МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

**ОСНОВИ СИСТЕМНОГО АДМІНІСТРУВАННЯ**

**МЕТОДИЧНІ ВКАЗІВКИ**

до виконання лабораторних робіт

з дисципліни «Основи системного адміністрування»

Львів – 2019

**ЛАБОРАТОРНА РОБОТА № 1**

**Тема роботи:** Управління дисками в Windows 10, створення програмних RAID-масивів.

**Мета роботи:** Вивчити принципи роботи файлових систем FAT та NTFS в ОС Windows 10; навчитись управляти дисковим простором та створювати програмні RAID масиви на динамічних дисках у Windows 10.

**ТЕОРЕТИЧНІ ВІДОМОСТІ**

**Файлові системи, диски і томи**

Комп’ютери на основі архітектури х86 для управління дисками завжди використовують головний завантажувальний запис (Master Boot Record, MBR). MBR містить таблицю розділів (partition table), що описує розбиття диску.

Системи Windows підтримують файлові системи FAT-12, FAT-16, FAT-32 і NTFS. Крім того, дві файлові системи підтримуються на пристроях CD-ROM та DVD: Compact Disc File System (CDFS) і Universal Disk Format (UDF). На вибір файлової системи впливають наступні фактори:

* мета, для якої використовуватиметься комп’ютер;
* апаратна платформа;
* кількість жорстких дисків та їх об’єм;
* вимоги до безпеки;
* прикладні програми, що використовуються в системі.

**Файлові системи FAT**

FAT (найчастіше під цим терміном розуміють FAT-16) – це проста файлова система, розроблена для невеликих дисків і простих структур каталогів. Її назва походить від назви методу організації файлів – таблиця розміщення фалів (File Allocation Table, FAT). Ця таблиця міститься на початку тому. З метою захисту тому на ньому зберігається дві копії FAT. Таблиця розміщення файлів та кореневий каталог повинні міститись за строго фіксованими адресами, щоб файли, необхідні для запуску системи, були коректно розміщені.

Початково компанія Microsoft розробила FAT для управління файлами на дискетах, і тільки потім прийняла її в я кості стандарту для управління дисками в MS-DOS. Спочатку для дискет і невеликих жорстких дисків (менше 16 Мбайт) використовувалась 12-розрядна версія FAT (так звана FAT-12). В MS-DOS 3.0 була уведена 16-розрядна версія FAT для більших дисків. У Windows XP, 10 2003 система FAT-12 застосовується тільки на гнучких дисках і томах, розміром менше 16 Мбайт.

Підтримка файлової системи FAT-16 включена також у Windows XP, 10, оскільки вона сумісна з більшістю операційних систем інших виробників. Крім того, використання FAT-16 забезпечує можливість оновлення більш ранніх версій операційних систем родини Windows.

**Файлова система FAT-32**

32-розрядна файлова система FAT-32 з’явилась у Windows 95 OSR2 і підтримується в системах Windows 98/ME та Windows 2000/XP/10/Server 2003. Вона забезпечує оптимальний доступ до жорстких дисків, підвищує швидкість і продуктивність усіх операцій вводу/виводу. FAT-32 це вдосконалена версія FAT, призначена для використання на томах розміром більше 2 Гбайт. У Windows XP, 10 та Windows Server 2003 система FAT-32 застосовується для форматування дисків DVD-RAM.

Для забезпечення максимальної сумісності з існуючими прикладним програмами, мережами і драйверами пристроїв FAT-32 була реалізована з мінімумом можливих змін в архітектурі та внутрішніх структурах даних. Усі утиліти Microsoft, призначені для роботи з дисками (Format, Fdisk, Defrag і ScanDisk), були перероблені для забезпечення підтримки FAT-32. В табл. 1 представлені порівняльні характеристики FAT-16 і FAT-32.

Таблиця 1. Порівняння характеристик FAT-16 і FAT-32

|  |  |
| --- | --- |
| **FAT-16** | **FAT-32** |
| Підтримується більшістю ОС, серед яких MS-DOS, Windows 9х/МЕ, [Windows NT](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19632&displayformat=dictionary" \t "Словник основних термінів: Windows NT), Windows XP, 10, OS/2 і UNIX | Підтримується усіма ОС Windows, починаючи з Windows 95 OSR2; підтримкаFAT32 є також і на інших платформах |
| Ефективна тільки на логічних дисках, розмір яких не перевищує 256 Мбайт | Не підтримуються диски, розмір яких менше 32 Мбайт |
| Підтримує стиснення диску тільки за допомогою таких DOS-утиліт, як DrvSpace | Не підтримує стиснення диску |
| На практиці обмежена по розміру до 65524 кластерів. Обмеження по кількості кластерів та їх розміру (64 Кбайт) приводять до обмеження на розмір диску (не більше 4 Гбайт). Однак кластери розміром 64 Кбайт можуть невірно розпізнаватись деякими програмами і системами. Окрім цього, FAT-12/16 зазвичай має обмеження на розмір кореневого [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у (в залежності від диску – від 200 до 400 входжень) | Використовує кластери меншого розміру, в результаті чого дисковий простір використовується більш ефективно. Максимальний розмір кластера – 16 Кбайт, максимальний розмір тому, що можна відформатувати – 32 Гбайт; читання і запис підтримується на томах до 2 Тбайт |
| Оскільки зі збільшенням розміру диску розмір кластеру FAT-16 збільшується, збереження [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів на таких дисках стає неефективним через внутрішню фрагментацію | Для дисків розміром від 257 Мбайт до 8 Гбайт розмір кластеру становить 4 Кбайт |

FAT-32 забезпечує наступні переваги порівняно з попередніми реалізаціями FAT:

* Підтримка дисків розміром до 2 Тбайт. Однак команда Format, що є в складі Windows, не дозволяє форматувати томи FAT-32, розмір яких перевищує 32 Гбайт. Однак драйвер Fastfat, що входить до комплекту Windows, дозволяє підключати і підтримувати будь-які томи FAT-32, в тому числі і такі, розмір яких перевищує 32 Гбайт. За винятком цього обмеження FAT-32 у Windows ХР/10/Server 2003 працює так само, як і в Windows 9х/МЕ.
* Більш ефективне використання дискового простору. FAT-32 використовує менші кластери (див. табл. 5), що дозволяє підвищити ефективність використання дискового простору на 10–15% порівняно з FAT.
* Підвищена надійність та швидше завантаження програм. На відміну від FAT-12 і FAT-16, FAT-32 має можливість розміщувати кореневий каталог в будь-якій області тому. Крім того, завантажувальний сектор FAT-32 було розширено порівняно з FAT-16, і він містить резервні копії життєво важливих структур даних. Підвищена стійкість FAT-32 обумовлена саме цими факторами.

**Файлова система NTFS**

Файлова система Windows NT (NTFS) забезпечує таке поєднання продуктивності, надійності та ефективності, якого неможливо досягти за допомогою будь-якої з реалізацій FAT (як FAT-16, так і FAT-32). Основними цілями розробки NTFS були забезпечення швидкісного виконання стандартних операцій над файлами (включно з читанням, записом та пошуком) та надання додаткових можливостей, включаючи стиснення та відновлення пошкодженої файлової системи на великих дисках.

NTFS володіє характеристиками захищеності, забезпечуючи контроль доступу до даних та привілеї власника, що відіграють винятково важливу роль в забезпеченні цілісності життєво важливих конфіденційних даних. Каталоги і файли NTFS можуть мати призначені їм права доступу незалежно від того, чи є вони спільними чи ні. NTFS – єдина файлова система у Windows NT/2000/XP /10 та Windows Server 2003, яка дозволяє призначати права доступу до окремих файлів. Однак, якщо файл буде скопійовано з розділу чи тому NTFS в розділ чи на том FAT, усі права доступу та інші унікальні атрибути, властиві NTFS, будуть втрачені.

У Windows 2000 була введена нова версія NTFS – NTFS 5.0. Нові структури даних, що з’явились в складі цієї реалізації, дозволяють використовувати оригінальні можливості Windows 2000, наприклад, квоти на використання диску для кожного користувача, шифрування файлів, відстеження посилань, точки з’єднання (junction points), вбудовані набори властивостей (native property sets). Крім того, додавати додатковий дисковий простір до томів NTFS 5.0 можна без перевантаження.

NTFS – найкращий вибір для роботи з томами великого об’єму. При цьому слід врахувати, що якщо до системи висуваються підвищені вимоги (до числа яких відносяться забезпечення безпеки та застосування ефективного алгоритму стиснення), то частину з них можна реалізувати тільки за допомогою NTFS. Тому в ряді випадків треба використовувати NTFS навіть на невеликих томах.

NTFS – єдина файлова система, на яку можна встановлювати систему, що відіграє роль контролера домену (на базі Active Directory).

**Обмеження файлових систем та питання сумісності**

В наведених нижче таблицях (табл. 2 і 3) зібрані дані про сумісність файлових систем NTFS і FAT, а також обмеження, що накладаються на кожну з цих файлових систем. Таблицею сумісності обов’язково слід користуватись при створенні систем з множинним завантаженням.

Таблиця 2. Підтримка файлових систем операційними системами

|  |  |  |  |
| --- | --- | --- | --- |
| [Операційна система](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19631&displayformat=dictionary) | [Файлова система](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19639&displayformat=dictionary) | | |
| **FAT** | **FAT-32** | **NTFS** |
| MS-DOS, Windows 3.1 х та Windows 95 (версії до OSR2) | + | – | – |
| Windows 95 OSR2, Windows 98 та Windows ME | + | + | – |
| [Windows NT](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19632&displayformat=dictionary) 4.0 | + | – | + |
| Windows 2000/XP/10/Server 2003 | + | + | + |

Таблиця 3. Обмеження файлових систем у Windows

|  |  |  |
| --- | --- | --- |
| **Обмеження** | **NTFS** | **FAT і FAT-32** |
| Розміри тому | Мінімальний розмір тому складає (фактично) приблизно 10 Мбайт.  На практиці рекомендується створювати томи, розмір яких не перевищує 256 Тбайт мінус 64 Кбайт.  За допомогою NTFS не можна форматувати дискети | FAT підтримує різні розміри томів – від об’єму дискет до 4 Гбайт (томи розміром більше 2 Гбайт можуть не підтримуватись іншими системами).  FAT-32 підтримує томи об’ємом від 32 Мбайт до 2 Тбайт. Під управлінням Windows XP, 10,  можна форматувати томи FAT-32, об’єм яких не перевищує 32 Гбайт |
| Розміри [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів | Практичний максимум 16 Тбайт мінус 64 Кбайт | FAT і FAT-32 підтримують [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)и розміром не більше 4 Гбайт |

**Розміри кластерів**

При форматуванні дискові томи розмічаються на кластери – це мінімальний простір, що виділяється на диску для файлів. Для будь-якої файлової системи розмір кластеру за замовчуванням визначається розміром тому. У табл. 4 наведено порівняльні розміри кластерів для FAT-16, FAT-32 і NTFS залежно від розміру диску.

Таблиця 4. Розміри кластерів за замовчуванням для FAT-16, FAT-32 та NTFS у Windows

|  |  |  |  |
| --- | --- | --- | --- |
| **Розмір диску** | **Розмір кластеру FAT-16** | **Розмір кластеру FAT-32** | **Розмір кластеру NTFS** |
| До 32 Мбайт включно | 512 байт | Не підтримується | 512 байт |
| 33–64 Мбайт | 1 Кбайт | 512 байт | 512 байт |
| 65–128 Мбайт | 2 Кбайт | 1 Кбайт | 512 байт |
| 129–256 Мбайт | 4 Кбайт | 2 Кбайт | 512 байт |
| 257–512 Мбайт | 8 Кбайт | 4 Кбайт | 512 байт |
| 513–1024 Мбайт | 16 Кбайт | 4 Кбайт | 1 Кбайт |
| 1–2 Гбайт | 32 Кбайт | 4 Кбайт | 2 Кбайт |
| 2–4 Гбайт | 64 Кбайт | 4 Кбайт | 4 Кбайт |
| 4–8 Гбайт | Не підтримується | 4 Кбайт | 4 Кбайт |
| 8–16 Гбайт | Не підтримується | 8 Кбайт | 4 Кбайт |
| 16–32 Гбайт | Не підтримується | 16 Кбайт | 4 Кбайт |
| Від 32 Гбайт | Не підтримується | Не підтримується | 4 Кбайт |

**Можливості і використання NTFS 5.0**

Тільки система NTFS дозволяє повною мірою використовувати усі засоби Windows ХР/10/Server 2003, що забезпечують безпеку та надійність зберігання даних на дискових накопичувачах. NTFS 5.0 дозволяє реалізовувати наступні можливості.

* Механізм дозволів на доступ до файлів і каталогів. Забезпечує гнучку систему обмежень для користувачів і груп.
* Стиснення файлів і каталогів. Вбудовані засоби стиснення даних дозволяють економити простір на дисках, при цьому всі процедури виконуються "прозоро" для користувача.
* Шифрування даних. Encrypting File System (EFS, Шифрована файлова система) забезпечує конфіденційність збереженої інформації, причому у Windows Server 2003 виправлені деякі недоліки цього механізму, що допускали "витік інформації".
* Дискові квоти. Можна обмежити простір, щозаймають на томі окремі користувачі.
* Механізм точок повторної обробки (reparse points). Дозволяє, зокрема, реалізувати точки з’єднання (junction points), за допомогою яких цільовий каталог (диск) відображається в порожній каталог (ця процедура називається монтуванням диску), що знаходиться в просторі імен файлової системи NTFS 5.0 локального комп’ютера. Цільовим каталогом може служити будь-який допустимий шлях Windows ХР, 10.
* Розподілене відстеження посилань на файли. Цей механізм дозволяє зберегти посилання на файл актуальним, навіть якщо він був переіменований чи переміщений на інший том, розміщений на тому ж комп’ютері або на іншому комп’ютері в межах домену.
* Розріджені (sparse) файли. NTFS ефективно зберігає такі файли, що містять велику кількість послідовних порожніх байтів.
* Журнал змін (change journal), де реєструються усі операції доступу до файлів і томів.

Порівняно з Windows 2000, системи Windows XP/10/Server 2003 мають наступні покращення в роботі з NTFS:

* за інформацією компанії Microsoft, на 5–8 відсотків збільшена швидкодія, і NTFS забезпечує практично таку ж продуктивність, як і FAT;
* швидше виконується перетворення систем з використанням команди Convert.exe. При цьому можуть бути задіяні різні, а не фіксовані розміри кластерів, до 4 Кбайт;
* на перетворені з FAT в NTFS томи встановлюються дозволи, прийняті на томах, що безпосередньо форматуються в NTFS;
* реалізовано нові можливості для дефрагментації.

Засоби NTFS 5.0 дозволяють більш ефективно вирішувати багато задач програмування. За допомогою цієї системи можна подолати ряд проблем, що виникають дотепер при роботі з іншими файловими системами.

Основою файлової системи NTFS є файл, що називається головною таблицею файлів (Master File Table, MFT). Він створюється при форматуванні тома для NTFS. MFT складається з масиву записів розміром 1 Кбайт. Кожен запис ідентифікує один файл, що розташовано на диску. При створенні файлу система NTFS знаходить порожній запис в MFT, потім заповнює його інформацією про створюваний файл. Зміст інформації, що записується в MFT, наведено в табл. 5.

Таблиця 5. Склад інформації, що записується в MFT

|  |  |
| --- | --- |
| **Тип інформації** | **Опис** |
| Стандартна інформація | Атрибути [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у, наприклад, "тільки читання", "прихований" і "системний"; час створення, останнього доступу, останньої зміни; лічильник жорстких зв’язків [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у |
| Ім’я | Ім’я [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у чи [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у в кодуванні Unicode. Якщо ім’я [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у не відповідає схемі 8.3 або [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary) має жорсткі зв’язки, атрибутів імені [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у може бути декілька |
| Дескриптор безпеки | Структура, що зберігає дані безпеки, асоційовані з [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ом, що управляють доступом [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а до [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у |
| Дані | Вміст [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у; [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)и не мають цього типу інформації |

NTFS оцінює розмір записуваної в MFT інформації. Якщо він не перевищує 1 Кбайт, інформація зберігається в запису MFT. Ці дані зберігаються в оперативній пам’яті і є резидент ними атрибутами файлу. В іншому випадку інформацію записується на диск, утворюючи нерезидентні атрибути файлу, а в запис MFT вміщується вказівник на відповідну область диску.

Оскільки операційні системи Windows 2000/2003/ХР/10 широко використовують механізм доступу до ресурсів за допомогою ярликів, на жорсткому диску зберігається велика кількість файлів з розширенням lnk. Крім того, на диску знаходиться багато файлів Desktop.ini. Описана схема зберігання інформації файлів в MFT дозволяє тримати дані невеликих файлів в оперативній пам’яті, що різко підвищує продуктивність файлової системи.

**Розділи і томи**

На відміну від ранніх операційних систем виробництва компанії Microsoft, що дозволяють використовувати фізичні диски тільки в базовому режимі зберігання інформації (basic storage), в системах Windows 2000/XP/10 існує новий тип зберігання інформації – диски з динамічним режимом зберігання даних (dynamic storage). Диск, ініціалізований для динамічного режиму зберігання, називається динамічним диском (dynamic disk).

Використовуючи динамічні диски, можна без перевантаження операційної системи управляти дисками і томами, а також динамічно розширювати томи. Для клієнтських систем – це, мабуть, єдина перевага динамічних дисків, однак і та не дуже цінна, оскільки на робочих станціях диск звичайно один і розмічається "раз і назавжди". Тому ефект від використання динамічних дисків можна в першу чергу одержати на серверних платформах, що мають складну дискову конфігурацію. Дискова система цих систем може складатися з будь-якої комбінації базових і динамічних дисків. Проте том, що складається з декількох дисків, повинен мати один режим зберігання даних.

У табл. 6 перераховані основні поняття для базових і динамічних дисків: поняттю, вказаному в одній колонці таблиці, відповідає логічний еквівалент з сусідньої колонки того ж рядка.

Таблиця 6. Організація базових і динамічних дисків

|  |  |
| --- | --- |
| **Базовий диск** | **Динамічний диск** |
| Системний (system partition) і завантажувальний розділи (boot partition) | Системний (system volume) і завантажувальний томи (boot volume) |
| Основний розділ (primary partition) | Простий том (simple volume) |
| Додатковий розділ (extended partiotion) | Прості томи і вільний простір диску |
| Логічний диск (logical drive) | Простий том |
| Набір томів (volume set) | Складений том (spanned volume) |
| Почерговий набір (stripe set without parity) | Почерговий том (stripped volume) |
| Дзеркальний набір (mirror set) | Дзеркальний том (mirrored volume) |
| Почерговий набір з парністю (stripe set with parity) | Том RAID-5 (RAID-5 volume) |

**Базовий режим зберігання інформації**

Розділом є частина базового диску, що функціонує як логічна автономна одиниця.

Основний розділ (primary partition) зарезервований для використання операційною системою. Кожен фізичний диск може мати до чотирьох основних розділів (або до трьох, якщо створений додатковий розділ).

Додатковий розділ (extended partition) створюється з використанням вільного простору диска, що залишився, і може бути розділений на логічні диски. На кожному фізичному диску може бути тільки один додатковий розділ.

Базові диски підтримуються MS-DOS і будь-якими системами Windows, отже тільки їх можна використовувати в конфігураціях з множинним завантаженням.

Системи Windows ХР, 10 і Windows Server 2003 не підтримують створені в Windows NT 4.0 багатодискові базові конфігурації: набори томів, дзеркальні і почергові набори, а також почергові набори з парністю. У цих системах (на дисках з MBR) з базовими дисками можливі наступні операції:

* + - * створення основних розділів і додаткового розділу (4 основних або 3 основних і один додатковий на кожному диску);
      * створення логічних дисків (у додатковому розділі);
      * розширення базового тому за допомогою команди DiskPart.exe (див. подробиці цієї операції в довідковій системі).

Базовий диск у будь-який момент можна перетворити на динамічний без втрати інформації. Зворотна процедура вимагає попередньої архівації даних на всіх дисках, оскільки вся інформація на диску при цьому втрачається.

**Динамічний режим зберігання інформації**

Динамічний диск ділиться не на розділи, а на томи. Том складається з одного або декількох фізичних дисків в одній з наступних конфігурацій:

* простий том;
* почерговий том;
* складений том;
* том RAID-5;
* дзеркальний том.

Базовий диск у будь-який момент може бути перетворений на динамічний диск без втрати інформації; зворотне перетворення приводить до втрати даних.

Відмовостійкі томи – дзеркальні і томи RAID-5 – підтримуються тільки на серверних платформах (Windows 2000 Server і Windows Server 2003). Проте системи Windows 2000 Professional і Windows ХР, 10 можна використовувати для віддаленого адміністрування таких томів.

Динамічні диски недоступні для комп'ютерів під управлінням MS-DOS, Windows 95, Windows 98, Windows ME, Windows NT 4.0 і Windows XP Home Edition, Windows 10.

Динамічні диски не підтримуються на портативних комп'ютерах, змінних (removable) і переносимих (detachable) дисках (підключених по шинам USB або IEEE 1394 (FireWire).

Не перетворюйте базові диски в динамічні, якщо на цих дисках є інші інсталяції Windows 2000, Windows ХР, 10 або Windows Server 2003 – після перетворення ці системи не зможуть завантажуватися. На одному динамічному диску може бути встановлена тільки одна операційна система (з перерахованих).

Виконати нову інсталяцію Windows Server 2003 можна тільки на динамічний том, який був перетворений з базового завантажувального або системного (що містить файли операційної системи) тому. Якщо динамічний том був створений з вільного простору, то встановлювати систему на нього не можна.

Вільний простір – це невикористана і неформатована частина жорсткого диску, яка може бути задіяна при створенні томів.

