Лабораторна робота № 4
Адміністрування захищених систем та мереж на базі ОС Windows

Частина 1
Тема роботи: Захист інформації на локальному комп'ютері з використанням ОС Windows 2000.

Мета роботи: Навчитися виконувати основні завдання, що виникають в процесі адміністрування ОС Windows 2000: створювати й видаляти облікові записи користувачів, налаштовувати основні параметри політики безпеки, переглядати журнали подій, встановлювати дозволу для об'єктів файлової системи на дисках NTFS, шифрувати файли та каталоги, виконувати резервне копіювання файлів і архівацію даних стану операційної системи.

Завдання на лабораторну роботу

1. Встановити дозволи для об'єктів файлової системи (при використанні файлової системи NTFS). Подивитися, як впливають встановлені дозволу на доступ до цих об'єктів.
2. Налаштувати параметри локальної політики безпеки.
3. Виконати перегляд системних журналів подій.
4. Зашифрувати вміст каталогу **D: \ KIT**. Подивитися, як впливає шифрування на доступність об'єктів файлової системи для інших користувачів.
5. Експортувати сертифікат і закритий ключ, створені для шифрування каталогу, в файл.
6. Розшифрувати зашифровані дані.

Частина 1 Тема роботи: Захист інформації на локальному комп'ютері з використанням ОС Windows 2000.

1. Створення загальних ресурсів та встановлення дозволів для них

Створіть в папці **C: \ KIT** папку **Lab6**. У цій папці створіть три папки з іменами **Folder1**, **Folder2** і **Folder3**.

Файлова система NTFS, яка використовується в системі Windows 2000, дозволяє встановлювати *дозволу* для папок і файлів. Щоб переглянути або змінити ці дозволи, клацніть на значку папки або файлу правою кнопкою миші, у контекстному меню виберіть пункт "*Властивості*"І у вікні перейдіть на вкладку"*Безпека*"(Рис. 1). Якщо вікно не має вкладки"*Безпека*", Це означає, що носій використовує файлову систему FAT або FAT32. Ці файлові системи не дозволяють встановлювати дозволи для папок і файлів.

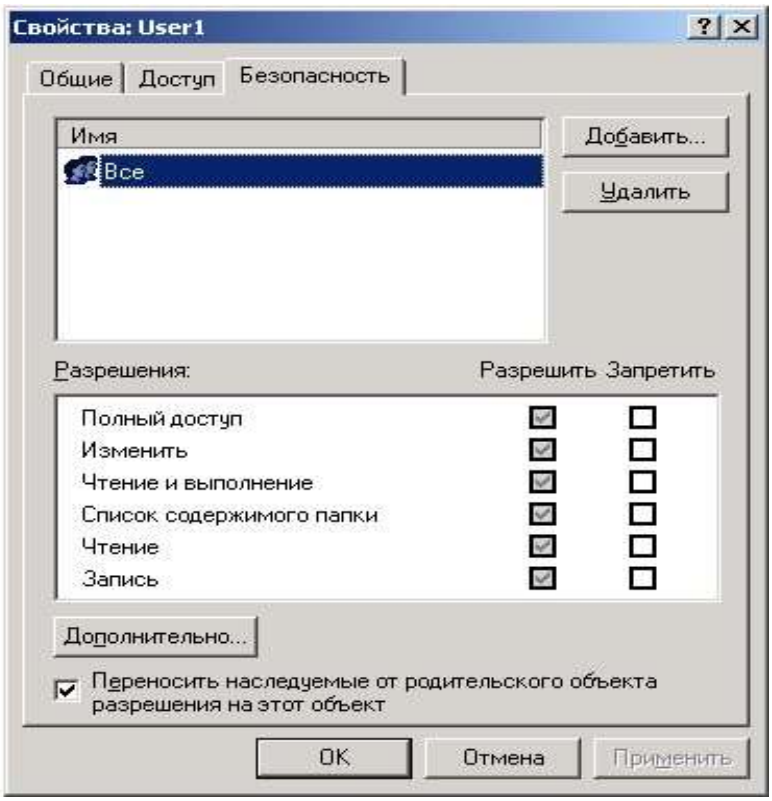


Рис.1. Вкладка "*Безпека*" вікна властивостей об'єкта файлової системи.

