ун-та,2006. – 196 с.
16. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с.
17. Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-Сум-Вінниця, 2009. – 240 с.
18. Єжова Л.Ф. Управління інформаційною безпекою / Л.Ф. Єжова, І.О. Мачалін, Я.В. Невойт, В.О. Хорошко. – В 2-х т. – К. : Вид-во ДУІКТ, 2011. – 236 с.

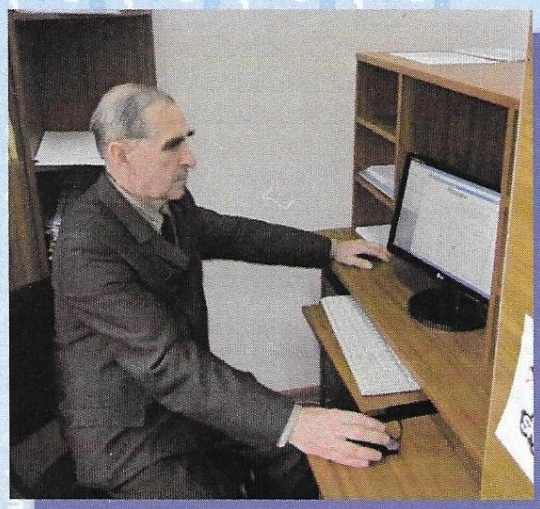
19. Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Издание 2-е испр. и доп.– М.:Машиностроение-1, 2006. − 260 с.
20. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защити информации. Т. 2 : Информационная безопасность. – К.: Арий, 2008. – 344 с.
21. Лужецький В.А. Захист персональних даних. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 487 с
22. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк. – М. : Изд-во "Высш. шк.", 2004. – 280 с.
23. Мельников В.П. Информационная безопасность и защита информации. – М.: «Академия», 2008. – 336 с.
24. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
25. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віх-рова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
26. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
27. Садердинов А.А. Информационная безопасность предприятия. – М.: «Дашков и К», 2005. – 336 с.
28. Хорошко В.А., Чекатов А.А. Методы и средства защиты информации. – К.: ЮНИОР, 2003. – 504 с.
29. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учеб. пособие / В. Ф. Шаньгин. – М. : ИД «ФОРУМ» ; ИНФРА-М, 2008.
30. Широчин В. П., Широчин С. В., Мухін В. Є. Основи безпеки комп`ютерних систем. К.: «Корнійчук». 2009 С.285.
31. Шорошев В.В. Основи формування політики безпеки комп’ютерних систем: наукове видання. – К.: Бізнес і безпека, 2006. – 141с.
32. Щеглов А.Ю. Защита компьютерной безопасности от несанкционированного доступа /А.Ю. Щеглов. – СПб. : Изд-во "Наука", 2004. – 384
33. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – К.: «МК-Прес», 2005. – 432 с.



АХРАМОВИЧ ВОЛОДИМИР МИКОЛАЙОВИЧ

Випускник Національного технічного університету, кандидат технічних наук, старший науковий співробітник, доцент.

Автор понад 120 наукових праць, у тому числі 13 авторських свідоцтв СРСР та 13 патентів Росії, одноосібний автор трьох навчальних та двох навчально-методичних посібників з інформаційних систем та технологій.



ЧЕГРЕНЕЦЬ ВОЛОДИМИР МИХАЙЛОВИЧ

Випускник Київського вищого інженерного авіаційного військового училища, кандидат технічних наук, доцент кафедри математичного та програмного забезпечення автоматизованих систем вищого інституту ВПС.

Автор понад 70 наукових праць, одноосібний автор трьох навчальних та 5 навчально-методичних посібників з інформаційних систем і технологій, ведучий виконавець трьох науково-дослідних робіт з технічного захисту інформації.