Системний том містить файли, жорстко прив'язані до устаткування (Ntldr, Boot.ini, Ntdetect.com), необхідні для завантаження системи.

Завантажувальний том містить файли операційної системи Windows, розташовані в папках %SystemRoot% і %SystemRoot%\system32.

Том – це логічна одиниця зберігання, утворена з вільного (unallocated) простору на одному або декількох дисках. Том можна відформатувати засобами файлової системи з призначенням йому імені (літери) або змонтувати як папку наявного тому. На динамічних дисках зазвичай використовується NTFS, проте за допомогою команди Format том можна відформатувати під FAT16 або FAT32. Томи на динамічних дисках можуть мати одну з декількох структур: простий, складений, дзеркальний, почерговий том і том RAID-5.

**Простий том** використовує простір одного фізичного диску. Це може бути одна ділянка на диску або декілька ділянок, сполучених одна з одною. Простий том може бути розширений в межах одного диску або на додатковий диск. Якщо простий том розширюється на декілька дисків, він стає складеним томом. Розширювати допускається тільки прості томи, відформатовані у файловій системі NTFS. Простий том не забезпечує відмовостійкості.

**Складений том** складається із зв'язаного разом простору декількох дисків (до 32 дисків). Він може бути розширений на додаткові диски і не може брати участь в дзеркальних системах. Складені томи створюються, коли на жодному жорсткому диску немає достатнього вільного простору. Ви можете розширити існуючий складений том з файловою системою NTFS, додавши до нього вільний простір. Не допускається розширювати: томи з файловою системою FAT або FAT32, системний том, завантажувальний том. Крім того, створюючи складені томи, можна розподіляти навантаження на дискові системи. Складені томи не забезпечують відмовостійкості. Оскільки томи такого типу розташовані на декількох жорстких дисках, зростає імовірність їх відмови, пов'язаної з виходом з ладу одного з дисків.

**Дзеркальний том** – це засіб забезпечення відмовостійкості, для чого дані дублюються на двох фізичних дисках. Всі дані одного диску копіюються на додатковий диск, що забезпечує можливість отримання надлишковості даних. Якщо один з дисків відмовляє, дані можуть бути доступні на вцілілому диску дзеркала. Дзеркальний том не може бути розширений. Дзеркало також відоме як RAID-1. Дзеркальними можна робити практично будь-які томи, включаючи системний і завантажувальний.

Дані на **почерговому томі** розбиваються на блоки по 64 кбайт при запису і поміщаються на декілька фізичних дисків (до 32), причому інформація рівномірно розподіляється серед усіх дисків, що входять до складу такого тому. Такий підхід зручний при необхідності швидкого запису або читання з фізичних дисків великого об'єму інформації. Швидкість роботи з дисковою системою збільшується за рахунок розпаралелювання потоків даних і одночасного запису або читання інформації з дисків тому. "Розщеплювання" інформації також корисно при балансуванні навантаження вводу/виводу в розрахованих на багато користувачів додатках. Томи з чергуванням записуваної інформації не забезпечують відмовостійкість. Том такого типу не може входити в дзеркальний набір і його не можна розширити. Чергування даних відоме як RAID-0.

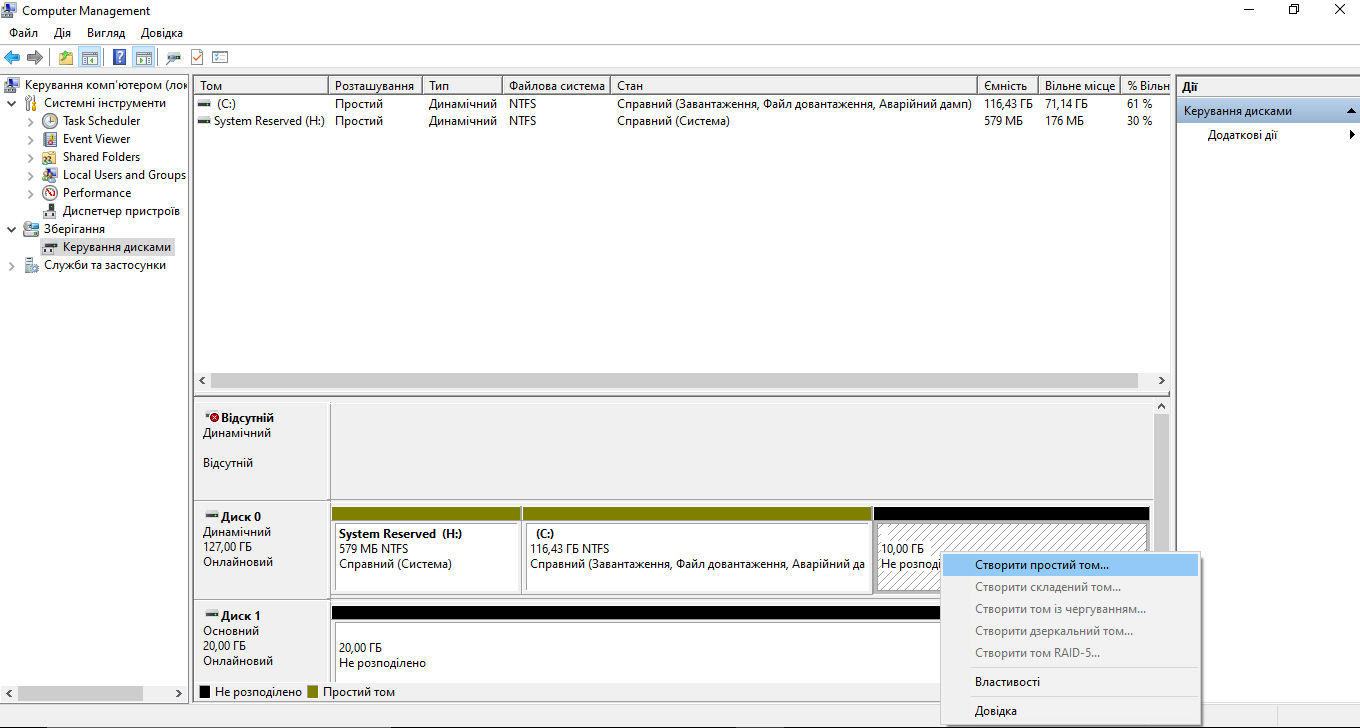
**Том RAID-5** є засобом забезпечення відмовостійкості дискової системи, оскільки такі томи розщеплюються при запису на три або більше дисків. Том RAID-5 забезпечує надлишковість інформації, завдяки підрахунку контрольної суми даних, розташованих на кожному диску. Контрольна сума (обчислювана величина, яка може бути використана для відновлення даних у разі їх руйнування) також розщеплюється і записується на всі диски масиву. Якщо відмовляє один з дисків масиву, то інформація, яка на ньому знаходилася, може бути відновлена з використанням даних працездатних дисків і контрольної суми. Том RAID-5 не може входити в дзеркальний набір і його не можна розширити.

**ЗАВДАННЯ ДО ВИКОНАННЯ РОБОТИ\***

**\*Використовувати своє ім’я або будь-який інакший ідентифікатор при іменуванні папок, файлів і т.д.**

1. Створити розширений розділ на першому жорсткому диску (рис. 1); створити 3 логічні диски в цьому розділі – файлова система FAT 32, розмір кластера 512 байт, 8 кБ, та 64 кБ відповідно.

Для цього необхідно створити новий том на нерозміченому диску, натиснувши правою кнопкою миші.

Рис. 1. Управління розділами у Windows 10

Відкриється майстер створення простих томів.

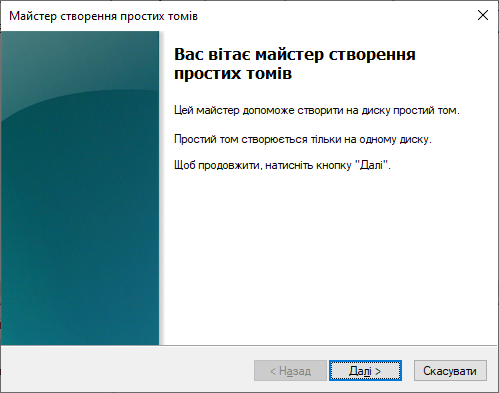


Рис. 2. Майстер створення простих томів

Після цього необхідно вказати розмір тому, що створюється, призначити йому букву і вказати налаштування форматування.

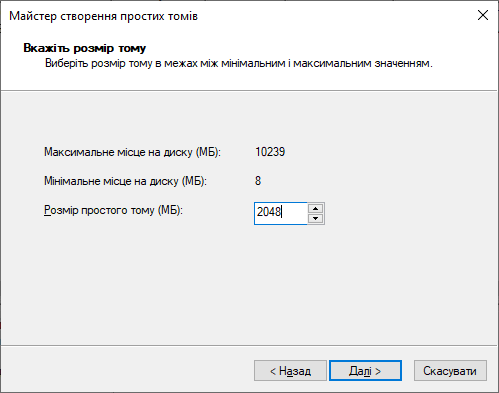


Рис. 3. Встановлення розміру тому

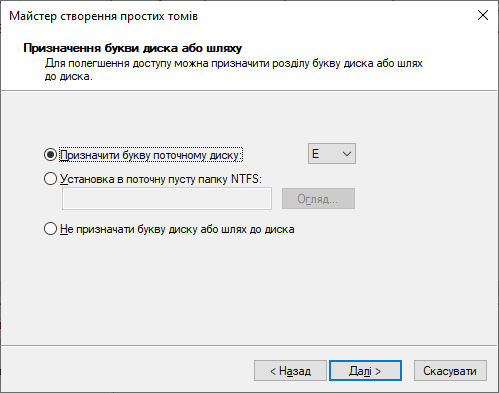


Рис. 4. Призначення тому букви

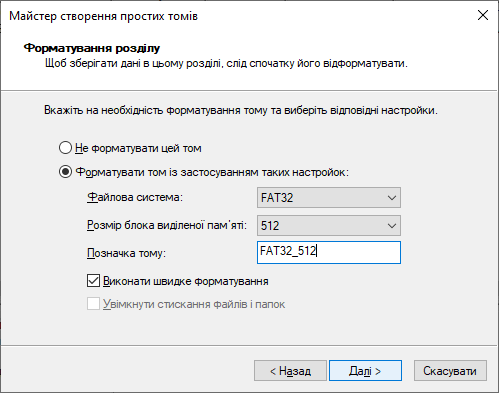


Рис. 5. Форматування розділу



Рис. 6. Завершення створення тому

Повторити аналогічні дії для створення кластерів на 8 кБ, та 64 кБ.

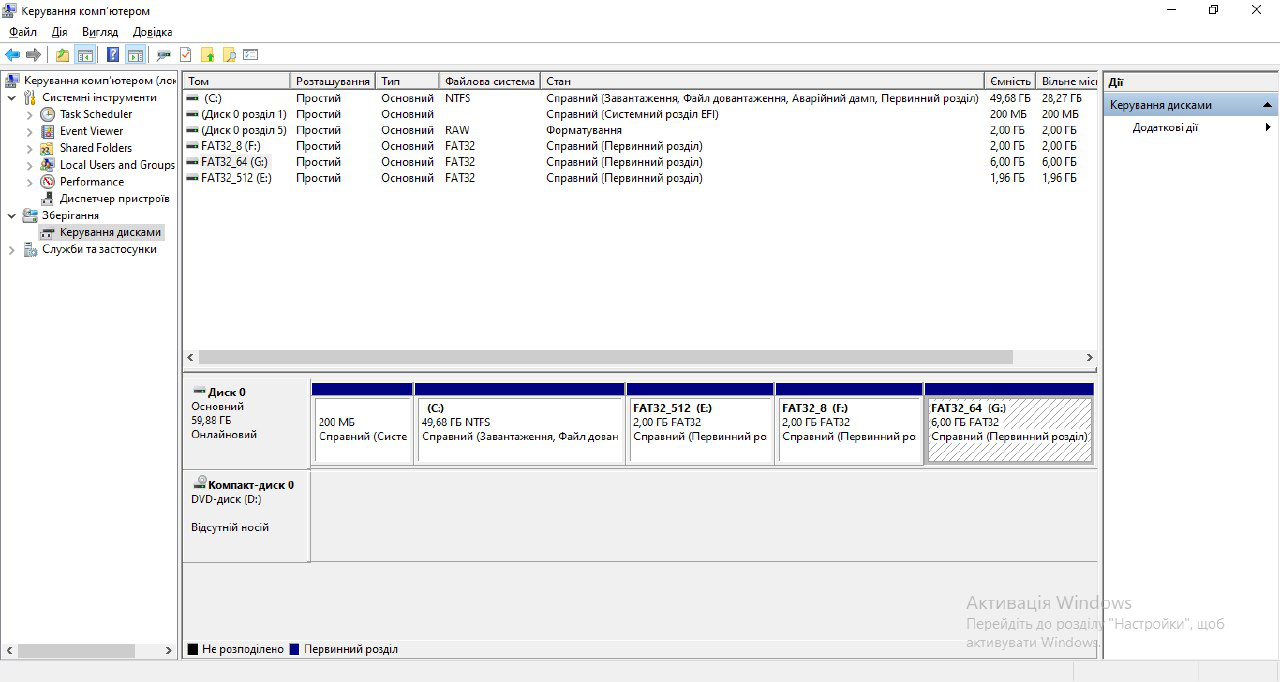
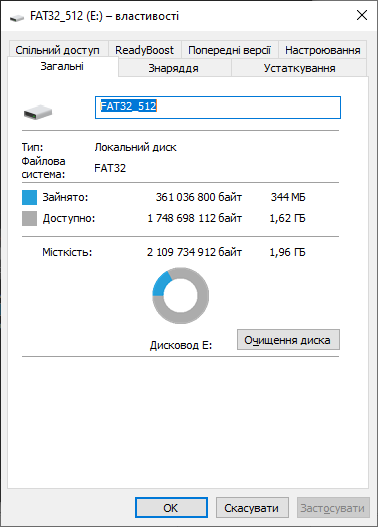
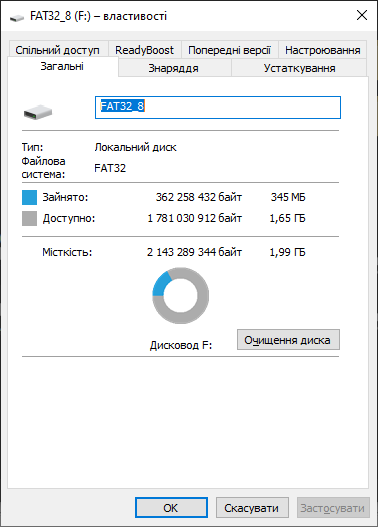


Рис. 7. Створені томи

1. Скопіювати папку, що містить велику кількість файлів невеликого розміру (наприклад c:\windows\fonts) на кожен з цих томів. Порівняти реальний розмір цієї папки на кожному томі (рис. 8).



(а)



(б)



(в)

Рис. 8. Кількість місця, що займає папка на диску, в залежності від розміру кластера (а – розмір кластера 512 байт, б – 8 кБ, в – 64 кБ).

1. Конвертувати файлову систему на цих томах в NTFS використовуючи утиліту convert.exe (рис. 9).

Запустивши командний рядок від імені адміністратора, переходимо у потрібний том за допомогою команди “ f: ”. Далі прописуємо команду “ convert f: /fs:ntfs /x ” і натискаємо Enter. Після цього буде необхідно ввести назву тому, задану при його створенні.

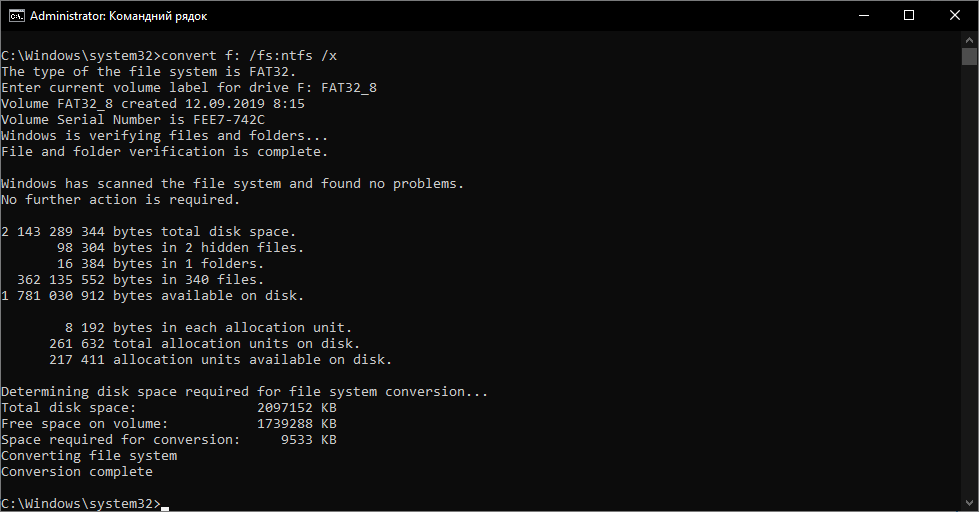


Рис. 9. Приклад роботи утиліти convert.exe.

Аналогічно конвертуємо файлові системи інших томів у NTFS.

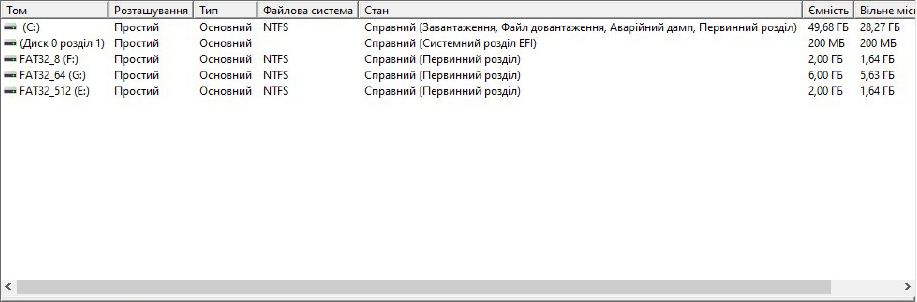


Рис. 10. Конвертація в NTFS

1. Створити на томі з файловою системою NTFS файл розміром 500–600 байт (наприклад текстовий документ). Переконатися, що кількість вільного/зайнятого місця на томі не змінилась (при необхідності дещо зменшити розмір файлу). Пояснити цей факт, чи буде такий самий ефект на томі з ФС FAT?

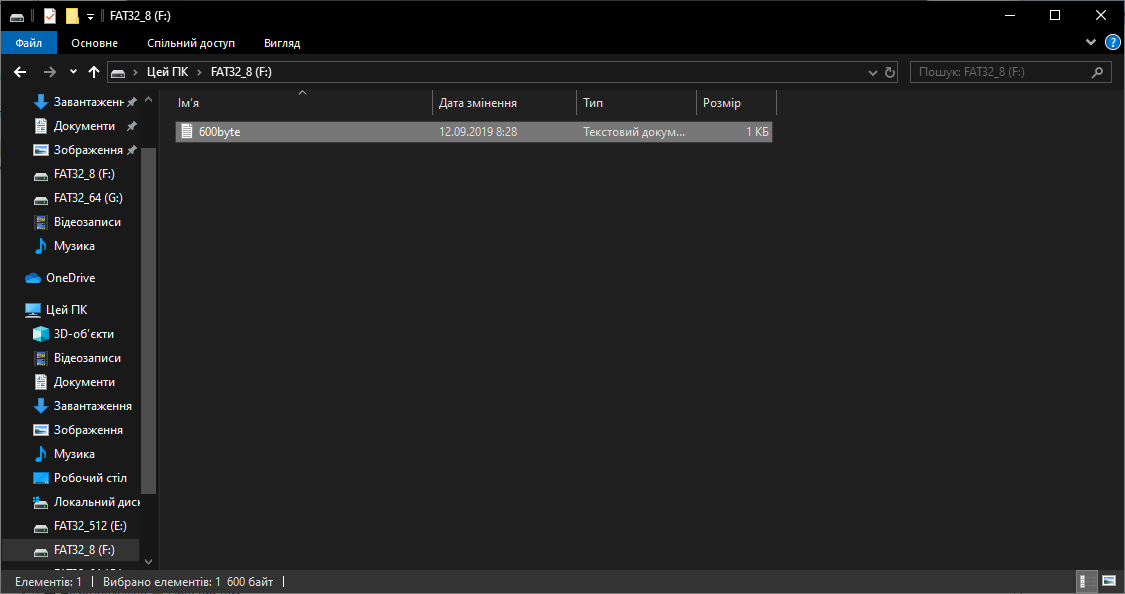


Рис. 11. Створення файлу

1. Створити на томі з ФС NTFS порожній файл. Записати якусь інформацію в іменований потік цього файлу (наприклад за допомогою команди echo або перенаправлення виводу іншого файлу в цей потік) – рис. 12. Переконатись, що хоча вільне місце на томі відображається коректно, розмір файлу "залишається" нульовим (незмінним) – рис. 13.

Запустивши командний рядок від імені адміністратора, переходимо до потрібного тому за допомогою команди “ f: ”. Далі прописуємо команду “ echo <текст> > <назва\_файлу>:stream ”.