Параметри безпеки, яка використовується успадковуються від батьківського об'єкта - каталогу, в якому знаходиться файл або папка. Щоб скасувати успадкування, зніміть прапорець "*Переносити успадковані від батьківського об'єкта дозволу на цей об'єкт*".

Встановлювані дозволу впливають на доступ до об'єкта таким чином:

- **Повний доступ** - Дозволений повний доступ до об'єкта;
- **Читання** - Дозволено читання файлів;
- **Читання та виконання** - Дозволено читання файлів і виконання виконуваних файлів;
- **Список вмісту папки** - Дозволено тільки переглядати вміст папки;
- **Запис** - Дозволено створення файлів;
- **Змінити** - Дозволена зміна, перейменування та видалення файлів.

Дозволи для створених вами папок повинні бути встановлені так, як вказано в таблиці 1.

Таблиця 1.

Ім'я папки	Дозволи
Folder1	Адміністратори - повний доступ, досвідчені користувачі - читання і виконання.
Folder2	Адміністратори - повний доступ, досвідчені користувачі - читання і виконання, користувачі - список вмісту папки, **user1** - Повний доступ.
Folder3	Адміністратори - повний доступ, все - читання і виконання, **user3** - Запис, **user4** -- зміна.

Щоб встановити вказані дозволи, відкрийте папку **C:\KIT\Lab6** у вікні "*Мій комп'ютер*", Клацніть правою кнопкою мишки на папці **Folder1** і в контекстному меню виберіть пункт "*Властивості*". У вікні перейдіть на вкладку "*Безпека*". Перед установкою дозволів для папки

Folder1 не забудьте відмінити *успадкування дозволів від батьківського об'єкта*. На питання про те, як вчинити з успадкованими від батьківського об'єкта дозволами, дайте відповідь "*Видалити*".

Після цього натисніть кнопку "*Додати ...*". З'явиться вікно вибору користувача або групи (рис.2).

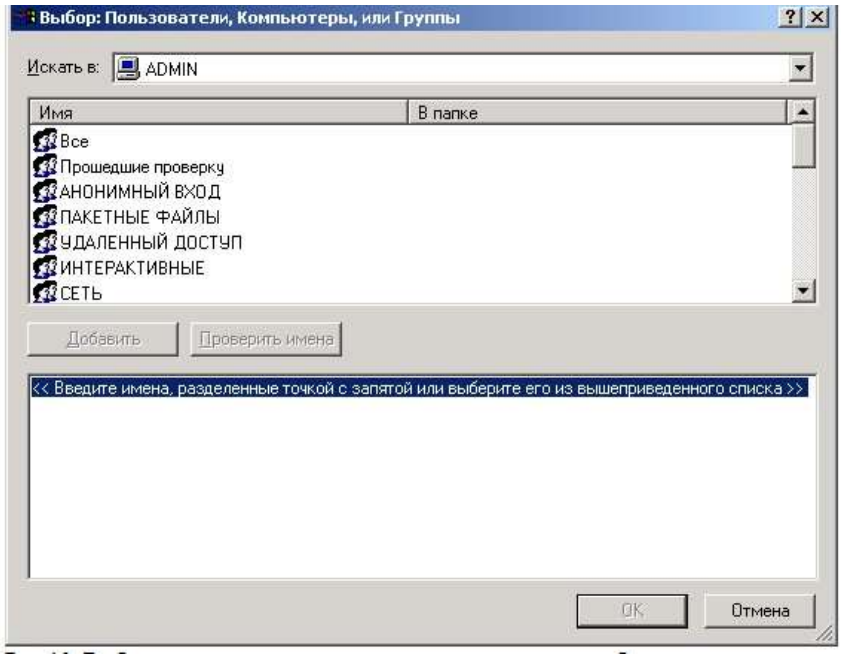


Рис.2. Вибір користувачів, які мають право на доступ до об'єкта

Встановіть повний доступ до цієї папки для групи "*Адміністратори*" і доступ на читання -- для групи "*Досвідчені користувачі*". Для цього у вікні вибору користувача або групи виберіть групи "*Адміністратори*" і "*Досвідчені користувачі*". Для групи "*Адміністратори*" встановіть прапорець "*Повний доступ*", А для групи "*Досвідчені користувачі*" – Прапорець "*Читання та виконання*". Вікно дозволів має виглядати так, як показано на рис.3. Після встановлення дозволів натисніть кнопку "*ОК*".