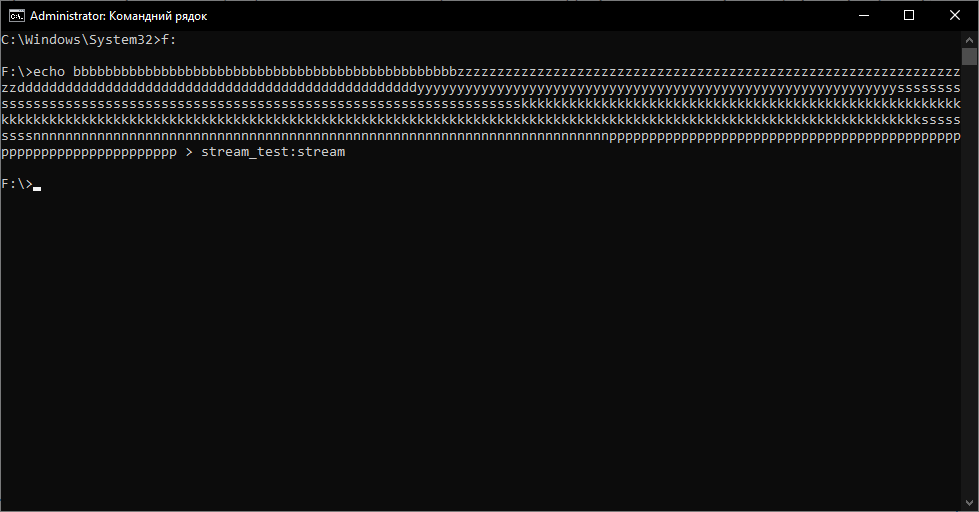


Рис. 12. Приклад використання іменованих потоків NTFS

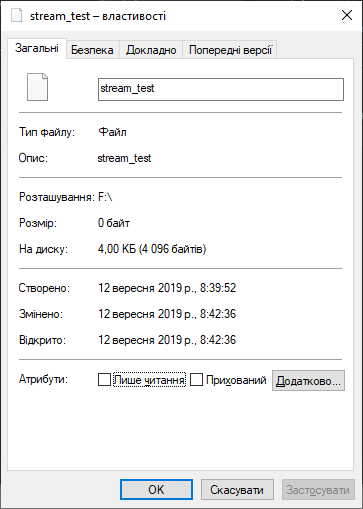


Рис. 13. Відображення системою розміру файлу з іменованими потоками NTFS

6. За допомогою оснастки «Керування дисками» перетворити базові диски в динамічні.

Для цього натискаємо правою кнопкою миші на диску і обираємо відповідний пункт.

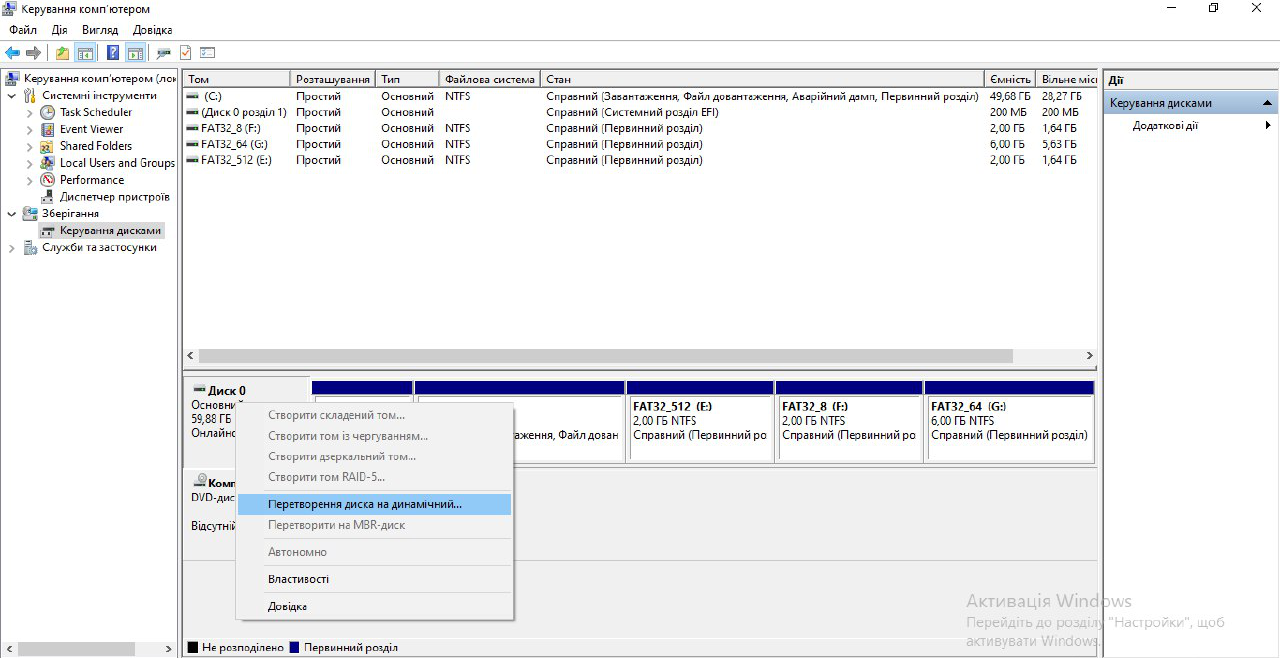


Рис. 14. Перетворення дисків

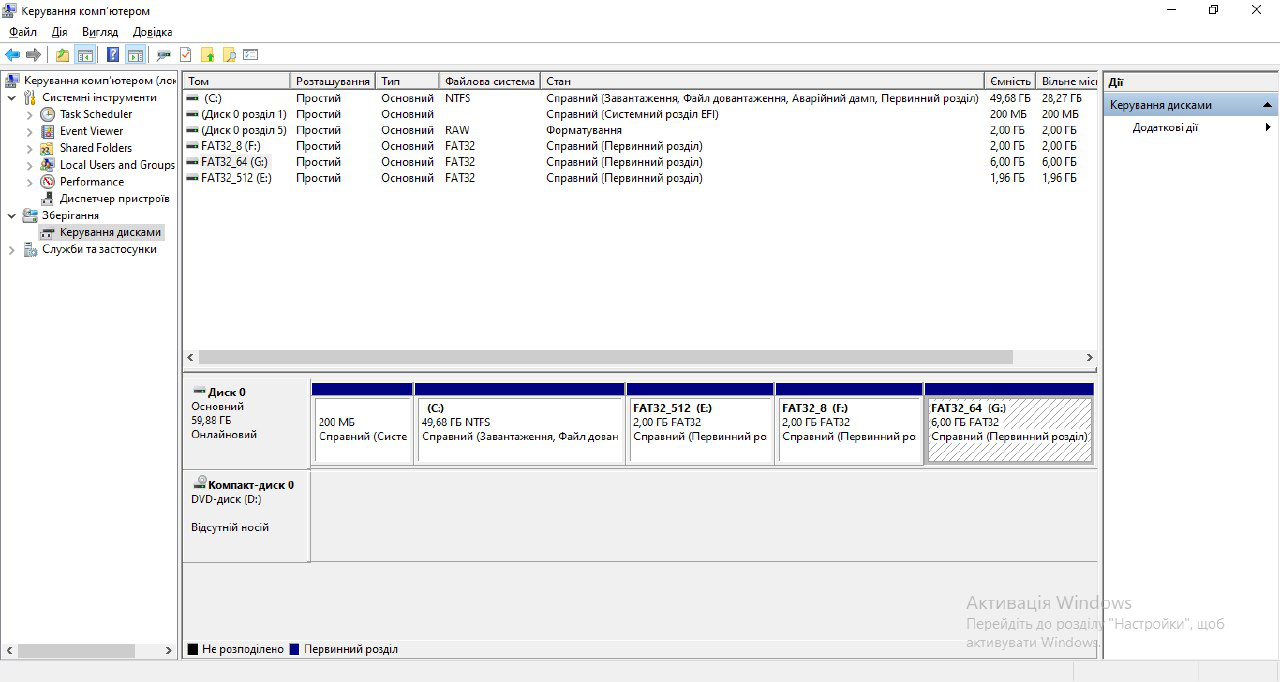


Рис. 15. Результат перетворення дисків у динамічні

7. Створити на динамічних дисках простий, складений та почерговий томи. Розширити простий том в межах одного диску. Розширити цей же том на інший диск; звернути увагу на тип тому, що утворився в результаті цієї операції.

Для створення складеного і почергового томів необхідно мати 2 фізичних диски, на яких частина дискового простору має бути не розміченою.

Натискаємо на цьому диску правою кнопкою миші і вибираємо відповідний пункт меню.

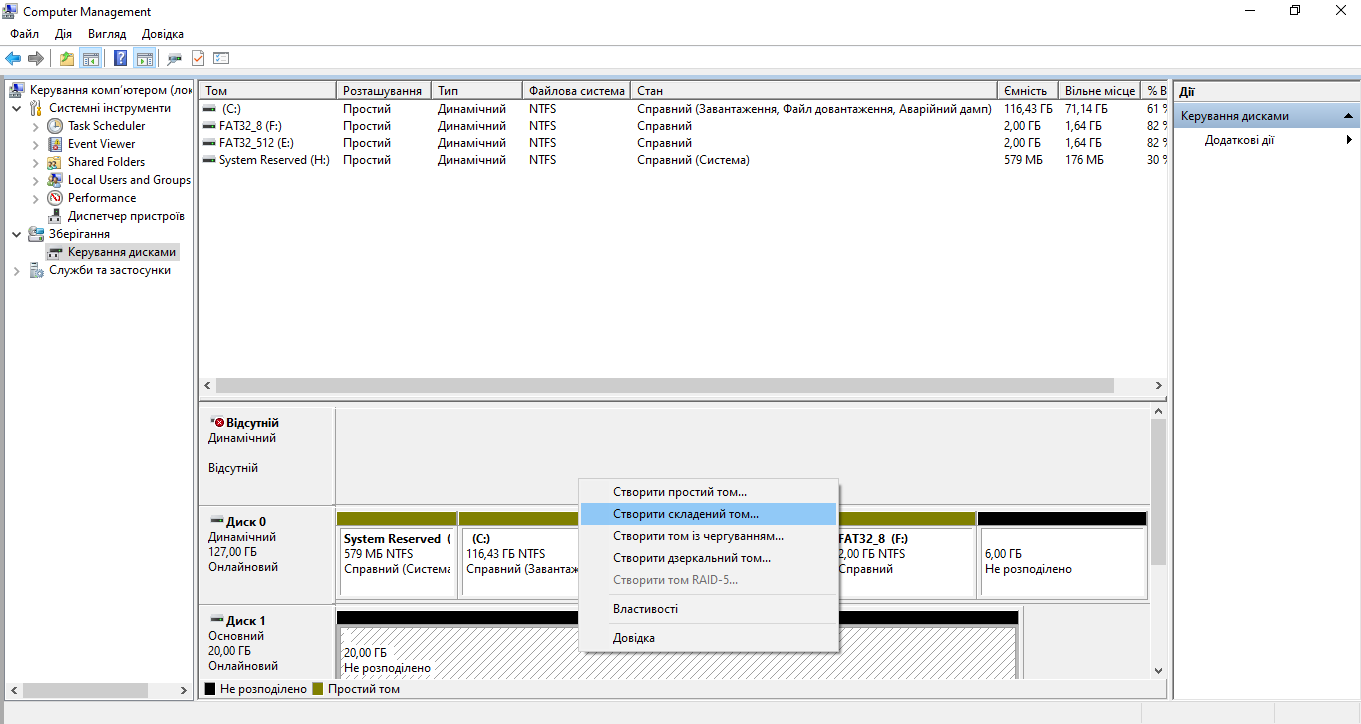


Рис. 16. Створення складеного тому

Після цього обираємо диски і зазначаємо обсяги дискового простору, а також форматування тому.

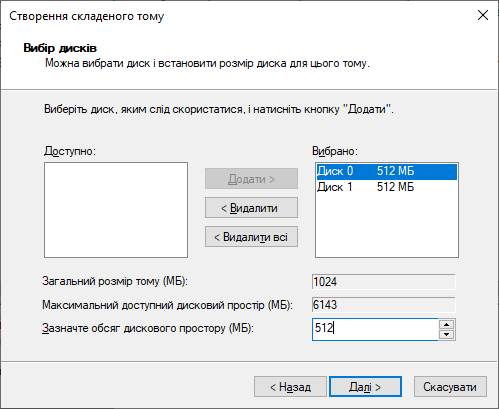


Рис. 17. Вибір дисків складеного тому

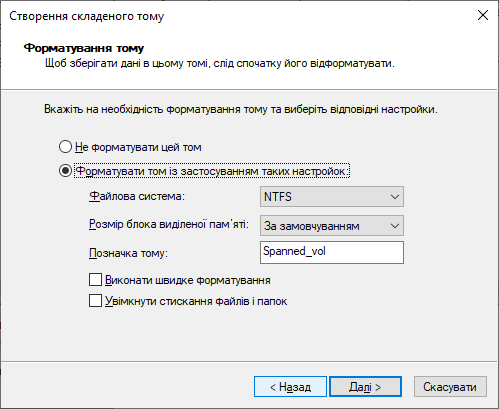


Рис. 18. Форматування складеного тому

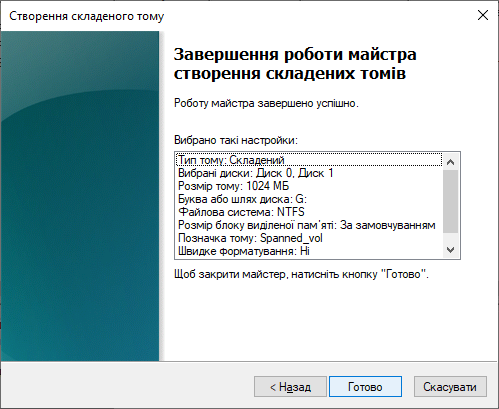


Рис. 19. Завершення створення складеного тому



Рис. 20. Результат створення складеного тому

Аналогічно створюємо том з чергуванням.

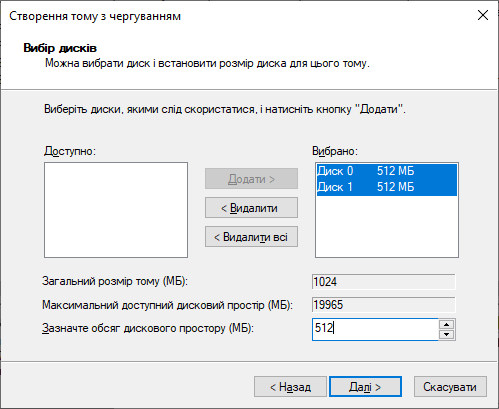


Рис. 21. Створення тому з чергуванням

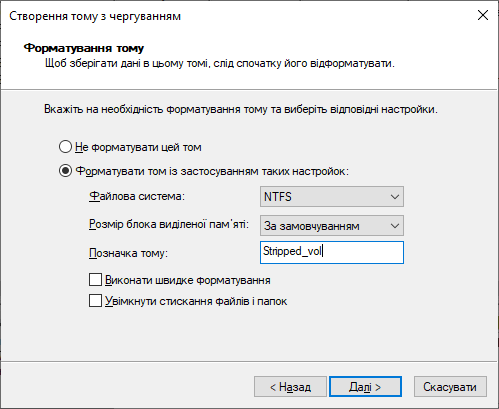


Рис. 22. Форматування тому з чергуванням

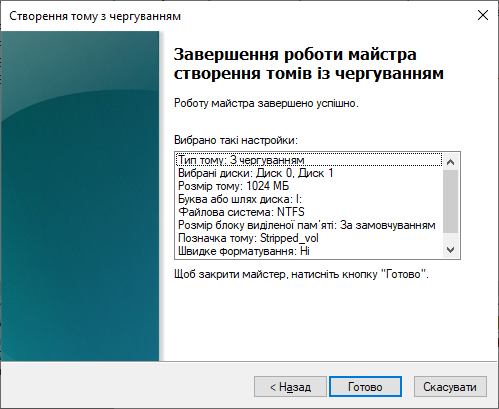
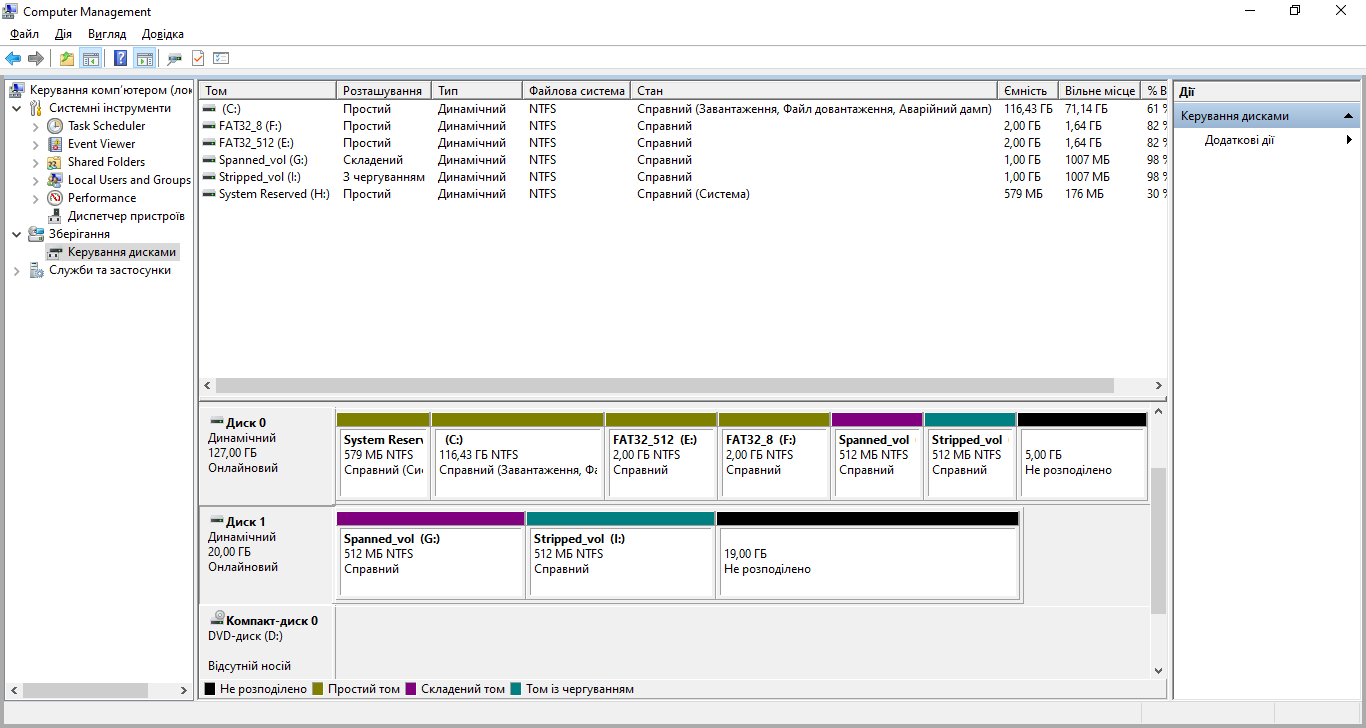


Рис. 23. Завершення створення тому з чергуванням

Рис. 24. Результат створення тому з чергуванням

Для того, щоб розширити том в межах одного диску, необхідне вільне місце на диску. Для цього можна видалити один створений том або лишити вільне місце під час їх створення в першому завданні. Натиснувши, правою кнопкою миші на томі, який необхідно розширити обираємо відповідний пункт меню.

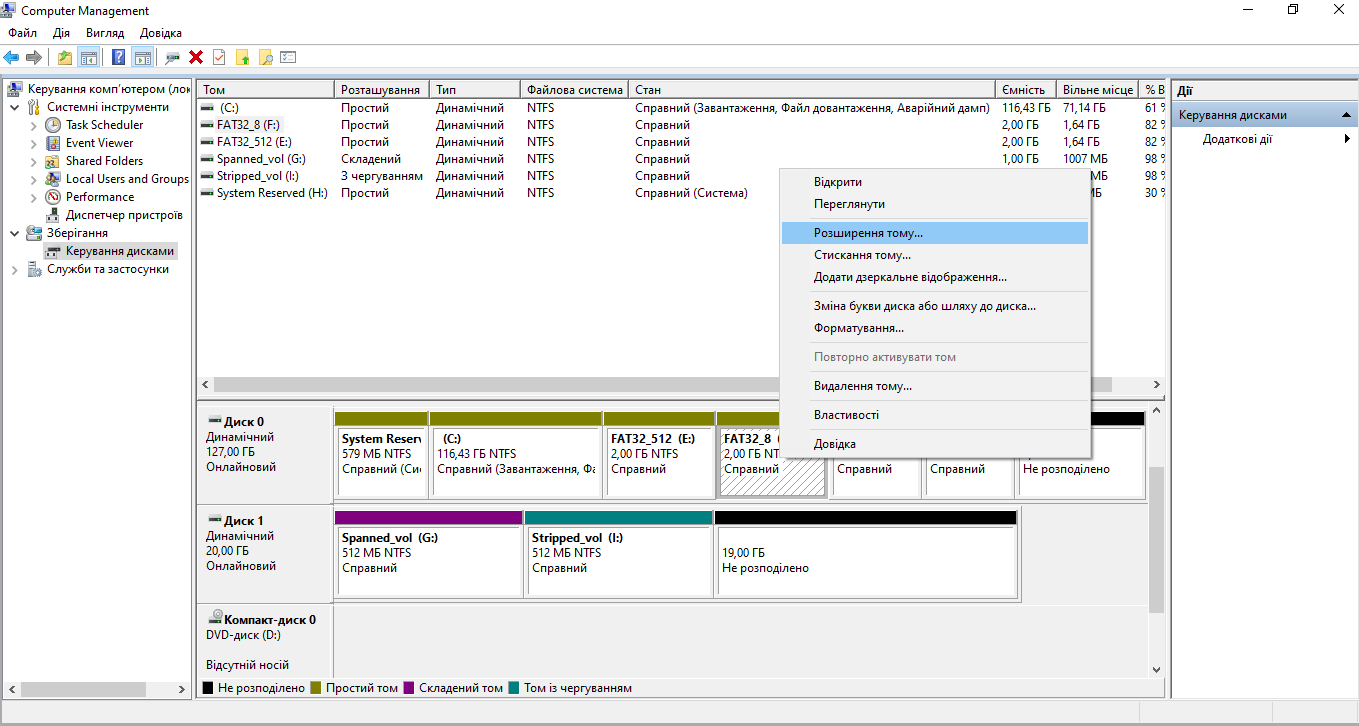


Рис. 25. Розширення тому

У майстрі розширення томів зазначити необхідний обсяг дискового простору.

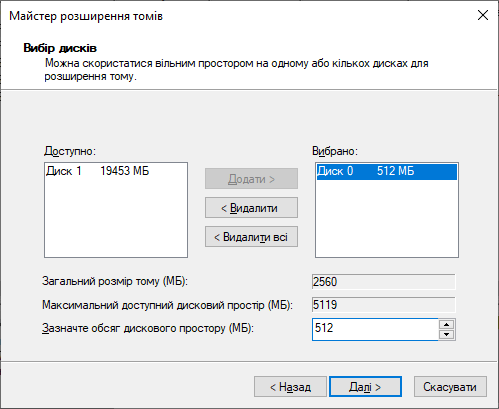


Рис. 26. Розширення тому

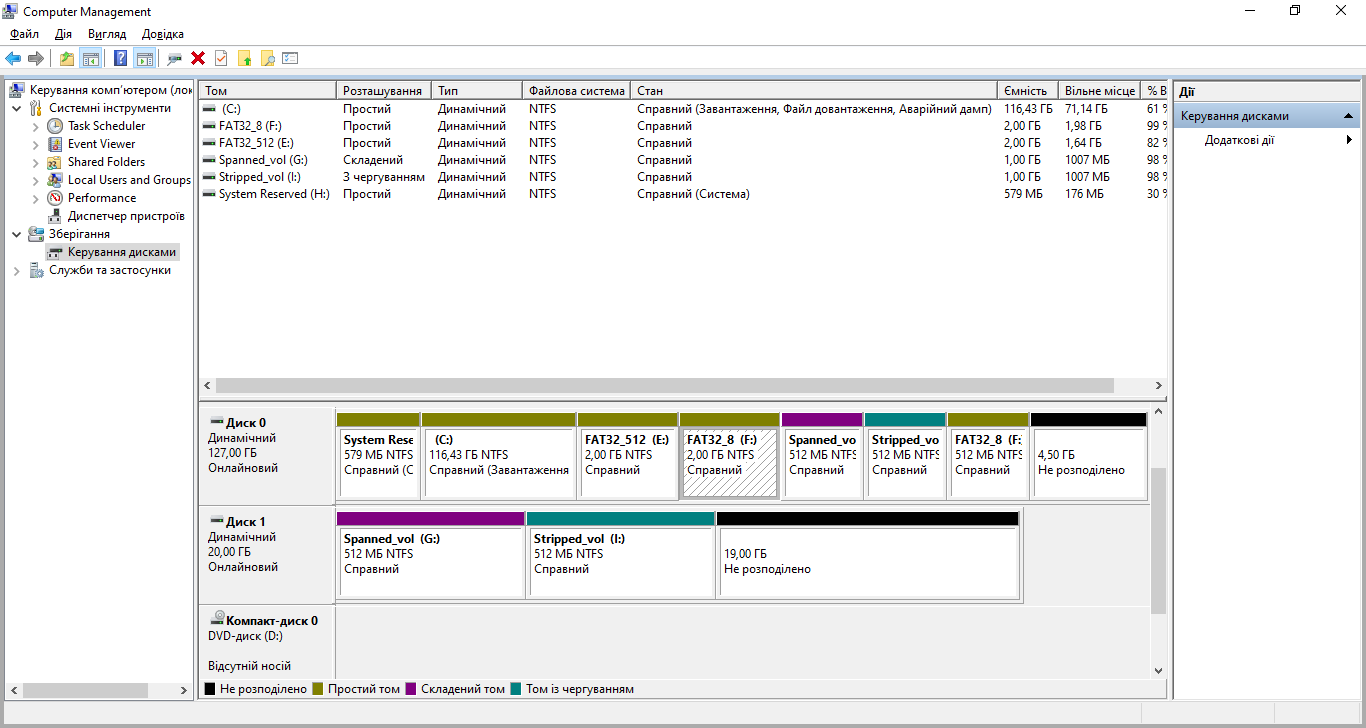


Рис. 27. Результат розширення тому

Розширюємо цей же том на інший диск.

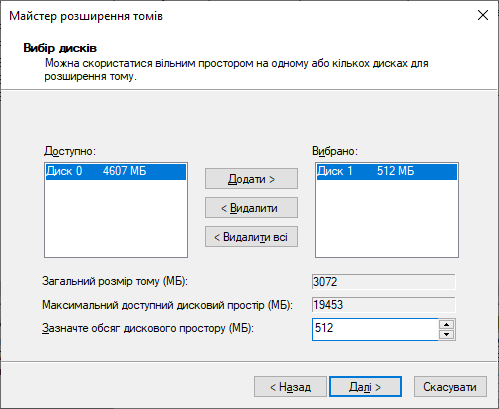


Рис. 28. Розширення тому на інший диск

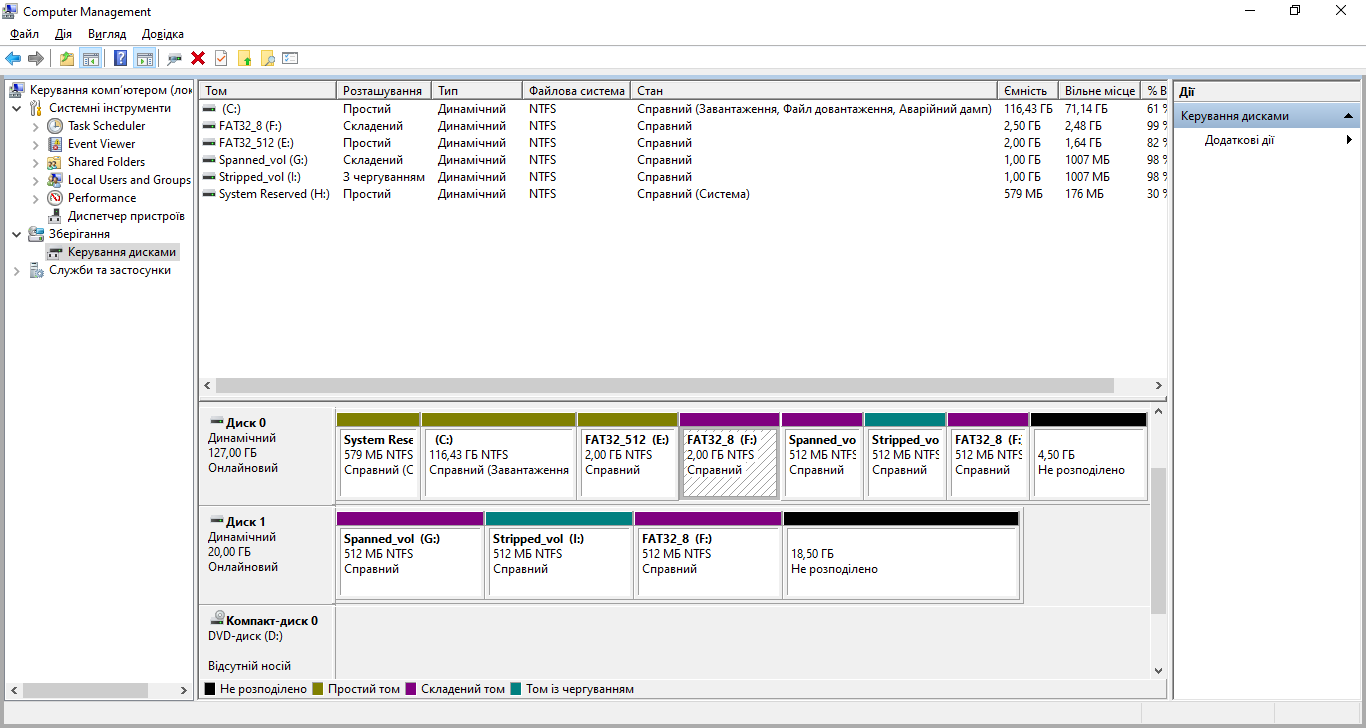


Рис. 29. Результат розширення тому на інший диск

У звіті до лабораторної роботи описати та пояснити отримані результати.

**КОНТРОЛЬНІ ЗАПИТАННЯ**

1. Переваги ФС NTFS над FAT. В яких випадках доцільніше використовувати одну й іншу файлову систему?
2. Які переваги і недоліки великого і малого розміру кластера? В яких випадках доцільніше використовувати великий, а в яких малий розмір кластера?
3. Чи можна встановити ОС Windows 10 на динамічний том?
4. Які типи томів можна створити на динамічних дисках під управлінням ОС Windows 10?
5. Яка мінімальна кількість фізичних жорстких дисків необхідна для створення масиву RAID-0; як називаються відповідні томи в ОС Windows?

**ЛАБОРАТОРНА РОБОТА № 2**

**Тема роботи:** Управління користувачами і групами в Windows 10.

**Мета роботи:** Навчитись виконувати адміністративні задачі управління користувачами і групами локального комп’ютера під управлінням ОС Windows 10; створювати і використовувати переміщувані та обов’язкові профілі користувачів.

**ТЕОРЕТИЧНІ ВІДОМОСТІ**

Створення облікових записів і груп займає важливе місце в забезпеченні безпеки усіх операційних систем і окремо Windows, оскільки, призначаючи їм права доступу і привілеї, адміністратор дістає можливість обмежити користувачів в доступі до конфіденційної інформації комп'ютерної мережі, дозволити або заборонити їм виконання в мережі певної дії, наприклад архівацію даних або завершення роботи комп'ютера.

Для роботи з локальними обліковими записами використовується оснащення "Local Users and Groups". Управління доменними обліковими записами ведеться централізовано на контролерах домену, при цьому використовується оснащення "Active Directory Users and Computers". Управління локальними обліковими записами на контролерах домену неможливе.

**Оснащення Local Users and Groups**

Оснащення Local Users and Groups (Локальні користувачі і групи) – це інструмент ММС, за допомогою якого виконується управління локальними обліковими записами користувачів і груп – як на локальному, так і на віддаленому комп'ютері. Запускати оснащення може будь-який користувач. Виконувати адміністрування облікових записів можуть тільки адміністратори і члени групи Power Users (Досвідчені користувачі).

Приклад вікна оснащення Local Users and Groups приведений на рис. 1.

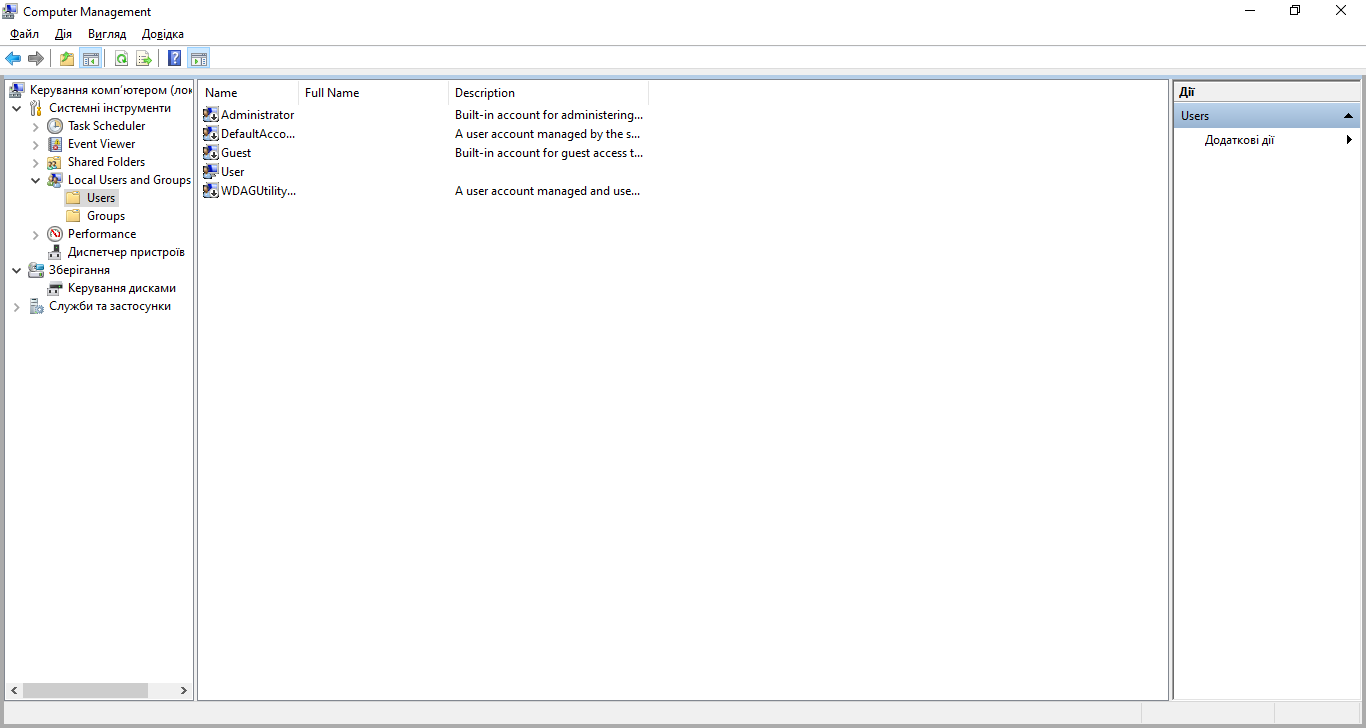


Рис. 1. Вікно оснащення Local Users and Groups у складі оснащення Computer Management

**Папка Users**

Відразу після установки системи Windows ХР, 10 папка Users (Користувачі) містить три автоматично створені вбудовані облікові записи. Два перші записи були і в системах Windows 2000, третя з'явилася в Windows XP.

* Administrator (Адміністратор) – цей обліковий запис використовують при установці і налаштуванні робочої станції або сервера, що є членом домену. Вона не може бути знищена, блокована або видалена з групи Administrators (Адміністратори), її можна тільки перейменувати.
* Guest (Гість) – цей обліковий запис застосовується для реєстрації в комп'ютері без використання спеціально створеного облікового запису. Обліковий запис Guest не вимагає введення пароля і за умовчанням є заблокованим. (Зазвичай користувач, обліковий запис якого блокований, але не видалений, при реєстрації одержує попередження, і входити в систему не може.) Він є членом групи Guests (Гості). Цьому обліковому запису можна надати права доступу до ресурсів системи так само, як і будь-якому іншому.
* SUPPORT\_388945a0 – компанія Microsoft зарезервувала цей запис за собою для підтримки довідкової служби Help and Support Service; запис є заблокованим.

Крім того, можуть з'явитися і інші призначені для користувача облікові записи, наприклад, після установки служб Інтернету – Internet Information Services.

Для роботи з локальними користувачами можна використовувати утиліту командного рядка net user.

**Папка Groups**

У системах Windows 2000 (на робочій станції або сервері, що є членом домену) папка Groups (Групи) містить шість вбудованих груп, що створюються автоматично при установці системи:

* Administrators (Адміністратори) – її члени володіють повним доступом до всіх ресурсів системи. Це єдина вбудована група, що автоматично надає своїм членам весь набір вбудованих прав. За умовчанням містить вбудований обліковий запис Administrator. Якщо комп'ютер підключений до домену, ця група також містить групу Domain Admins.
* Backup Operators (Оператори архіву) – члени цієї групи можуть архівувати і відновлювати файли в системі незалежно від того, якими правами ці файли захищені. Крім того, оператори архіву можуть входити в систему і завершувати її роботу, але вони не мають права змінювати налаштування безпеки. За умовчанням порожня.
* Guests (Гості) – ця група дозволяє виконати реєстрацію користувача за допомогою облікового запису Guest і отримати обмежені права на доступ до ресурсів системи. Члени цієї групи можуть завершувати роботу системи. За умовчанням містить користувача Guest.
* Power Users (Досвідчені користувачі) – члени цієї групи можуть створювати облікові записи користувачів, але вони мають право модифікувати настройки безпеки тільки для створених ними облікових записів. Крім того, вони можуть створювати локальні групи і модифікувати склад членів створених ними груп. Те ж саме вони можуть робити з групами Users, Guests і Power Users. Члени групи Power Users не можуть модифікувати членство в групах Administrators і Backup Operators. Вони не можуть бути власниками файлів, архівувати або відновлювати каталоги, завантажувати і вивантажувати драйвери пристроїв і модифікувати налаштування безпеки і журнал подій. За умовчанням порожня.
* Replicator (Реплікатор) – членом групи Replicator повинен бути тільки обліковий запис, за допомогою якого можна реєструватися в службі реплікації контролера домену. Її членами не слід робити робочі облікові записи. За умовчанням порожня.
* Users (Користувачі) – члени цієї групи можуть виконувати більшість призначених для користувача функцій, наприклад, запускати додатки, користуватися локальним або мережним принтером, завершувати роботу системи або блокувати робочу станцію. Вони також можуть створювати локальні групи і регулювати склад їх членів. Вони не можуть отримати доступ до загального каталогу або створити локальний принтер. За умовчанням містить службові облікові записи NT AUTHORITY\ Authenticated Users (S-1-5-11) і NT AUTHORITY\ INTERACTIVE (S-1-5-4). Якщо комп'ютер підключений до домену, ця група також містить групу Domain Users.

У системах Windows XP, 10 з'явилися ще три групи.

* Network Configuration Operators (Оператори настройки мережі) – група, члени якої мають деякі права по налаштуванню мережних служб і параметрів. За умовчанням порожня.
* Remote Desktop Users (Користувачі віддаленого робочого столу) – ця група містить імена користувачів, яким явно дозволений віддалений доступ до робочого столу.
* Help Services Group (Група служб підтримки) – група для підтримки довідкової служби Help and Support Service. За умовчанням містить обліковий запис SUPPORT\_388945a0.
* Ще чотири групи з'явилися в системах Windows Server 2003.
* Performance Log Users – члени цієї групи можуть віддалено запускати журнали реєстрації. За умовчанням містить службовий обліковий запис NT\_AUTHORITY\NETWORK SERVICE (S-l-5-20).
* Performance Monitor Users – група, члени якої можуть виконувати моніторинг продуктивності комп'ютера. За умовчанням порожня.
* Print Operators – члени цієї групи можуть адмініструвати принтери в домені. За умовчанням порожня.
* Telnet Clients – група, члени якої мають доступ до служби Telnet Server на даному комп'ютері. За умовчанням порожня.

Для роботи з локальними групами можна використовувати утиліту командного рядка net localgroup.

**Управління робочим середовищем користувача**

Робоче середовище користувача складається з налаштувань робочого столу, наприклад, кольору екрану, налаштувань миші, розміру і розташування вікон, з налаштувань процесу обміну інформацією по мережі і з пристроєм друку, змінних середовища, параметрів реєстру і набору доступних додатків.

Для управління середовищем користувача призначені наступні засоби систем Windows 2000/XP/2003/10.

* Профілі користувачів. У профілі користувача зберігаються всі налаштування робочого середовища системи, визначені самим користувачем. Це можуть бути, наприклад, налаштування екрану і з'єднання з мережею. Всі налаштування, що виконуються самим користувачем, автоматично зберігаються в папці, ім'я якої для щойно встановленої системи виглядає таким чином: %SystemDrive%\Documents and Settings\%username%.
* Сценарій входу в систему (сценарій реєстрації) є командним файлом, що має розширення .bat або .cmd, виконуваним файлом з розширенням .ехе або сценарієм VBScript, який запускається при кожній реєстрації користувача в системі або виході з неї. Сценарій може містити команди операційної системи, призначені, наприклад, для створення з'єднання з мережею або для запуску додатку. Крім того, за допомогою сценарію можна встановлювати значення змінних середовища, що вказують шляхи пошуку, каталоги для тимчасових файлів та іншу інформацію.
* Сервер сценаріїв Windows (Windows Scripting Host, WSH). Сервер сценаріїв незалежний від мови і призначений для роботи на 32-розрядних платформах Windows. Він включає як ядро сценаріїв Visual Basic Scripting Edition (VBScript), так і JScript. Сервер сценаріїв Windows призначений для виконання сценаріїв прямо на робочому столі Windows або у вікні консолі команд. При цьому сценарії не потрібно вбудовувати в документ HTML.

**Профілі користувачів**

На ізольованому комп'ютері з Windows ХР, 10 локальні профілі користувачів створюються автоматично. Інформація локальних профілів необхідна для підтримки налаштувань робочого столу локального комп'ютера, характерних для конкретного користувача. Профіль створюється для кожного користувача в процесі його першої реєстрації в комп'ютері.

Профіль користувача має наступні перевагами:

* при реєстрації користувача в системі робочий стіл одержує ті самі налаштування, які існували у момент попереднього виходу користувача з системи;
* декілька користувачів можуть працювати на одному і тому ж комп'ютері в індивідуальних середовищах (не можна тільки мати власні параметри роздільної здатності екрану і частоти розгортки; тут потрібно застосовувати профілі обладнання);
* при роботі комп'ютера в домені профілі користувачів можуть бути збережені на сервері. В цьому випадку користувач дістає можливість працювати зі своїм профілем при реєстрації на будь-якому комп'ютері мережі. Такі профілі називаються переміщуваними (roaming profile). Різновидом переміщуваних профілів є обов'язкові профілі (mandatory profiles). Такий профіль користувач не може змінювати, і всі зміни, зроблені в налаштуваннях системи, втрачаються при виході з неї. У Windows ХР, 10 і Windows Server 2003 обов'язкові профілі підтримуються тільки для сумісності, замість них рекомендується застосовувати групові політики.