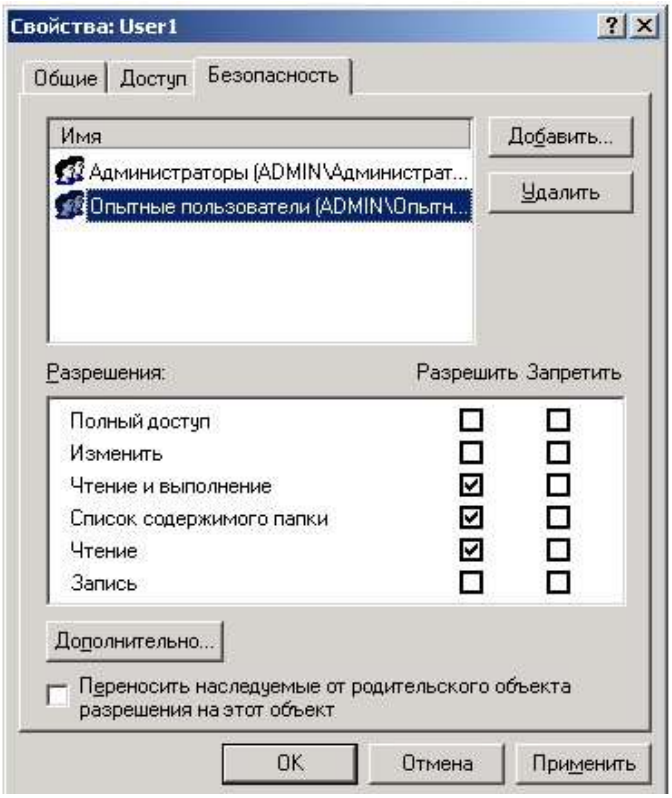
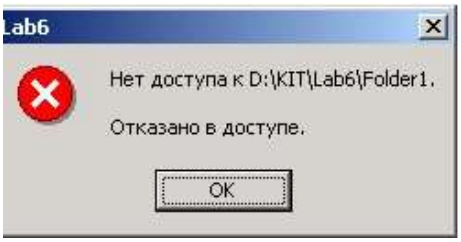


Рис.3. Так повинні бути встановлені дозволу для папки **Folder1**

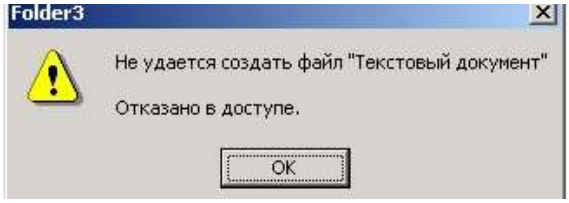
Таким же чином змініть дозволу для інших папок відповідно до таблиці 1.

Завершіть сеанс і увійдіть в систему під іменем **user1**. Подивіться, як змінилися ваші права доступу до папок.

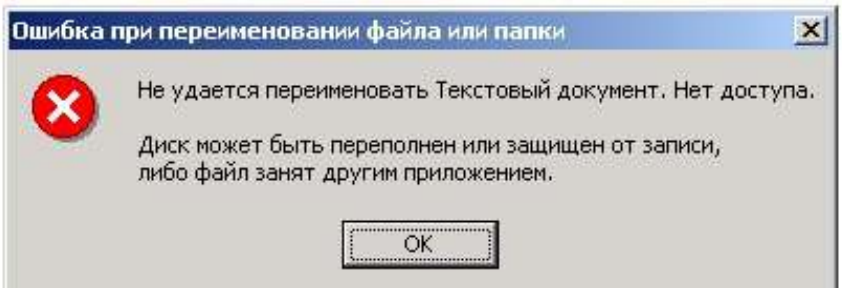
Щоб перевірити, чи є у вас право на **читання**, досить спробувати відкрити папку. Якщо доступ на читання у вас немає, буде видано таке повідомлення:



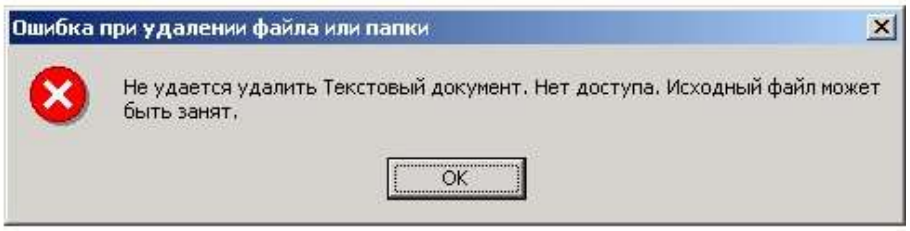
Щоб дізнатися, чи маєте ви право на **запис**, спробуйте створити в папці будь-який файл, наприклад, текстовий. Для створення файлу у вікні "*Мій комп'ютер*" в меню "*Файл*" виберіть команду "*Створити*" і з випадаючого списку виберіть пункт "*Текстовий документ*". Якщо ви не маєте права на запис, ви побачите таке повідомлення:



Щоб дізнатися, чи маєте ви право на **зміна**, Спробуйте перейменувати або видалити створений файл. Якщо ви не маєте права на зміну, перейменування файлу ви побачите таке повідомлення:



При видаленні ви отримаєте ще одне повідомлення:



Подивіться, як впливають встановлені права доступу до папок. Після цього завершіть сеанс і увійдіть в систему під іменем **user2**, Потім під іменами **user3** і **user4**. Подивіться, як при цьому змінюються ваші права доступу до папок. Зробіть висновок, яка різниця існує між роздільною здатністю для конкретного користувача і дозволом для групи.

Після цього ввійдіть до системи з правами адміністратора (під своїм ім'ям) і видаліть створені папки.

2. Налаштування основних параметрів локальної політики безпеки

Для виконання налаштування локальної політики безпеки виконайте команду *Пуск Налаштування Панель управління Адміністрування Локальна політика безпеки.* При цьому відкриється вікно "*Локальні параметри безпеки*"(Рис.4).