**Налаштування, що зберігаються в профілі користувача**

Профіль користувача зберігає налаштування конфігурації і параметри, що індивідуально призначаються кожному користувачу і що повністю визначають його робоче середовище (табл. 1).

Таблиця 1. Налаштування профілю користувача

|  |  |
| --- | --- |
| **Об'єкт** | **Відповідні йому параметри** |
| Windows Explorer | Всі налаштування, визначені самим [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)ем, що стосуються програми Windows Explorer |
| Панель завдань | Всі персональні групи програм і їх властивості, всі програмні об'єкти і їх властивості, всі налаштування панелі завдань |
| Налаштування [принтер](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19635&displayformat=dictionary)а | Мережні з'єднання [принтер](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19635&displayformat=dictionary)а |
| [Панель управління](http://vns.lp.edu.ua/mod/page/view.php?id=55349) | Всі налаштування, визначені самим [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)ем, що стосуються панелі управління |
| Стандартні | Налаштування всіх стандартних додатків, що запускаються для конкретного [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а |
| Додатки, що працюють в операційній системі | Будь-який додаток, спеціально створений для роботи в середовищі Windows ХР, 10/2003, може володіти засобами відстеження своїх налаштувань щодо кожного [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. Якщо така інформація існує, вона зберігається в профілі [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а |
| Електронна підказка | Будь-які закладки, встановлені в довідковій системі Windows |
| Консоль управління Microsoft | Індивідуальний [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary) конфігурації і поточного стану консолі управління |

**Структура нового профілю користувача**

Профіль користувача створюється на основі профілю, що призначається за умовчанням. Він зберігається на кожному комп'ютері, де працює Windows ХР, 10. Файл NTUSER.DAT, що знаходиться в папці Default User, містить налаштування конфігурації, що зберігаються в реєстрі Windows ХР, 10. Крім того, кожен профіль користувача використовує загальні програмні групи, що знаходяться в теці All Users.

**Структура профілю користувача**

При створенні профілю користувача використовується профіль, що призначається за умовчанням, що знаходиться в папці Default User. Папка Default User, папки профілів індивідуальних користувачів, а також папки All Users, LocalService і NetworkService знаходяться в папці Documents and Settings кореневого каталогу на завантажувальному томі. У папці кожного користувача знаходяться файл NTUSER.DAT і список посилань на об'єкти робочого столу. На рис. 2 показана структура тек локального профілю користувача. У цих папках, зокрема, зберігаються посилання на різні об'єкти робочого столу. Файл ntuser.dat.LOG є журналом трансакцій, що фіксує зміни профілю і дозволяє відновити його у разі, коли відбувається пошкодження файлу NTUSER.DAT.

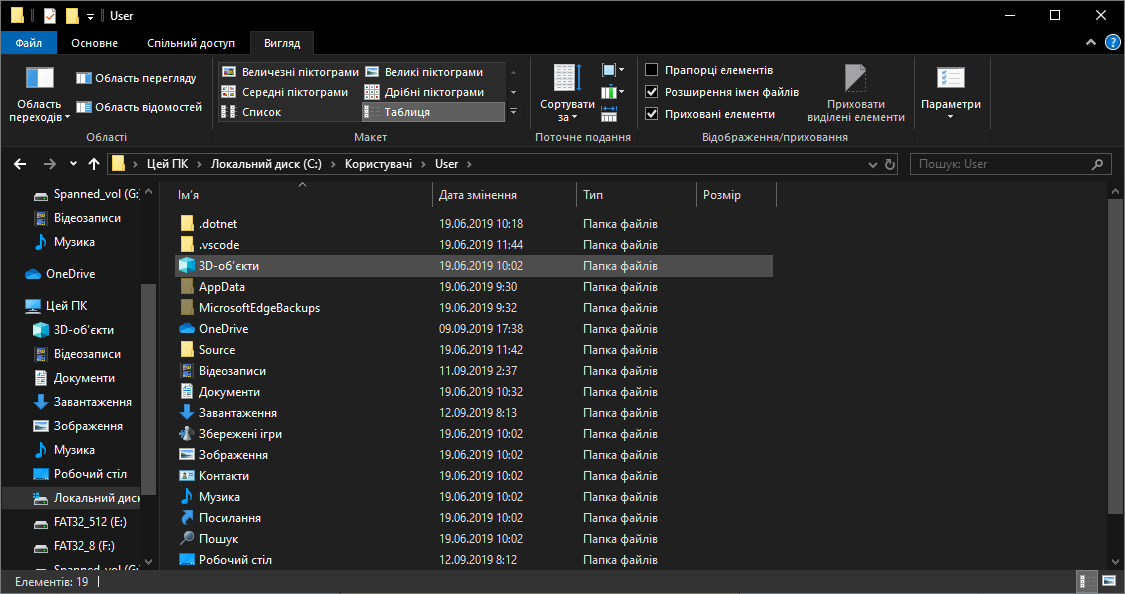


Рис. 2. Структура підпапок профілю користувача

У табл. 2 перераховані підпапки, що знаходяться усередині папки локального профілю користувача, і описано їх вміст. Деякі з цих підпапок є прихованими і можуть бути не видні при звичайному перегляді. Всі вказані папки, окрім Local Settings, входять в переміщуваний профіль користувача (при роботі комп'ютера у складі домену). При використанні звичайного профілю локальні папки Application Data, Desktop, My Documents, My Pictures і Start Menu можна перепризначувати на спільні мережні диски за допомогою оснащення-розширення Folder Redirection (Перенаправлення папки), що входить в оснащення Group Policy Object Editor (Групова політика).

Таблиця 2. Вміст папки локального профілю користувача

|  |  |
| --- | --- |
| **Підпапка** | **Вміст** |
| Application Data | Дані, що відносяться до конкретних додатків, наприклад, індивідуальний словник. Розробники додатків самі вирішують, які дані повинні бути збережені в папці профілю [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а |
| Cookies | Службові [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)и, отримані з перегляду [веб-сервер](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19624&displayformat=dictionary)ів |
| Desktop (Робочий стіл) | Об'єкти робочого столу, включаючи [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)и і ярлики |
| Favorites (Вибране) | Ярлики часто використовуваних програм і папок |
| Local Settings | Дані про локальні налаштування, що впливають на роботу програмного забезпечення комп'ютера |
| My Documents (Мої документи) | Дані про документи і графічні [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)и, що використовуються [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)ем |
| My Recent Documents (Документи, що недавно використалися) | Дані про документи і графічні [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)и, відкриті [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)ем останнім часом |
| NetHood | Ярлики об'єктів мережного оточення |
| PrintHood | Ярлики об'єктів папки [принтер](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19635&displayformat=dictionary)а |
| Recent | Ярлики недавно використовуваних об'єктів |
| SendTo | Ярлики об'єктів, куди можуть надсилатися документи |
| Start Menu (Головне меню) | Ярлики програм |
| Templates (Шаблони) | Ярлики шаблонів |
| UserData | Службова інформація |

Для управління профілями користувача є більше десятка групових політик, які доступні у вікні оснащення Group Policy Object Editor в розділах Computer Configuration | Administrative Templates | System | User Profiles та User Configuration | Administrative Templates | System | User Profiles.

**ЗАВДАННЯ ДО ВИКОНАННЯ РОБОТИ\***

**\*Використовувати своє ім’я або будь-який інакший ідентифікатор при іменуванні папок, файлів і т.д.**

1. Створити користувача з обмеженими та адміністративними правами. Змінити користувачам рисунки, що відображаються на екрані привітання при вході в систему. Змінити паролі користувачам (звернути увагу на попередження системи при зміні паролю чужого облікового запису). Видалити один зі створених облікових записів користувача.

Для того, щоб створити нового користувача, переходимо в налаштуваннях в розділ «Інші користувачі».

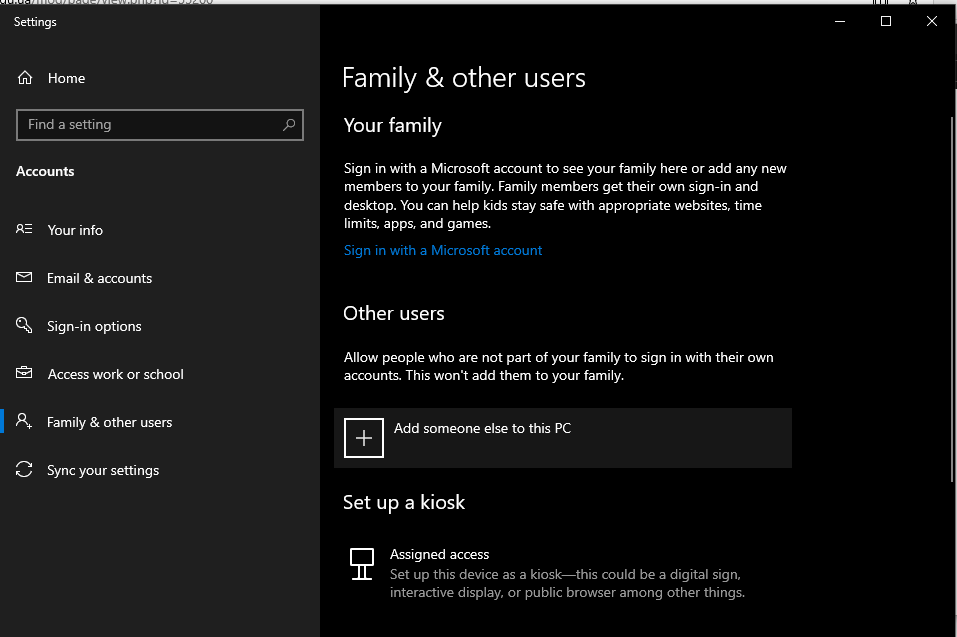


Рис. 3. «Облікові записи користувачів»

Натиснувши кнопку «Додати нового користувача» і вказавши, що в нього немає облікового запису Microsoft, заповнюємо необхідні поля.



Рис. 4. Створення нового облікового запису

Переконаємося, що тип облікового запису щойно створеного користувача - «Стандартний», натиснувши кнопку «Змінити тип аккаунта».

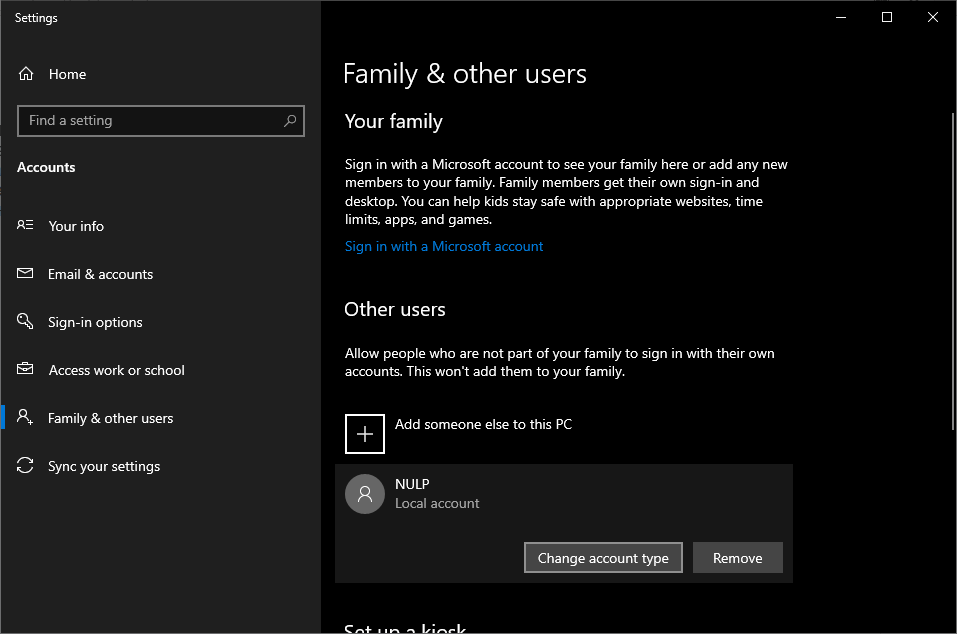


Рис. 5. Аккаунт користувача

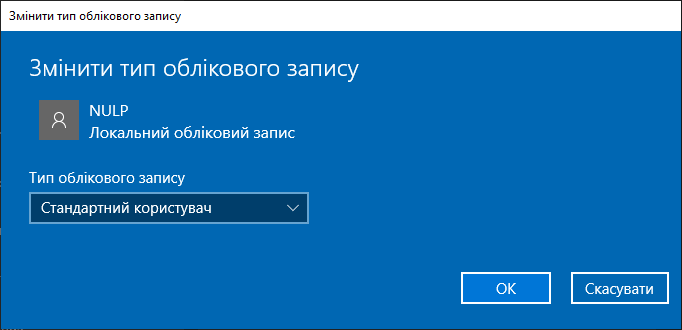


Рис. 6. Тип облікового запису

Перейдемо до перегляду інформації про свій обліковий запис User. Його тип – Адміністатор. Змінимо фотографію профілю, а також встановимо пароль у розділі «Варіанти входу».

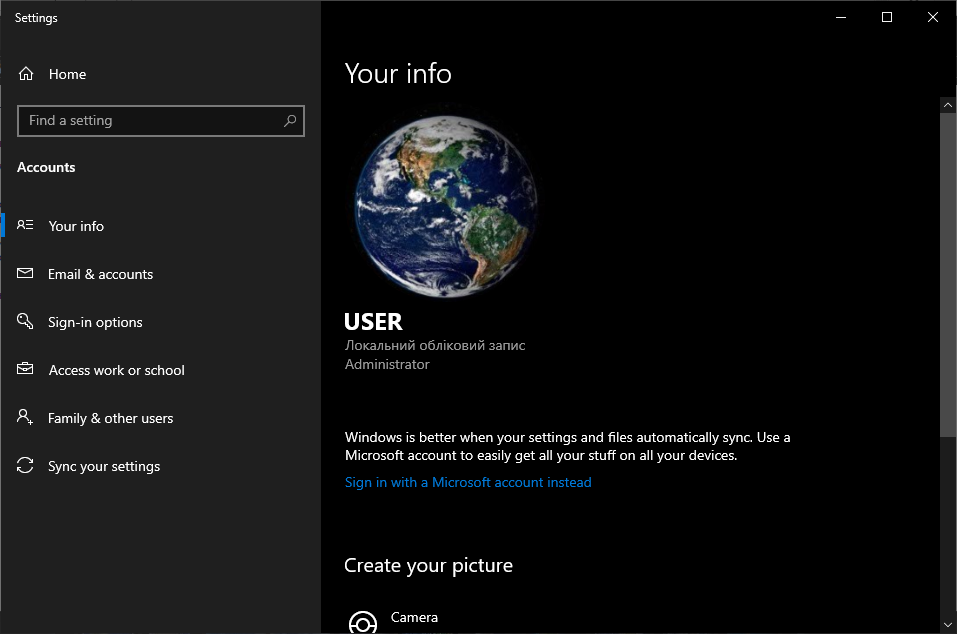


Рис. 7. Зміна фотографії профілю

Обираємо пункт «Пароль» і заповнюємо необхідні поля.

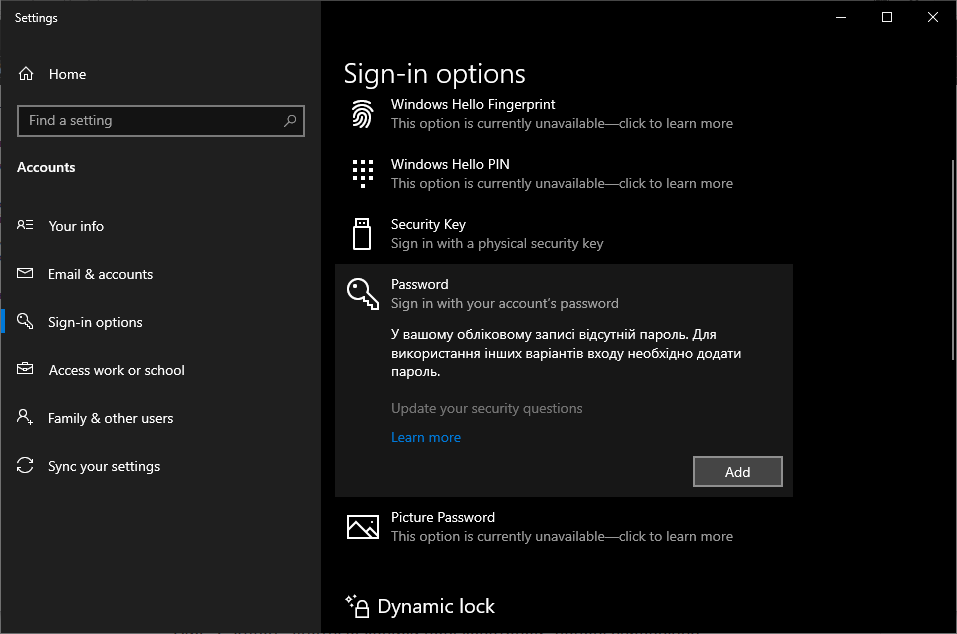


Рис. 8. Опції входу

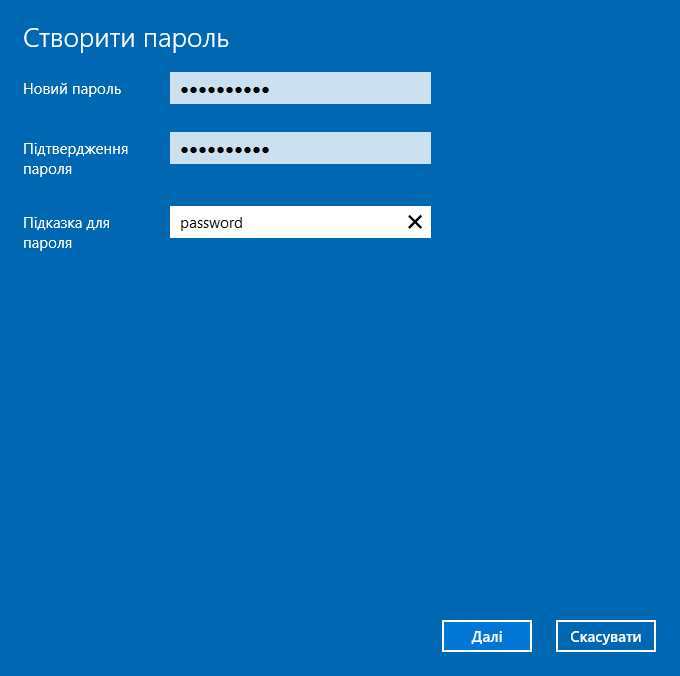


Рис. 9. Створення паролю

У результаті маємо 2 облікових записи.

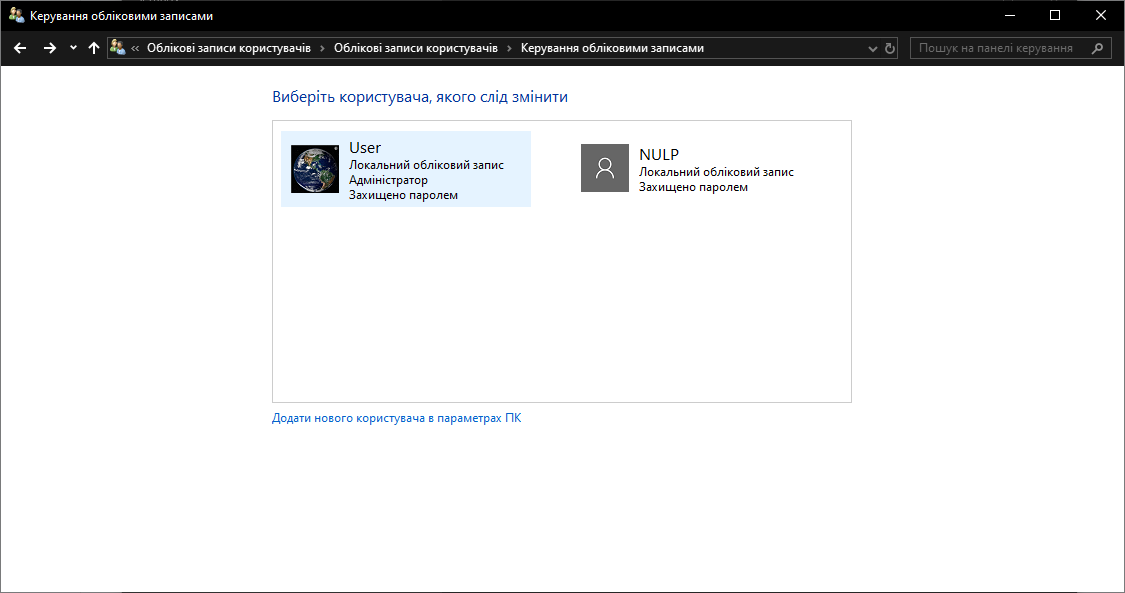


Рис. 10. Облікові записи користувачів

Змінимо пароль користувачу, створеному в попередньому завданні.