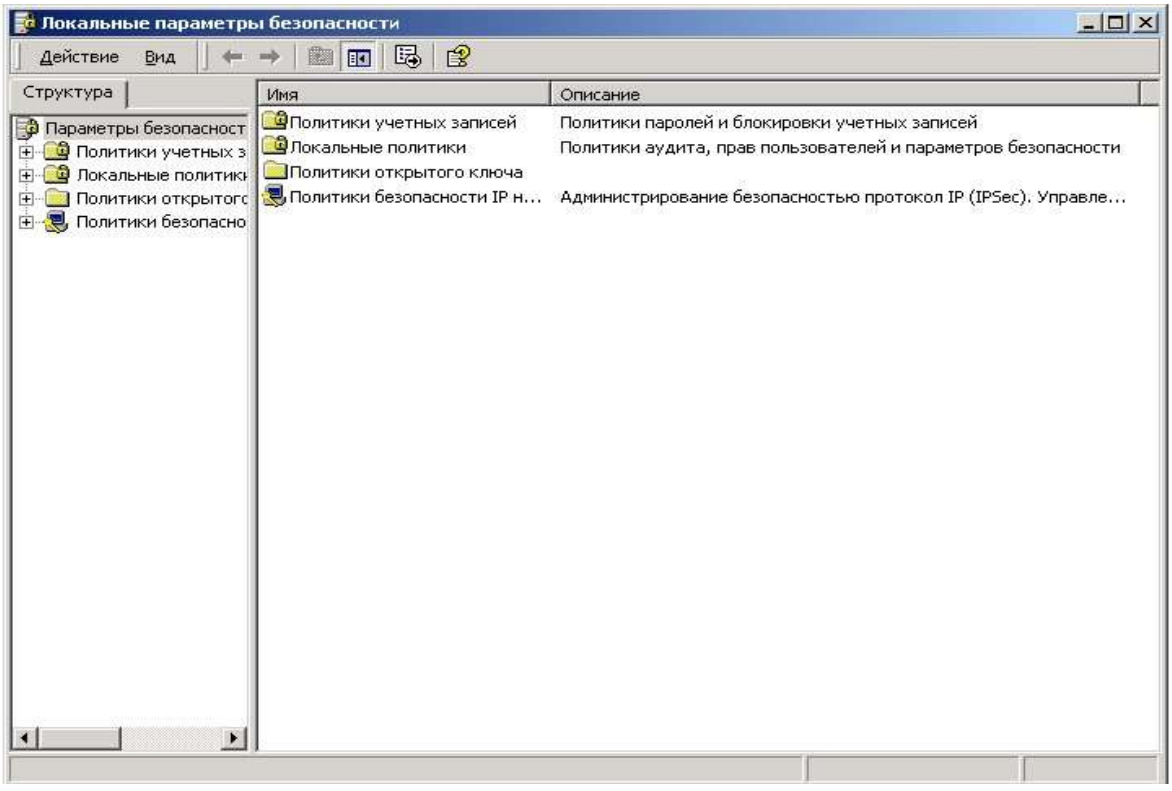


Рис.4. Вікно локальних параметрів безпеки.

У лівій частині вікна консолі виберіть розділ "*Політики облікових записів*" і в ньому підрозділ "*Політика паролів*". Встановіть параметр "*Макс. термін дії пароля*" рівним 0.

Перейдіть у розділ "*Локальні політики*" і в ньому відкрийте підрозділ "*Політика аудита*". Встановіть для параметра "*Аудит входу в систему*" значення **успіх** і **відмова**.

Перейдіть до підрозділу "*Параметри безпеки*". Встановіть значення параметрів так, як вказано у таблиці 2.

Таблиця 2.

Параметр	**Значення**
Вимкнути CTRL + ALT + DEL запит на вхід в систему	Відключений
Не відображати останнього імені користувача у діалозі входу	Включено
Дозволити завершення роботи системи без виконання входу в систему	Відключений

Після налаштування параметрів безпеки завершити сеанс і знову увійдіть в систему під тим же ім'ям. Подивіться, як змінився процес входу в систему.

3. Переглядач журналів

Для перегляду системних журналів виконайте команду *Пуск*→ *Налаштування*→ *Панель управління*→ *Адміністрування*→ *Перегляд подій*. На екрані з'явиться вікно "*Перегляд подій*", зображене на рис.5.