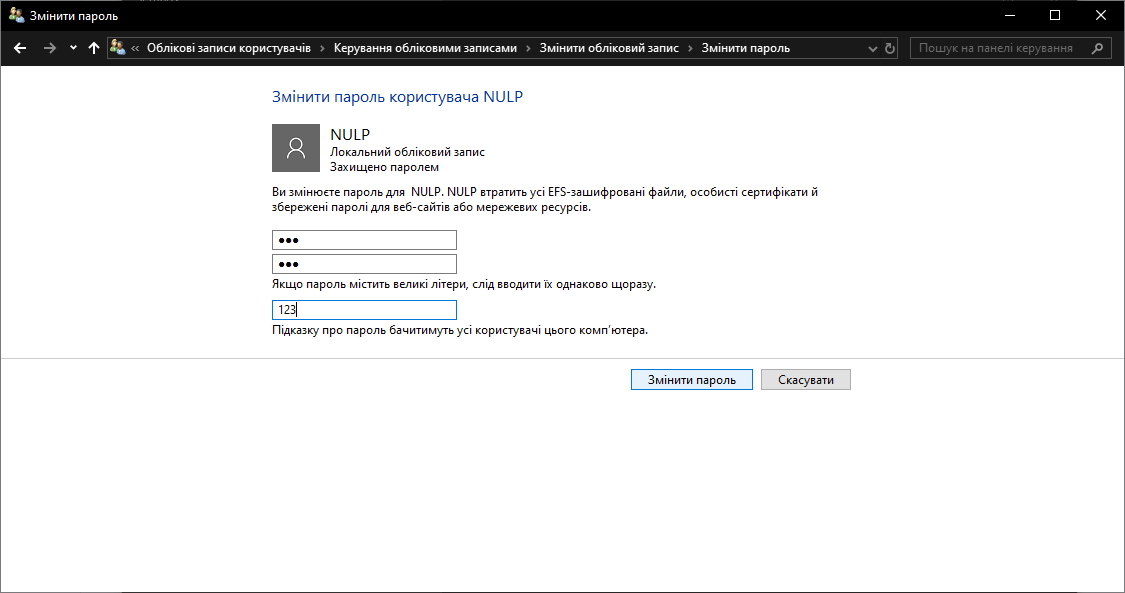


Рис. 11. Зміна паролю

1. За допомогою оснащення «Local Users and Groups» консолі mmc створити користувача, призначити йому початковий пароль та поставити вимогу зміни пароля при наступному вході в систему.
2. Натискаємо правою кнопкою миші по вкладці User і обираємо відповідний пункт меню. Заповнюємо потрібні поля і додаємо нового користувача.

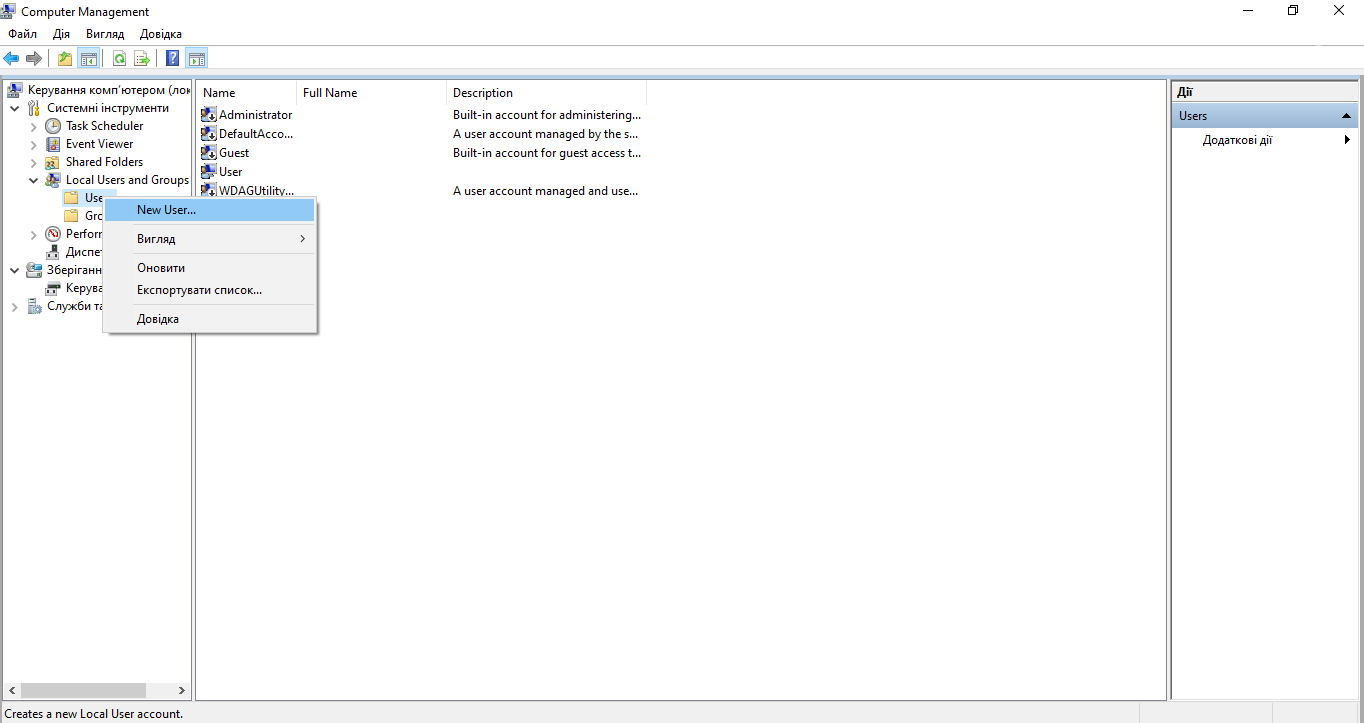


Рис. 12. Меню оснащення mmc

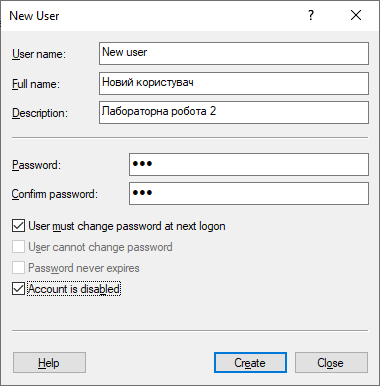


Рис. 13. Створення облікового запису

1. За допомогою оснастки «Local Users and Groups» консолі mmc внести створеного користувача в групу. Створити нову групу та внести в неї цього ж користувача .

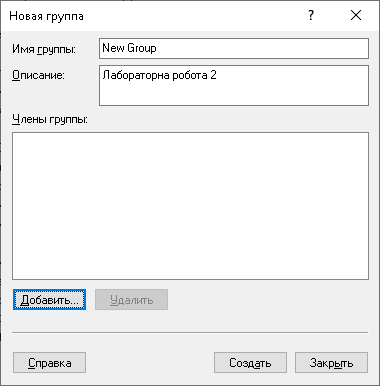


Рис. 14. Створення нової групи

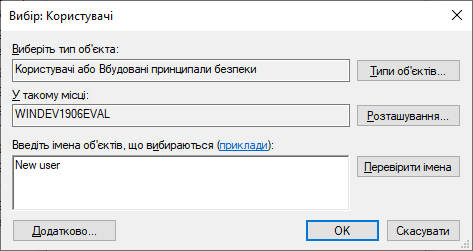


Рис. 15. Додавання користувача в групу

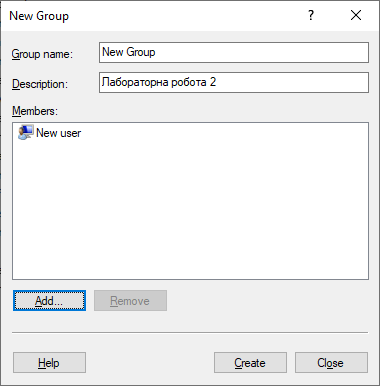


Рис. 16. Користувач, доданий в групу

Переглянемо властивості щойно створеного користувача і переконаємося, що він належить до створеною групи.

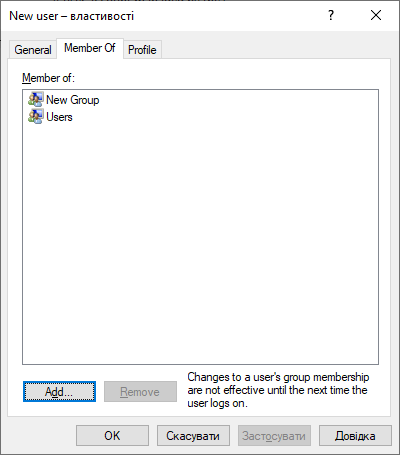


Рис. 17. Властивості користувача

1. За допомогою утиліти командного рядка net user створити користувача (довідка по цій утиліті викликається за допомогою команди net help user або net user /?) з обмеженим терміном дії облікового запису (місяць) та з дозволом входити в систему тільки з 8:00 до 17:00 в робочі дні. Змінити системну дату / час на вихідний день / неробочий час (17:00–08:00) та перевірити можливість входу цього користувача в систему. Змінити системну дату на більш ніж місяць вперед та перевірити можливість входу цього користувача в систему.

Виконавши наступну команду, встановимо необхідні параметри для користувача.

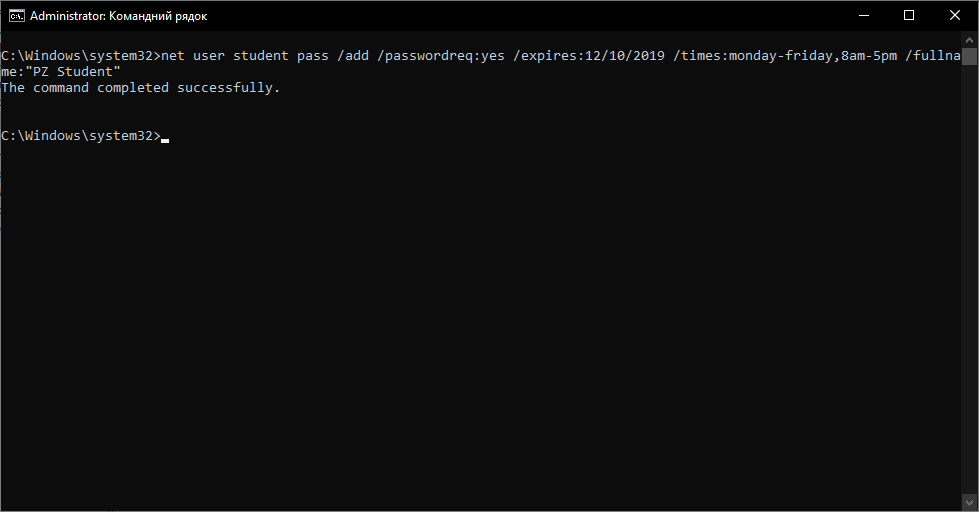


Рис. 18. Управління користувачами за допомогою командного рядка

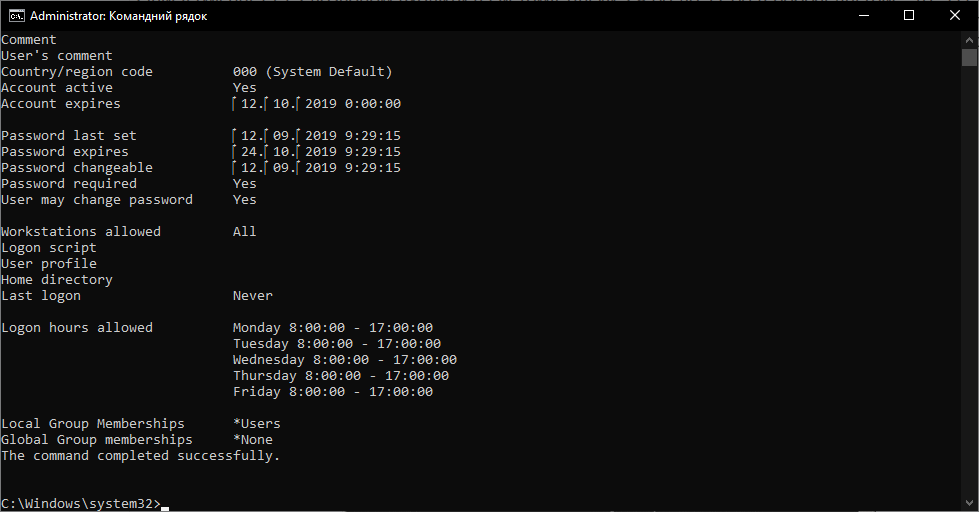


Рис. 19. Вивід відомостей про обліковий запис за допомогою командного рядка

1. За допомогою утиліти командного рядка net localgroup створити нову групу та внести в неї користувача (довідка по цій утиліті викликається за допомогою команди net help localgroup або net localgroup /?), вивести відомості про цю групу на екран.

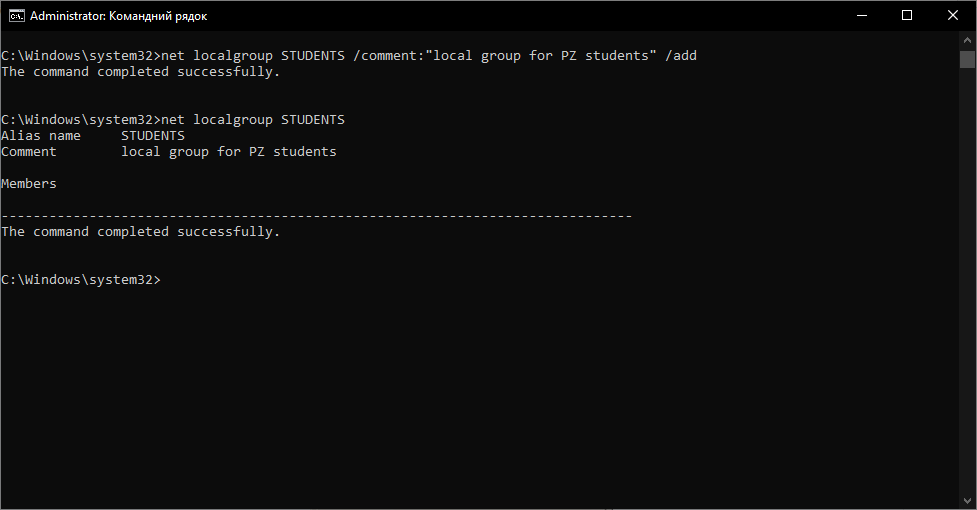


Рис. 20. Управління локальними групами за допомогою командного рядка

Викликавши правою кнопкою властивості доданої групи, аналогічно необхідно додати в неї користувача.

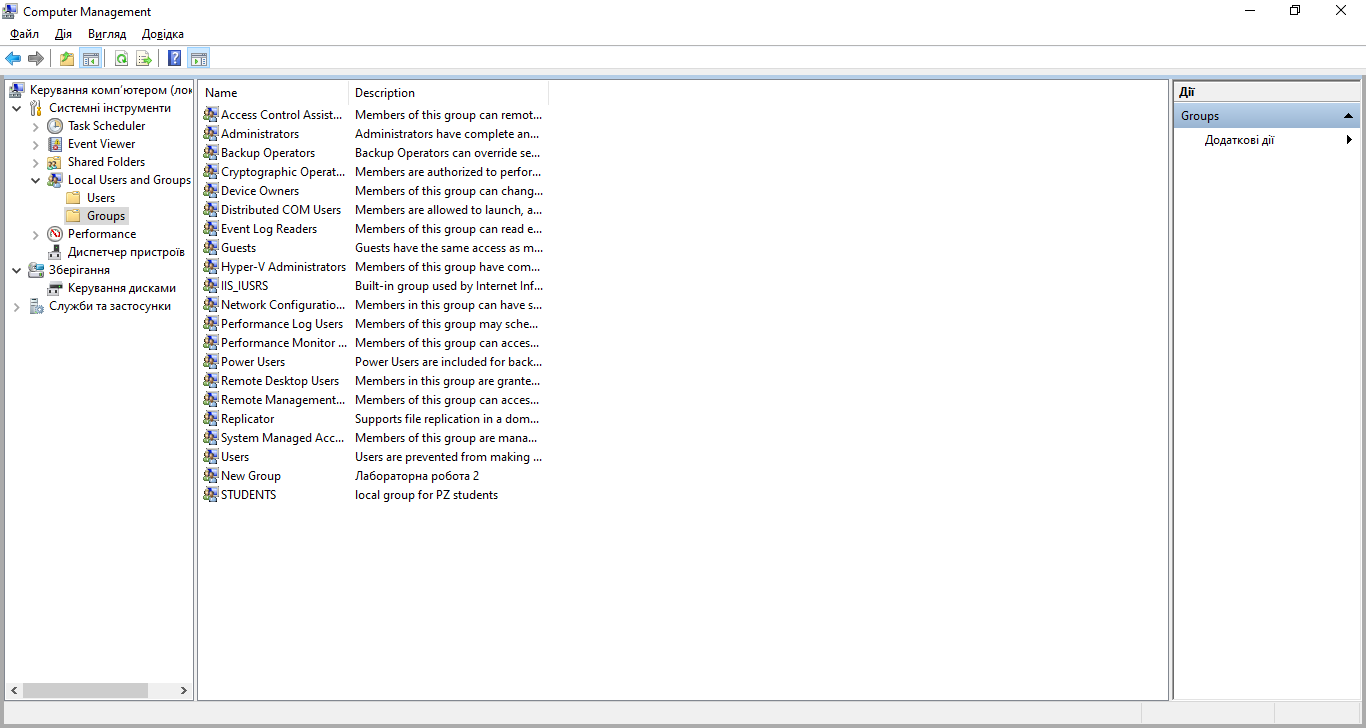


Рис. 21. Додавання користувача

1. Створити новому користувачу переміщуваний профіль. (Скопіювати створений профіль після Windows 7 немає можливості <http://forum.oszone.net/thread-195120.html> ). Є можливість скопіювати профіль користувача за замовчуванням. Для цього цей профіль копіюється в нову папку (наприклад на інший том або ж на інший комп’ютер в мережі): Мій комп’ютер | Властивості | Додатково | Профілі користувачів: Параметри | Копіювати; у вікні, що з’явиться вказують шлях копіювання та дозволи на використання профілю.

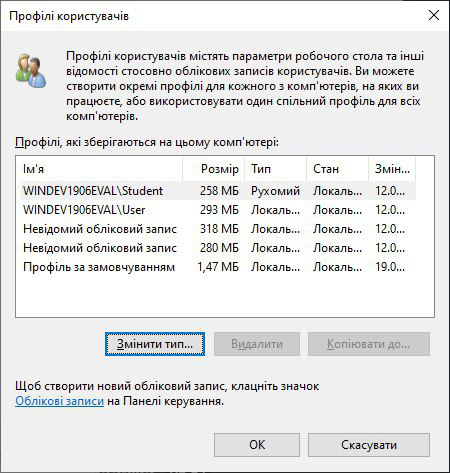


Рис. 22.Вікно профілів користувачів у властивостях комп’ютера

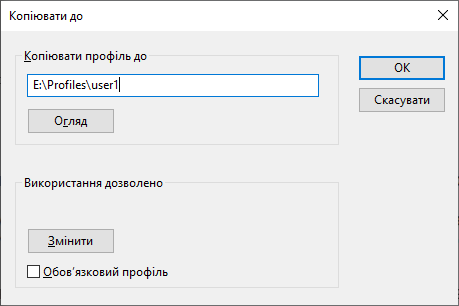


Рис. 23. Копіювання профілю користувача

Після створення папки з профілем необхідно зробити відповідні налаштування у властивостях облікового запису користувача. Якщо необхідно, щоб при вході користувача в систему виконувались певні команди / програми, тут же можна прописати сценарій входу (зверніть увагу: файл сценарію повинен розміщуватись в папці %systemroot%\system32\repl\Import\Scripts; якщо такого шляху не існує, його треба створити).

Увійти в систему під користувачем, для якого робились налаштування, переконатись у правильності виконаних дій.

Зробити профіль цього користувача обов’язковим: для цього слід перейменувати файл ntuser.dat в папці профілю у файл ntuser.man. Увійти в систему під цим користувачем, переконатись, що зміни налаштувань не зберігаються при виході користувача з системи.

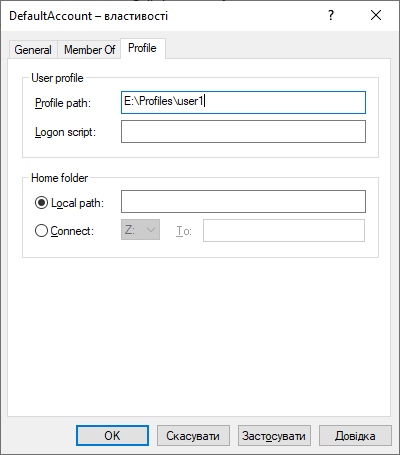


Рис. 24. Налаштування переміщуваного профілю користувача

**КОНТРОЛЬНІ ЗАПИТАННЯ**

1. Які користувачі створюються автоматично при інсталяції системи Windows XP, 10?
2. Як в Windows XP, 10 користувач може змінити свій пароль?
3. Що таке профіль користувача, що таке обов’язковий профіль?
4. Призначення груп користувачів в Windows XP, 10, вбудовані групи.
5. Як в Windows XP, 10 зробити обліковий запис користувача, що дійсний протягом певного періоду часу?

**ЛАБОРАТОРНА РОБОТА № 3**

**Тема роботи:** Дозволи та квоти NTFS. Шифрування файлів: EFS.

**Мета роботи:** Навчитись ефективно налагоджувати систему логічного розділення доступу до об’єктів файлової системи в ОС Windows 10; управляти квотами на томах NTFS та використовувати шифровану файлову систему EFS.

**ТЕОРЕТИЧНІ ВІДОМОСТІ**

**Права доступу (дозволи) для файлів і каталогів**

Встановлюючи користувачам певні дозволи на доступ до файлів і каталогів (папок), адміністратори системи можуть захищати конфіденційну інформацію від несанкціонованого доступу. Кожен користувач має певний набір дозволів на доступ до кожного об'єкту файлової системи.

Крім того, користувач може бути власником файлу або папки, якщо сам їх створює. Питання передачі права володіння розглядається нижче.

Дозволи користувача на доступ до об'єктів файлової системи працюють за принципом доповнення (адитивності). Це значить, що діючі дозволи, тобто ті дозволи, які користувач реально має відносно конкретного каталогу або файлу, утворюються зі всіх прямих і непрямих дозволів, призначених користувачу для цього об'єкту за допомогою логічної функції АБО. Наприклад, якщо користувач має прямо призначений дозвіл для каталогу на читання, а опосередковано через членство в групі йому дано дозвіл на запис, то в результаті користувач зможе читати інформацію у файлах каталогу і записувати в них дані.