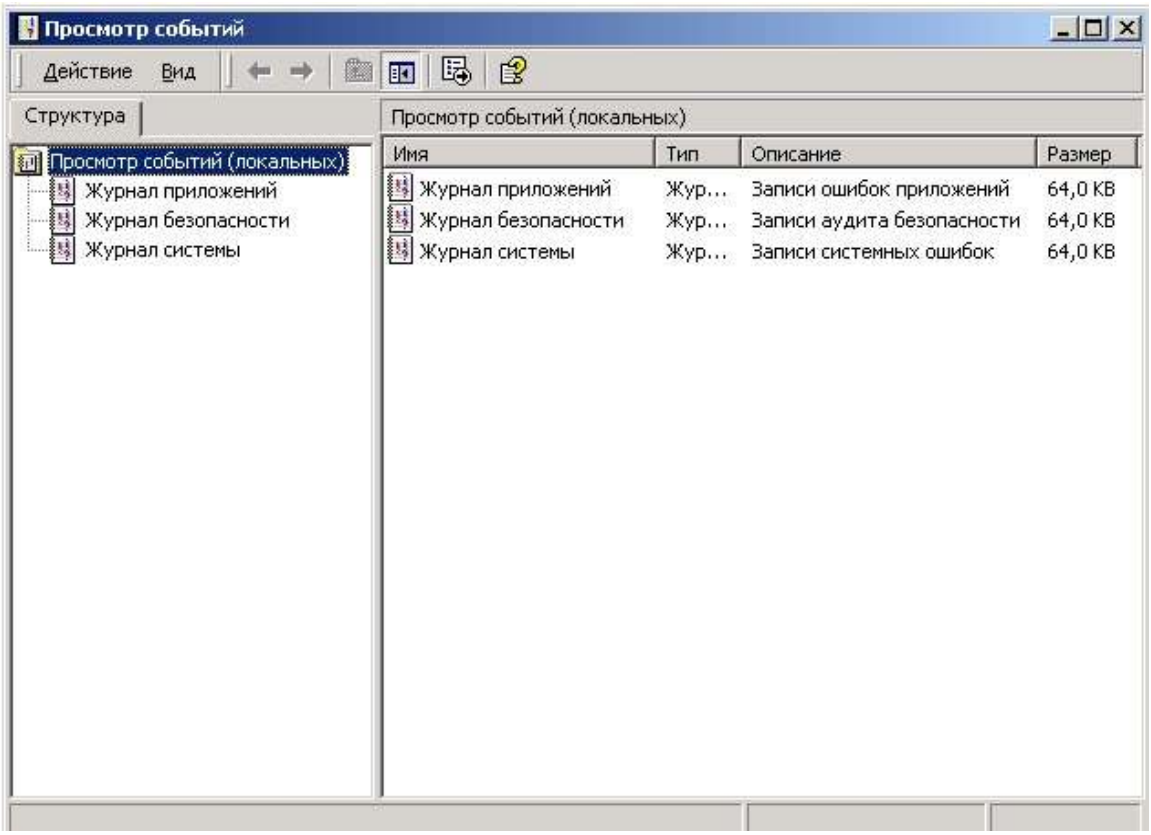


Рис.5. Вікно "*Перегляд подій*".

Перегляньте журнал додатків, журнал системи та журнал безпеки. Зверніть увагу, чи була внесена в журнал безпеки запис про ваш вході в систему. Якщо була, то це означає, що ви успішно налаштували аудит входу в систему.

4. Шифрування об'єктів файлової системи

Зашифруйте вміст каталогу **C: \ KIT**. Для цього клацніть на ньому правою кнопкою миші і в контекстному меню виберіть пункт "*Властивості*". Відкриється вікно властивостей об'єкта (рис.6). У цьому вікні натисніть кнопку "*Інші ...*".

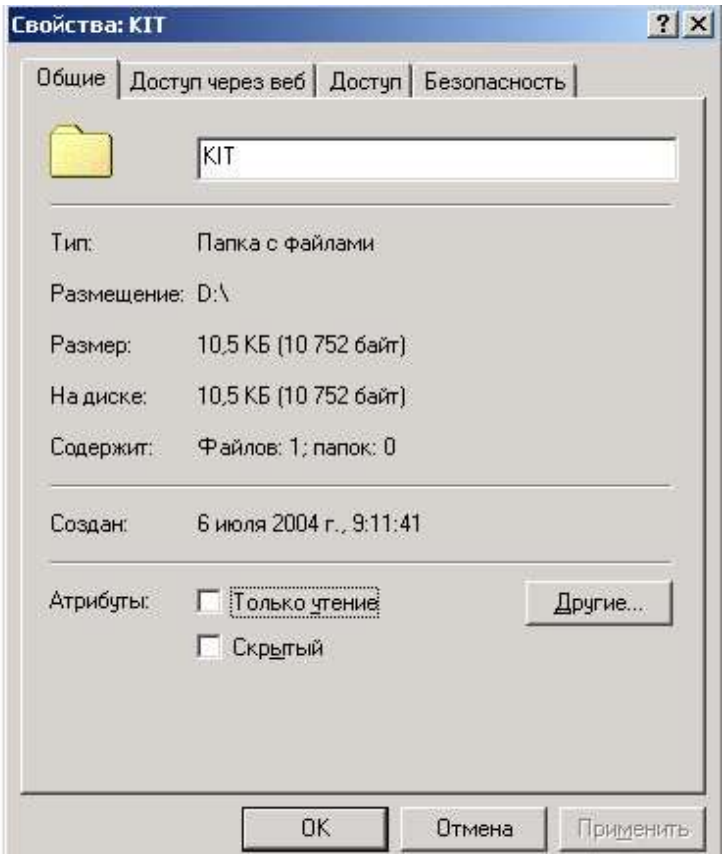


Рис.6. Вікно властивостей об'єкта.

Відкриється вікно додаткових атрибутів об'єкта (рис.7), в якому встановіть параметр "*Шифрувати вміст для захисту даних*"Та натисніть кнопку"*ОК*".

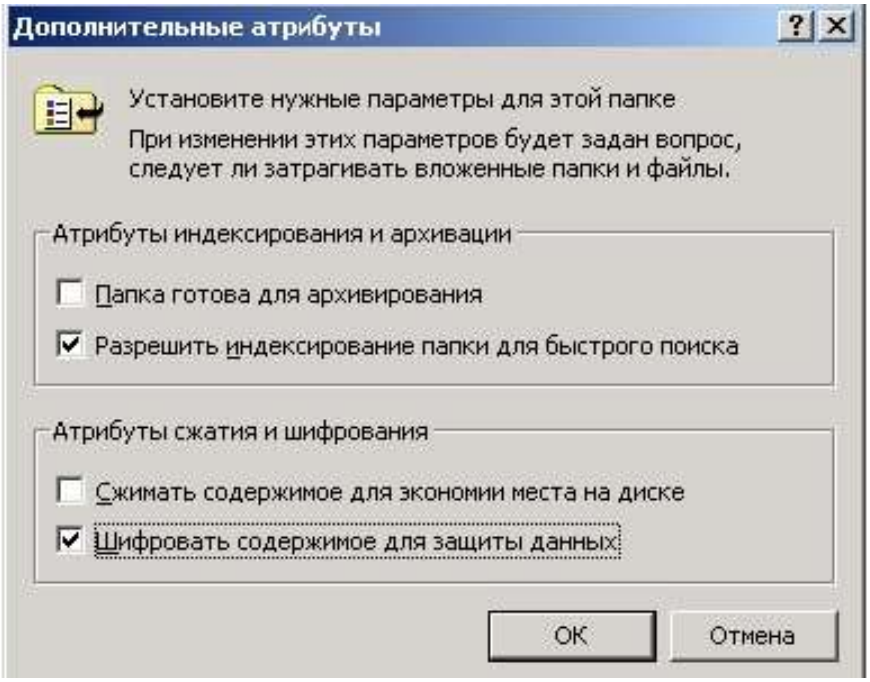


Рис.7. Вікно додаткових атрибутів об'єкта.

У вікні підтвердження (рис.8) виберіть параметр "*До цієї папки та всіх вкладених папок і файлів*"Та натисніть кнопку"*ОК*". У вікні властивостей об'єкта також натисніть кнопку"*ОК*". Папка буде зашифрована.

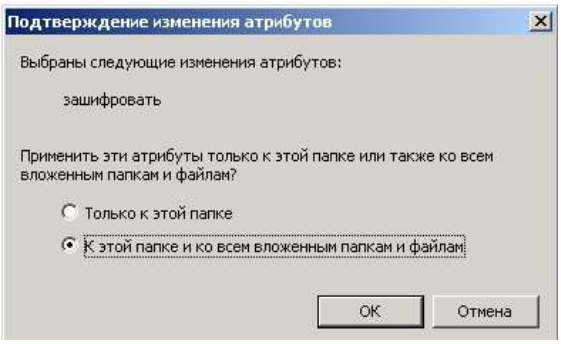


Рис.8. Вікно підтвердження зміни атрибутів об'єкта.

Щоб подивитися, як впливає шифрування на доступність об'єктів файлової системи для інших користувачів, вийдіть із системи та ввійдіть під ім'ям будь-якого із створених вами користувачів. Згідно з дозволами NTFS всі вони мають повний доступ до цієї папки. Ви побачите, що всі користувачі можуть відкрити папку. Однак спробуйте відкрити будь-який з файлів, і ви побачите повідомлення про те, що у вас немає доступу.

У той же час ви можете перейменувати або видалити будь-який із зашифрованих файлів. Це підтверджує те, що шифрована файлова система не змінює прав на доступ до файлу, вона тільки зашифровує дані файлу.

5. Експорт сертифікату та закритого ключа шифрованого файлової системи

Експортуйте сертифікат і закритий ключ шифрованого файлової системи у файл на диску, щоб у разі видалення ключа в локальному сховищі сертифікатів можна було розшифрувати дані.

Відкрийте папку **C:\inetsdk\bin**. Запустіть на виконання утиліту **certmgr.exe** (менеджер сертифікатів). Відкрийте сховище сертифікатів *Приватні.* Перегляньте що знаходяться в ньому

сертифікати. Ви побачите сертифікат, для якого буде вказано призначення "*Шифрована файлова система*" і постачальник "*EFS File Encryption Certificate*" (Рис.9).

Експортуйте сертифікат і відповідний йому закритий ключ у свою робочу папку під ім'ям **EFS.pfx**.