Слід зазначити, що правило додавання дозволів за допомогою логічного АБО не виконується, коли користувач має певний дозвіл, а групі, в яку він входить, відмовлено в цьому дозволі (або навпаки). В цьому випадку відмова в дозволі (Deny) має вищий пріоритет над наданням дозволу, тобто в результаті користувач не матиме цього дозволу. Поява можливості відмови користувачу або групі в дозволі для файлів і каталогів зробила непотрібним дозвіл No Access, що застосовувався в Windows NT 4.0. Тепер для відмови користувачу в дозволі на доступ до якого-небудь файлу або каталогу слід включити користувача в групу, якій відмовлено в дозволі Full Control (Повний доступ) для даного об'єкту файлової системи1[[1]](#footnote-1).

Кожен зі стандартних дозволів складається з набору спеціальних (особливих) дозволів, що задають можливість виконання тієї або іншої дії з файлами або каталогами. У табл. 1 показано відповідність стандартних і спеціальних дозволів для файлів і каталогів. Детальний опис спеціальних дозволів наведено в табл. 2.

Таблиця 1 Відповідність стандартних і спеціальних дозволів

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Спеціальні дозволи** | **Стандартні дозволи** | | | | | |
| **Full Control** | **Modify** | **Read & Execute** | **List Folder Contents** | **Read** | **Write** |
| **Traverse Folder/Execute File** (Огляд папок/ Виконання [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів) | **+** | **+** | **+** | **+** |  |  |
| **List Folder/Read Data** (Зміст папок/ Читання даних) | **+** | **+** | **+** | **+** | **+** |  |
| **Read Attributes**(Читання атрибутів) | **+** | **+** | **+** | **+** | **+** |  |
| Read **Extended Attributes** (Читання додаткових атрибутів) | **+** | **+** | **+** | **+** | **+** |  |
| **Creat Files/Write Data** (Створення [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів/Запис даних) | **+** | **+** |  |  |  | **+** |
| **Create Folders/Append Data** (Створення папок/ Дозапис даних) | **+** | **+** |  |  |  | **+** |
| **Write Attributes** (Запис атрибутів) | **+** | **+** |  |  |  | **+** |
| **Write Extended Attributes**(Запис додаткових атрибутів) | **+** | **+** |  |  |  | **+** |
| **Delete Subfolders and Files**(Видалення підпапок і [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів) | **+** |  |  |  |  |  |
| **Delete** (Видалення) | **+** | **+** |  |  |  |  |
| **Read Permissions** (Читання дозволів) | **+** | **+** | **+** | **+** | **+** | **+** |
| **Change Permissions**(Зміна дозволів) | **+** |  |  |  |  |  |
| **Take Ownership**(Зміна власника) | **+** |  |  |  |  |  |

Хоча дозволи "List Folder Contents" ("Список вмісту папки") і "Read & Execute" ("Читання і виконання") включають одні і ті ж спеціальні дозволи, вони успадковуються по-різному. Дозвіл "List Folder Contents" успадковується тільки каталогами, але не файлами, і відображається тільки при перегляді дозволів на доступ до папок. Дозвіл "Read & Execute" успадковується як файлами, так і папками, і завжди відображається при перегляді дозволів на доступ до файлів або папок.

Таблиця 4. Спеціальні дозволи для [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів і [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів

|  |  |
| --- | --- |
| **Спеціальний дозвіл** | **Опис** |
| **Traverse Folder / Execute File** | Визначає можливість переміщення по [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ам [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ової системи незалежно від того, має або не має [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary) дозволу для перегляду [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів, що перетинаються в процесі переміщення. На роботу цього дозволу впливає [політика](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=4385&displayformat=dictionary) безпеки Bypass Traverse Checking (Обхід перехресної перевірки) (див. вузол **Local Policies | User Rights Assignment**в параметрах безпеки). Дозвіл Execute File (Виконання [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів) визначає можливість виконання програм. |
| **List Folder / Read Data** | Визначає можливість перегляду імен [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів або під[каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів даного [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у (відноситься тільки до [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у). Дозвіл Read Data (Читання даних) визначає можливість перегляду вмісту [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у. |
| **Read Attributes** | Визначає можливість перегляду атрибутів [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у. Самі атрибути визначаються операційною системою. |
| **Read Extended Attributes** | Визначає можливість перегляду додаткових атрибутів [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у. Самі додаткові атрибути визначаються операційною системою. |
| **Create Files /Write Data** | Визначає можливість створення [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів усередині [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у (відноситься тільки до [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів). Дозвіл Write Data (Запис даних) визначає можливість зміни вмісту [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів або перезапису існуючих даних [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у новою інформацією (відноситься тільки до [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів). |
| **Create Folders / Append Data** | Визначає можливість створювати під[каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)и усередині даного [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у (відноситься тільки до [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів). Дозвіл Append Data (Дозапис даних) визначає можливість приєднання нових даних до існуючого [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у без зміни, знищення або перезапису існуючої інформації (відноситься тільки до [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів). |
| **Write Attributes** | Визначає можливість зміни атрибутів [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у. Атрибути визначаються операційною системою. |
| **Write Extended Attributes** | Визначає можливість зміни додаткових атрибутів [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у. Додаткові атрибути визначаються програмою і можуть бути нею змінені. |
| **Delete Subfolders and Files** | Визначає можливість видалення під[каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів і [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів, що знаходяться в даному каталозі, навіть якщо для цих під[каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів і [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів немає дозволу Delete (Видалення). Цей дозвіл є тільки у [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів. |
| **Delete** | Визначає можливість видалення [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у. Якщо вам відмовлено в дозволі Delete (Видалення) для даного [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у або [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у, ви все ж таки можете видалити їх, одержавши дозвіл Delete Subfolders and Files (Видалення підпапок і [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів) на батьківський [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary). |
| **Read Permissions** | Визначає можливість читання дозволів для [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів і [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів, таких як Full Access, Read і т.д. |
| **Change Permissions** | Визначає можливість зміни дозволів для [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів і [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)ів, таких як Full Access, Read і т.д. |
| Take Ownership | Визначає можливість взяття у власність даного [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у. Власник [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)у або [каталог](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19627&displayformat=dictionary)у може завжди змінити дозволи до цього об'єкту, незалежно від інших дозволів. |

**Визначення діючих дозволів для файлів і папок**

Як вже зазначалось, користувач або група одержують дозволи на доступ до файлів або папок безпосередньо і через членство в групах (в доменах Windows 2000 і Windows Server 2003 групи можуть бути членами інших груп). Тому, коли виникає питання "а які ж врешті-решт права має даний користувач?" відповідь одержати не так просто і швидко. Системи Windows 10 і Windows Server 2008 пропонують нову можливість – визначення діючих дозволів (effective permissions).

При визначенні дозволів, що діють, потрібно пам'ятати про те, що користувач може мати права на операції з об'єктом, призначені не за допомогою механізму дозволів, а через політики безпеки. Наприклад, користувач може змінювати власника об'єкту, навіть якщо у нього немає дозволу Take Ownership, проте якщо таке право йому дане в політиках безпеки.

**Квоти дискового простору**

Адміністрування великих комп'ютерних мереж, де сервери підтримують роботу сотень користувачів, зв'язане з рядом складнощів. Одна з них – облік дискового простору серверу, зайнятого файлами співробітників компанії. Як правило, користувачі, що зберігають свої файли на сервері, мало піклуються про актуальність інформації і про знищення застарілих або непотрібних даних. Безліч тимчасових файлів і копій одного й того ж файлу, що знаходяться в різних папках, лише посилюють ситуацію. В результаті в лічені місяці навіть на великих жорстких дисках серверу може не виявитися необхідного для роботи вільного простору.

Як правило, у великих організаціях дерево каталогів вельми розгалужене, тому візуальний контроль витрачання дискового простору користувачами віднімає у адміністраторів багато часу і зусиль.

Подібна проблема просто розв'язується за допомогою введення квот на дисковий простір, доступний для роботи кожному користувачу. У попередніх версіях операційної системи Windows NT не було штатних можливостей ввести квоту на доступний дисковий простір, тому будь-який користувач міг розпоряджатися усім простором жорстких дисків комп'ютера. У Windows 10 і Windows Server 2008 адміністратор може квотувати дисковий простір по кожному тому і для кожного користувача. (З цього випливає, що неможливо задати квоту для окремих каталогів або груп.)

Система враховує загальний простір, зайнятий файлами, власником яких є контрольований користувач: якщо користувач володіє файлом, розмір останнього додається до загальної суми зайнятого користувачем дискового простору. Важливо відзначити, що, оскільки квотування виконується на рівні тому, не має значення, чи знаходиться том на одному фізичному жорсткому диску або на різних пристроях. І навпаки, якщо на одному фізичному диску зберігається декілька томів, то квотування може здійснюватися індивідуально по кожному тому.

Після установки квот дискового простору користувач зможе зберігати на томі обмежений об'єм даних, тоді як на цьому томі може залишатися вільний простір. Якщо користувач перевищує видану йому квоту, в журнал подій вноситься відповідний запис. Потім, залежно від конфігурації системи, користувач або зможе записати інформацію на том ("м'який" режим обмежень), або йому буде відмовлено в записі через відсутність вільного простору ("жорсткий" режим).

Квоти можна використовувати на локальних і спільних мережних дисках (в цьому випадку загальний доступ повинен бути дозволений на рівні кореневого каталогу тому). Стиснення файлів не має значення при обчисленні зайнятого простору – завжди враховується розмір початкового нестиснутого файлу.

Встановлювати і проглядати[[2]](#footnote-2) квоти на диску можна тільки в розділі з NTFS 5.0 і за наявності необхідних повноважень (що задаються за допомогою локальних або доменних групових політик) у користувача, що встановлює квоти. За умовчанням для роботи з квотами потрібно бути членом групи Administrators.

**Передача права володіння**

У попередніх версіях Windows NT право володіння файлом або папкою було характеристикою, жорстко прив'язаною до творця даного об'єкту. Користувач, що створив файл або каталог, ставав власником цього об'єкту. Право володіння не могло бути передане іншому користувачу. Єдине виключення складав адміністратор, який міг стати власником об’єкту. Сам користувач не міг передати право володіння папкою або файлом іншому користувачу.

Операційні системи Windows 10 і Windows Server 2008 забезпечують гнучкіше користування таким засобом забезпечення безпеки інформації, як право володіння об'єктом файлової системи. Тепер адміністратор або уповноважений користувач може призначити будь-якого користувача власником якого-небудь об'єкту файлової системи (ця можливість є тільки в Windows Server 2008) або користувач сам може стати власником об'єкту, не створеного ним самим. Природно, що для цього він повинен мати необхідні дозволи (Take Ownership). Крім того, за допомогою локальних або доменних політик безпеки можна вказувати, які користувачі завжди можуть ставати власниками файлів або інших об'єктів (за умовчанням таке право мають тільки адміністратори), при цьому вони можуть навіть не мати ніяких дозволів для цього об'єкту[[3]](#footnote-3).

Для передачі володіння об'єктом файлової системи або для проглядання поточного власника файлу або папки слід відкрити відповідне вікно властивостей, перейти на вкладку Security, потім натиснути кнопку Advanced. З'явиться вікно Advanced Security Settings (рис. 1).

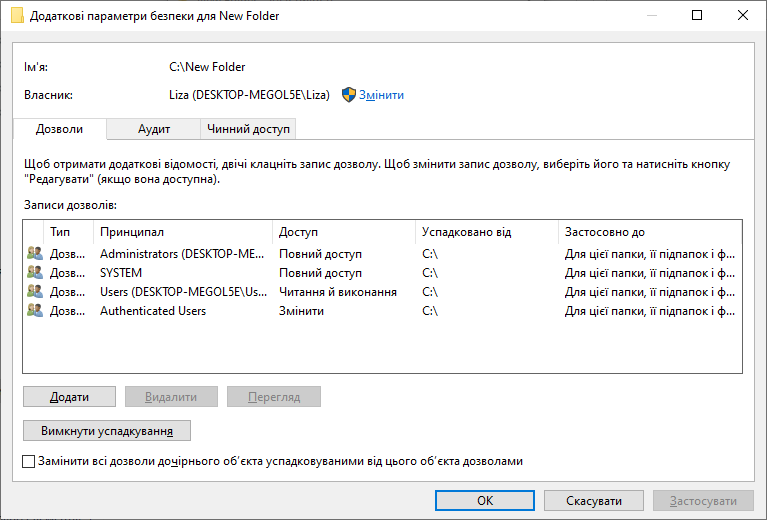


Рис.1. Діалогове вікно Advanced Security Settings

У Windows Server 2008 адміністратор або інший користувач, що отримав (через відповідну політику безпеки) право зміни власників об'єктів, може натиснути кнопку **Other Users or Groups** (Інші користувачі або групи) і вибрати користувача (або групу), якого він хоче призначити власником об'єкту.

**Шифруюча файлова система EFS**

На персональному комп'ютері операційну систему можна завантажити не з жорсткого, а з гнучкого чи компакт диска. Це дозволяє обійти проблеми, пов'язані з відмовою жорсткого диска і руйнуванням завантажувальних розділів. Проте, оскільки за допомогою змінного носія можна завантажувати різні операційні системи, будь-який користувач, що одержав фізичний доступ до комп'ютера, може обійти вбудовану систему управління доступом файлової системи NTFS і за допомогою певних інструментів прочитати інформацію жорсткого диска.

Єдиний надійний спосіб захисту інформації – це шифруюча файлова система. На ринку програмного забезпечення існує цілий набір продуктів, що забезпечують шифрування даних за допомогою утвореного від пароля ключа на рівні додатків. Проте такий підхід має ряд обмежень.

* Ручне шифрування і дешифрування. Служби шифрування більшості продуктів непрозорі для користувачів. Користувачу доводиться розшифровувати файл перед кожним його використанням, а потім знову зашифровувати. Якщо користувач забуває зашифрувати файл після закінчення роботи з ним, інформація залишається незахищеною. Оскільки кожного разу необхідно вказувати, який файл повинен бути зашифрований (і розшифрований), застосування такого методу захисту інформації сильно утруднене.
* Просочування інформації з тимчасових файлів і файлів підкачки. Практично всі додатки в процесі редагування документів створюють тимчасові файли. Вони залишаються на диску незашифрованими, не зважаючи на те, що оригінальний файл зашифрований. Крім того, шифрування інформації на рівні додатків виконується в режимі користувача. Це значить, що ключ, вживаний для такого типу шифрування, може зберігатися у файлі підкачки. В результаті, за допомогою вивчення вмісту файлу підкачки можна одержати ключ і розшифрувати всі документи користувача.
* Слабка криптостійкість ключів. Ключі утворюються від паролів або випадкових фраз. Тому у випадку, якщо пароль легко запам'ятовується, атаки за допомогою словників можуть привести до швидкого злому системи захисту.
* Неможливість відновлення даних. Більшість продуктів, що дозволяють шифрувати інформацію, не надають засобів відновлення даних, що для користувачів є додатковим мотивом не застосовувати засоби шифрування. Це особливо стосується тих працівників, які не хочуть запам'ятовувати додатковий пароль. З другого боку, засіб відновлення даних за допомогою пароля – ще одна прогалина в системі захисту інформації. Все, що необхідно зловмиснику, – це пароль, призначений для запуску механізму відновлення даних, який дозволить отримати доступ до зашифрованих файлів.

Всі перераховані вище проблеми дозволяє вирішити шифруюча файлова система (Encrypting File System, EFS), вперше реалізована у Windows 2000, яка працює тільки на NTFS 5.0.

EFS містить наступні компоненти операційної системи (рис. 2):

* Драйвер EFS. Драйвер EFS є надбудовою над файловою системою NTFS. Він обмінюється даними зі службою EFS – запитує ключі шифрування, набори DDF (Data Decryption Field) і DRF (Data Recovery Field), – а також з іншими службами управління ключами. Одержану інформацію драйвер EFS передає бібліотеці реального часу файлової системи EFS (File System Run-Time Library, FSRTL), яка прозоро для операційної системи виконує різні операції, характерні для файлової системи (читання, запис, відкриття файлу, приєднання інформації).
* Бібліотека реального часу файлової системи EFS. FSRTL – це модуль, який знаходиться усередині драйвера EFS і реалізовує виклики NTFS, що виконують такі операції, як читання, запис і відкриття зашифрованих файлів і каталогів, а також операції, пов'язані з шифруванням, дешифруванням і відновленням файлів при їх читанні або запису на диск. Хоча драйвери EFS і FSRTL реалізовані у вигляді одного компоненту, вони ніколи не обмінюються даними безпосередньо. Для передачі повідомлень один одному вони використовують механізм викликів (callouts) NTFS, призначений для управління файлами. Це гарантує, що вся робота з файлами відбувається за безпосередньої участі NTFS.

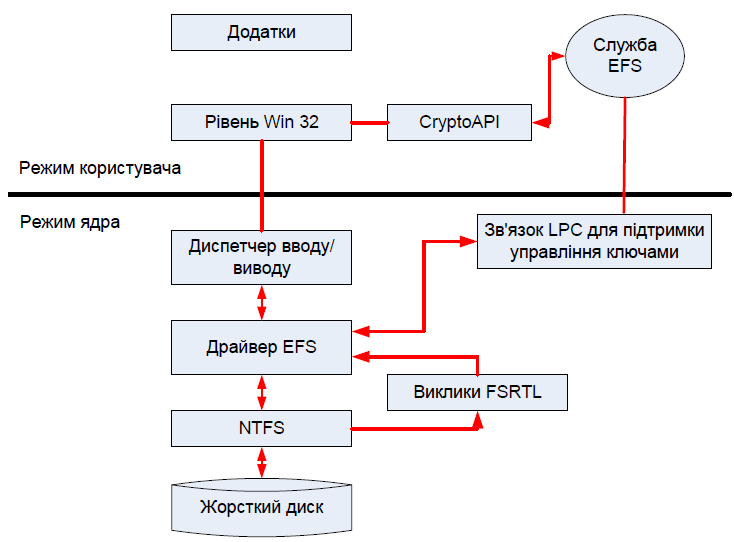


Рис. 2. Архітектура EFS

* Служба EFS. Служба EFS (EFS Service) є частиною системи безпеки операційної системи. Для обміну даними з драйвером EFS вона використовує порт зв'язку LPC, що існує між локальним адміністратором безпеки (Local Security Authority, LSA) і монітором безпеки, що працює в привілейованому режимі. У режимі користувача для створення ключів шифрування файлів і генерування даних для DDF і DRF служба EFS використовує CryptoAPI. Вона також підтримує набір API для Win32.
* Набір API для Win32. Цей набір інтерфейсів прикладного програмування дозволяє виконувати шифрування файлів, дешифровку і відновлення зашифрованих файлів, а також їх імпорт і експорт (без попередньої дешифровки). Ці API підтримуються стандартним системним модулем DLL – advapi32.dll.

EFS заснована на шифруванні з відкритим ключем і використовує всі можливості архітектури CryptoAPI. Кожен файл шифрується за допомогою випадково генерованого ключа, залежного від пари відкритого (public) і приватного (private) ключів користувача. Подібний підхід значною мірою утруднює здійснення великого набору атак, заснованих на криптоаналізі. При криптозахисті файлів може бути застосований будь-який алгоритм симетричного шифрування. EFS дозволяє здійснювати шифрування і дешифрування файлів, що знаходяться на віддалених файлових серверах.

Дані зашифровуються за допомогою симетричного алгоритму із застосуванням ключа шифрування файлу (File Encryption Key, FEK). FEK – це генерований випадковим чином ключ певної довжини. Своєю чергою, FEK шифрується за допомогою одного або декількох відкритих ключів, призначених для криптозахисту ключа. В цьому випадку створюється список зашифрованих ключів FEK, що дозволяє організувати доступ до файлу декільком користувачам. Для шифрування набору FEK використовується відкрита частина пари ключів кожного користувача. Список зашифрованих ключів FEK зберігається разом із зашифрованим файлом в спеціальному атрибуті EFS, званому полем дешифрування даних (Data Decryption Field, DDF). Інформація, необхідна для дешифрування, прив'язується до самого файлу. Приватна частина ключа користувача використовується при дешифруванні FEK. Вона зберігається в безпечному місці, наприклад на смарт-карті або іншому пристрої, що має високий ступінь захищеності.

FEK застосовується для створення ключів відновлення. Для цього FEK шифрується за допомогою одного або декількох відкритих ключів відновлення. Список FEK, зашифрованих для цілей відновлення, зберігається разом із зашифрованим файлом в спеціальному атрибуті EFS, званому полем відновлення даних (Data Recovery Field, DRF). Завдяки існуванню набору зашифрованих ключів FEK агенти відновлення даних можуть дешифрувати файл. Для шифрування ключа FEK в полі DRF необхідна тільки відкрита частина пари ключів відновлення, її присутність в системі необхідна у будь-який момент часу для нормального функціонування файлової системи. Сама процедура відновлення виконується досить рідко, коли користувач звільняється з організації або забуває приватну частину ключа. Тому агенти відновлення можуть зберігати приватну частину ключів відновлення в безпечному місці, наприклад на смарт-картах або інших добре захищених пристроях.

EFS тісно взаємодіє з NTFS 5.0. Тимчасові файли, створювані додатками, успадковують атрибути оригінальних файлів (якщо файли знаходяться в розділі NTFS). Разом з файлом шифруються також і його тимчасові копії. EFS знаходиться в ядрі Windows і використовує для зберігання ключів спеціальний пул, що не вивантажується на жорсткий диск. Тому ключі ніколи не потрапляють у файл підкачки.