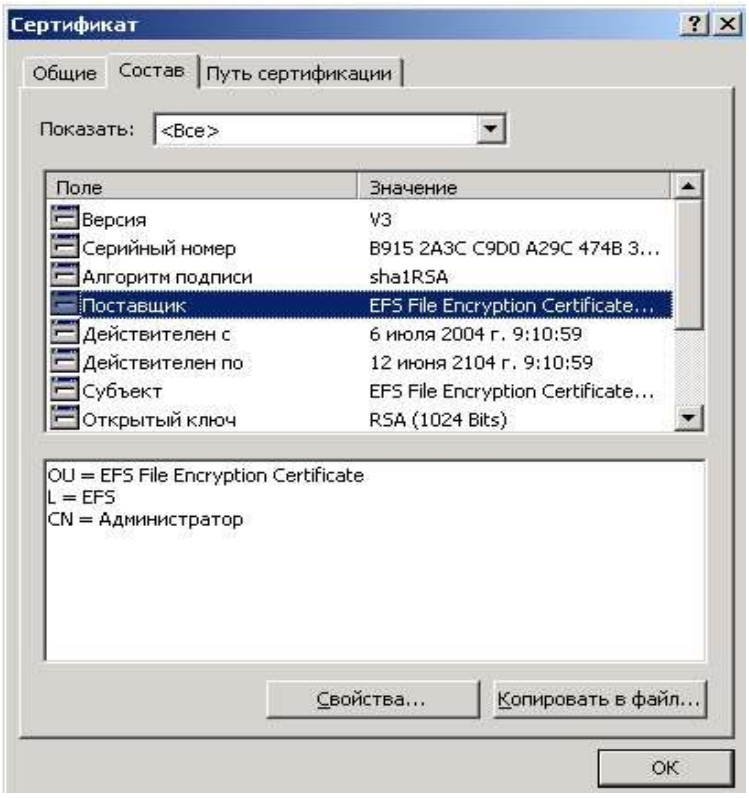


Рис.9. Сертифікат шифрованого файлової системи.

6. Розшифровка зашифрованих даних

Розшифруйте вміст каталогу **C: \ KIT**. Для цього клацніть на ньому правою кнопкою миші і в контекстному меню виберіть пункт "*Властивості*". Відкриється вікно властивостей об'єкта. У цьому вікні натисніть кнопку"*Інші ...*". Відкриється вікно додаткових атрибутів об'єкта, в якому зніміть прапорець "*Шифрувати вміст для захисту даних*" та натисніть кнопку "*ОК*". У вікні підтвердження виберіть параметр "*До цієї папки та всіх вкладених папок і файлів*" та натисніть кнопку"*ОК*". У вікні властивостей об'єкта також натисніть кнопку "*ОК*". Папка буде розшифровано.

Контрольні питання до лабораторної роботи

Питання, які ви повинні вивчити до лабораторної роботи 1.

Які два варіанти налаштування входу в систему ви знаєте?

2. Які стандартні групи користувачів передбачає операційна система Windows 2000? Які права доступу мають члени кожної з цих груп?
3. За яким принципом побудована робота шифрованого файлової системи (EFS)? Як здійснюється шифрування і розшифрування даних?
4. Як EFS розшифровує дані у разі втрати закритого ключа користувача? Завдяки чому це можливо?

Питання, які ви вивчите при виконанні лабораторної роботи

1. Як створити резервну копію даних стану операційної системи? Яку програму слід використовувати для створення резервної копії?
2. Як створити обліковий запис для нового користувача? Які дані необхідно ввести при створенні облікового запису?
3. Як встановити дозволи на доступ до папки або файлу за використання файлової системи NTFS? Як скасувати успадкування дозволів від батьківського об'єкта?
4. Як впливає на доступ до об'єкта встановлення таких дозволів: "**читання**","**читання і виконання**","**запис**", **змінити**"?
5. Для чого в політиці безпеки встановлюють параметр "**Вимкнути CTRL + ALT + DEL запит на вхід в систему**"?
6. Що таке аудит? Для чого система веде журнал аудиту?
7. Як переглянути системні журнали? Яка інформація зберігається в кожному з журналів?
8. Як зашифрувати або розшифрувати каталог або файл?
9. Що може зробити з зашифрованих файлом користувач, якому дозволу NTFS дають повний доступ до файлу, якщо він не має закритого ключа?
10. Як видалити обліковий запис користувача?