У Windows Server 2008 файлова система EFS має деякі нові можливості:

* із зашифрованими файлами можуть працювати декілька користувачів. Користувач, що зашифрував файл, може дозволити іншим локальним і доменним користувачам (на комп'ютерах під управлінням Windows XP і Windows 10) працювати з цим файлом;
* можна шифрувати автономні папки і файли (offline folders);
* агент відновлення (recovery agent) за умовчанням не використовується;
* стандартний алгоритм шифрування – Advanced Encryption Standard, AES (Rijndael) (256 біт). Алгоритм DESX, що використовується за умовчанням системою EFS в Windows XP і Windows 10, не може застосовуватися для шифрування файлів в Windows Server 2008;
* замість AES може використовуватися алгоритм шифрування 3DES (128 або 168 біт), для цього потрібно змінити політику безпеки;
* зашифровані файли можуть розташовуватися у веб-папках;
* сертифікати EFS можуть автоматично доставлятися користувачу службами сертифікатів (Certificate Services) і механізмом автоматичного підпису сертифікатів;
* особисті ключі можуть зберігатися і відновлюватися за допомогою засобів архівації, що є в службах сертифікатів;
* вся службова інформація, що зберігається на диску, не просто видаляється, а очищується (заповнюється порожніми байтами); це збільшує захищеність шифрованих даних.

Конфігурація EFS, встановлювана за умовчанням, дозволяє користувачу шифрувати свої файли без жодного втручання з боку адміністратора. В цьому випадку EFS автоматично генерує для користувача пару ключів (відкритий і особистий), що застосовуються для криптозахисту даних, і підписує сертифікат.

Шифрування і дешифрування файлів може бути виконане як для певних файлів, так і для цілого каталогу. Ці операції прозорі для користувача. При шифруванні каталогу автоматично шифруються і всі його файли і підкаталоги. Кожен файл має унікальний ключ, що дозволяє легко виконувати операцію перейменування. Якщо ви перейменовуєте файл, що знаходиться в зашифрованому каталозі, і переносите його в незашифрований каталог, сам файл залишається зашифрованим (за умови, що цільовий каталог знаходиться на томі NTFS 5.0). Засоби шифрування і дешифрування доступні через Windows Explorer. Крім того, можна використовувати всі можливості шифрування даних за допомогою набору утиліт командного рядка і інтерфейсів адміністрування.

Найсерйозніша і, на жаль, доволі поширена помилка при роботі з EFS полягає у тому, що користувачі шифрують дані на локальному комп'ютері, а потім встановлюють заново операційну систему. В цьому випадку дані будуть безповоротно втрачені, оскільки доступ до них мали тільки два користувачі тієї системи, в якій дані були зашифровані: користувач, що виконав цю операцію, і агент відновлення. Помилка полягає у тому, що для розшифрування даних необхідно пред'явити сертифікати одного з названих користувачів, а для цього відповідні сертифікати потрібно було експортувати і зберегти.

EFS має в своєму розпорядженні вбудовані засоби відновлення зашифрованих даних за умов, коли невідомий приватний ключ користувача. Користувачі, які можуть відновлювати зашифровані дані за умов втрати приватного ключа, називаються агентами відновлення даних[[4]](#footnote-4).

Агенти відновлення даних мають сертифікат (Х.509 v.3) на відновлення файлів і особистий ключ, за допомогою яких виконується операція відновлення зашифрованих файлів. Використовуючи ключ відновлення, можна одержати тільки генерований випадковим чином ключ, за допомогою якого був зашифрований конкретний файл. Тому агенту відновлення не може випадково стати доступною інша конфіденційна інформація.

**ЗАВДАННЯ ДО ВИКОНАННЯ РОБОТИ\***

**\*Використовувати своє ім’я або будь-який інакший ідентифікатор при іменуванні папок, файлів і т.д.**

1. Створити на томі NTFS нову папку; у властивостях об’єкту перейти на вкладку "Безпека". (Звернути увагу на те, які дозволи призначені за замовчуванням.) Для того, щоб дозволити усім користувачам створювати файли і папки у цій папці, але заборонити її видаляти, а також для перегляду та редагування елементарних дозволів, натисніть кнопку "Додатково" (рис. 4). Щоб додати елементарний дозвіл для користувача чи групи натисніть "Додати" (рис. 5); додайте суб’єкта безпеки та задайте для нього дозволи. (Зверніть увагу на меню "Застосувати", яке управляє об’єктами безпеки, на які поширюватиметься заданий дозвіл!)

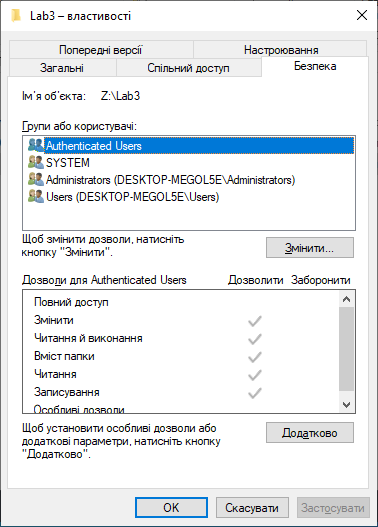


Рис. 3. Вкладка "Безпека" властивостей об'єкту файлової системи

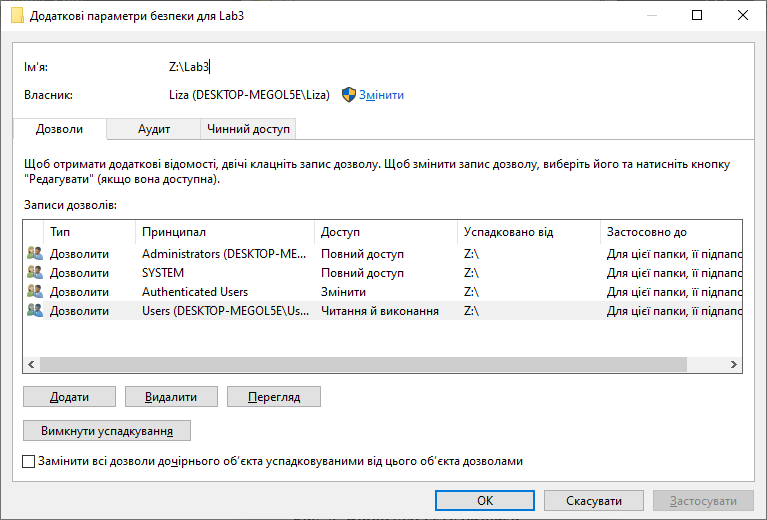


Рис. 4. Додаткові параметри налаштувань безпеки

Натискаємо «Додати» і вводимо ім’я об’єкта, якому надається доступ, а також виставляємо необхідні параметри.

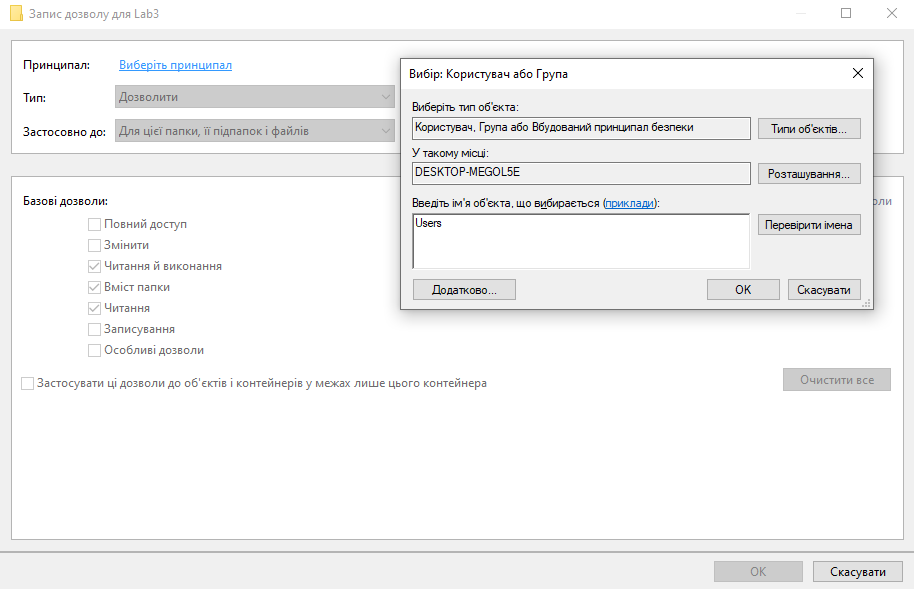


Рис. 5. Додавання користувача

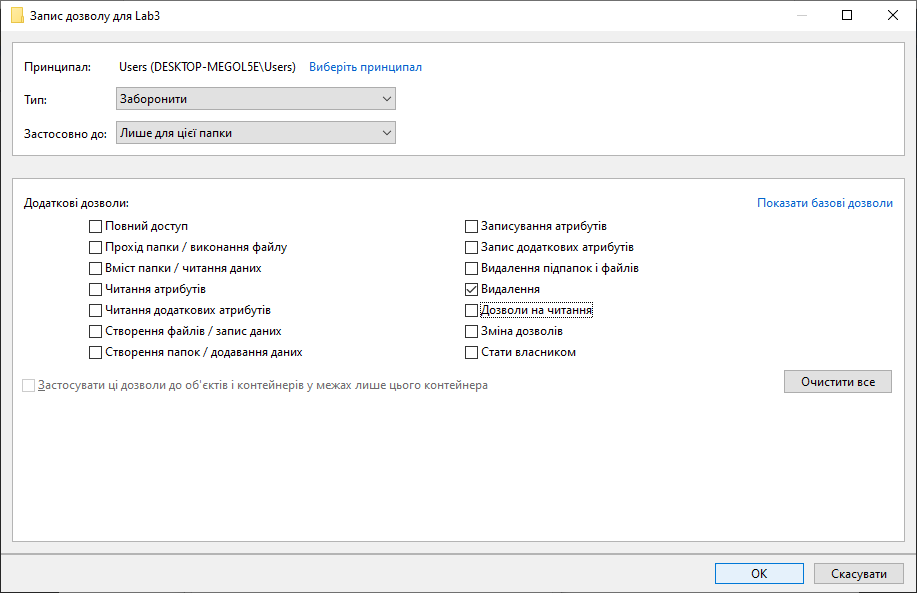


Рис. 6. Задання дозволів

2. Увійти до системи під іншим користувачем (за необхідності створивши його) та переконатися у неможливості видаляти цю папку (рис. 7), однак маючи змогу створювати в ній файли та підпапки. Створити таку підпапку; переконатись, що як власник об’єкту цей користувач має право на зміну усіх дозволів. Заборонити групі «Administrators» повний доступ до створеної підпапки.

Увійшовши від іншого користувача і натиснувши правою кнопкою миші на створеній папці, бачимо, що він не має права видалити дану папку. Проте, можна створити підпапку. Наприклад, folder1. Для неї ж забороняємо повний доступ Адміністраторам.

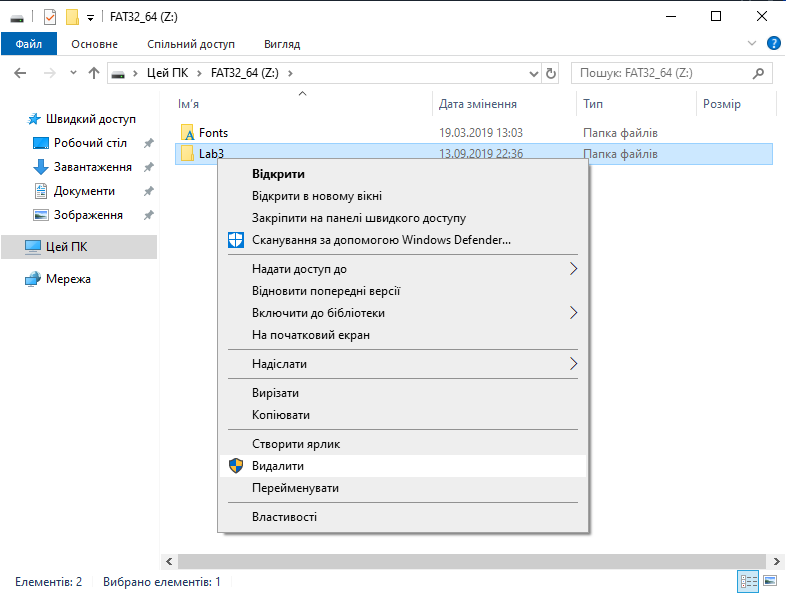


Рис. 7. Заборона видалення

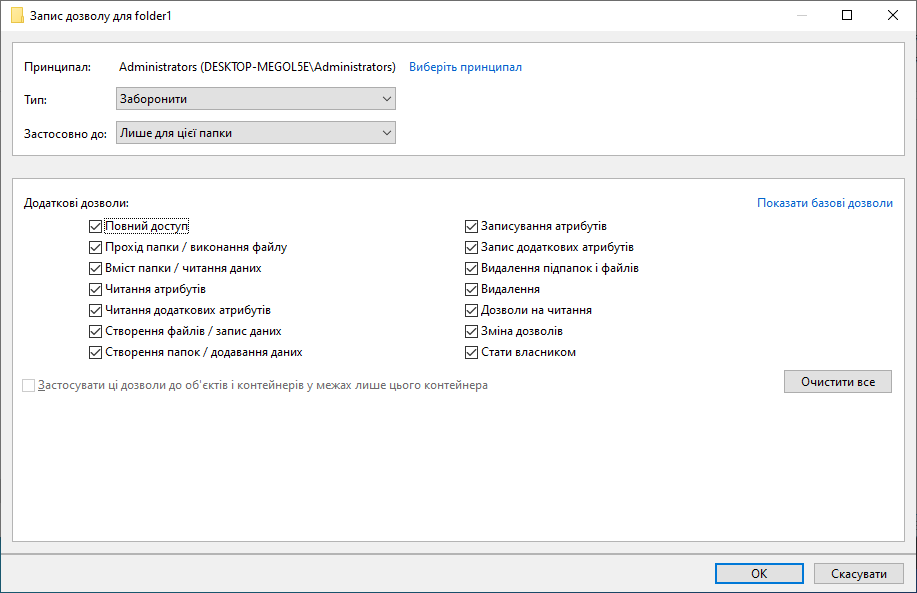


Рис. 8. Повна заборона доступу до підпапки

3. Увійти до системи як користувач з адміністративними повноваженнями. Переконатись у відсутності доступу до підпапки, створеної у ході виконання п. 2 лабораторної роботи. Зайти на вкладку "Безпека" властивостей об’єкту. У звіті до лабораторної роботи пояснити отримане повідомлення. В додаткових параметрах безпеки змінити власника папки (див рис. 1). Звернути увагу на можливість зміни власника як тільки для поточного об’єкту, так і для субконтейнерів і об’єктів. Переглянути список управління доступом після зміни власника – які суб’єкти та які права доступу є в цьому списку?

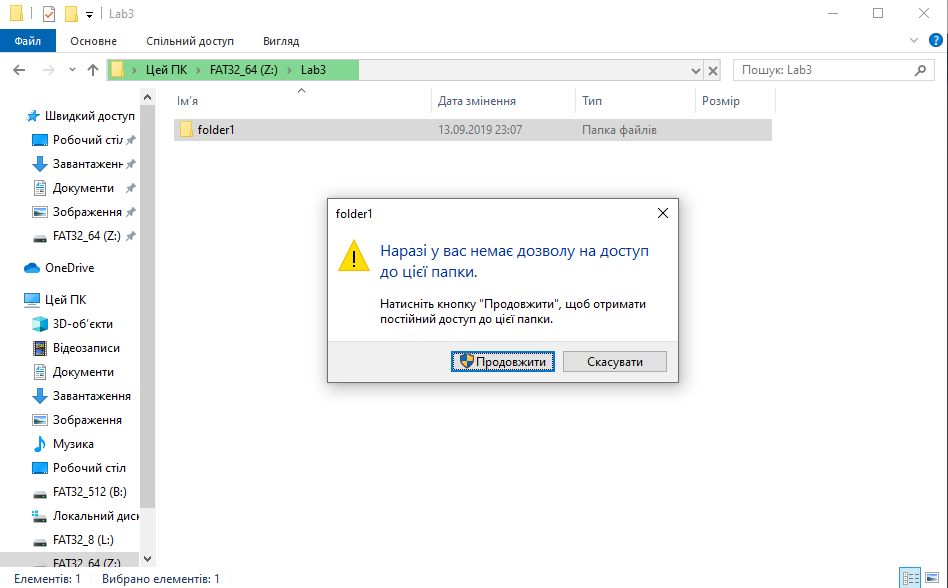


Рис. 9. Повідомлення системи про відмову в доступі на виконання операції

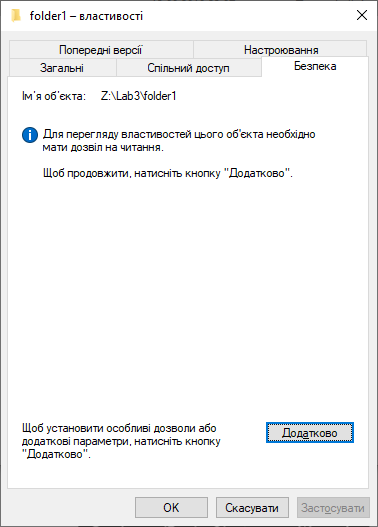


Рис. 10. Повідомлення системи безпеки

Змінимо власника папки у додаткових налаштуваннях безпеки, надавши доступ до неї Адміністраторам.

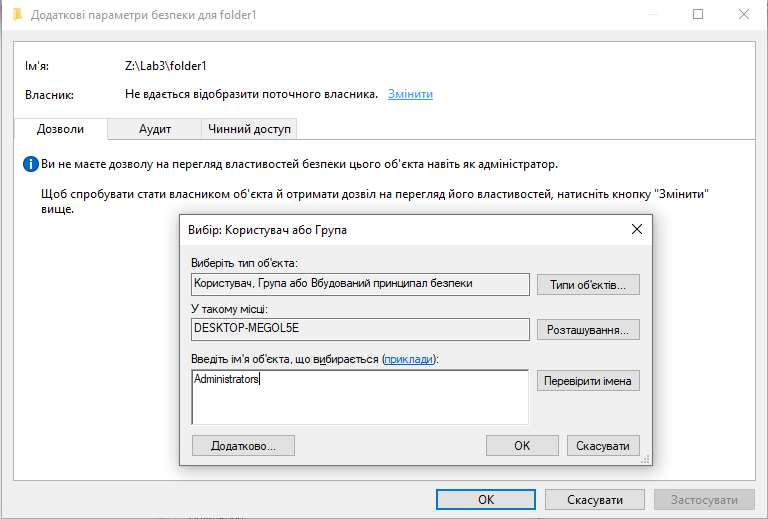


Рис. 11. Зміна налаштувань безпеки

Після цього буде додано власником Адміністратора.

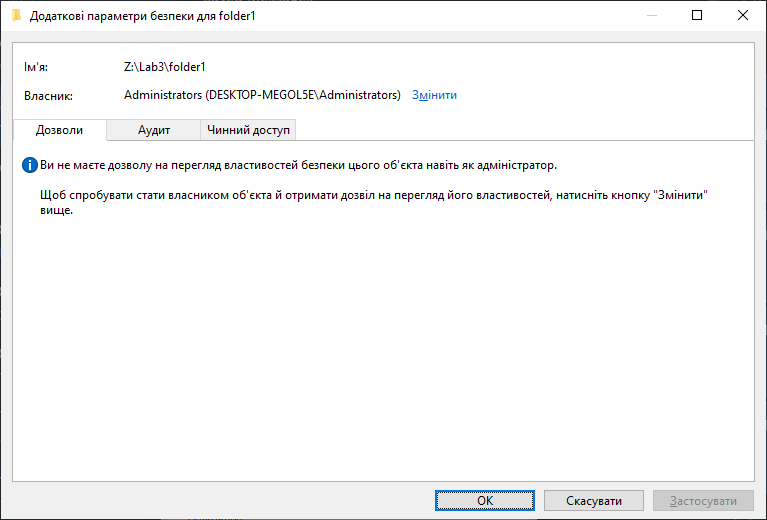


Рис. 12. Зміна власника

Натискаємо «Змінити» і бачимо що Адміністратори мають повний доступ до папки.

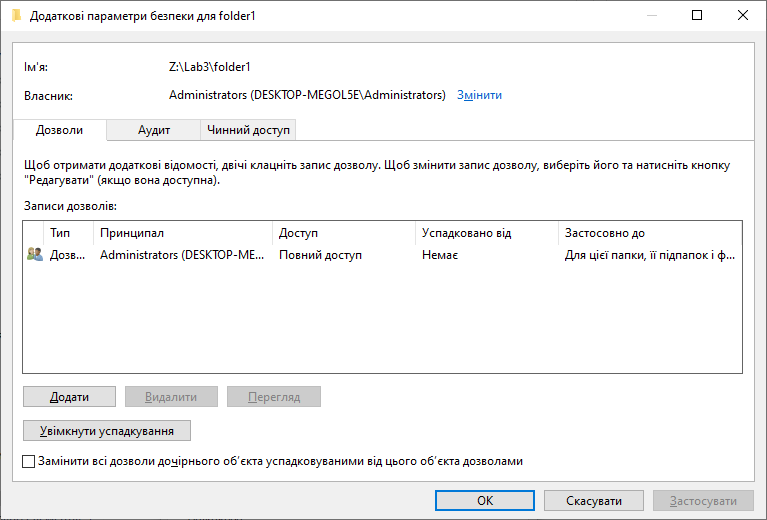


Рис. 13. Надання доступу

4. Для приведення налаштування безпеки усіх вкладених субконтейнерів і об’єктів до шаблонного зразка батьківської папки використати відмітку "Замінити всі дозволи дочірнього…" вкладки "Додатково" додаткових параметрів безпеки для папки (рис. 14).

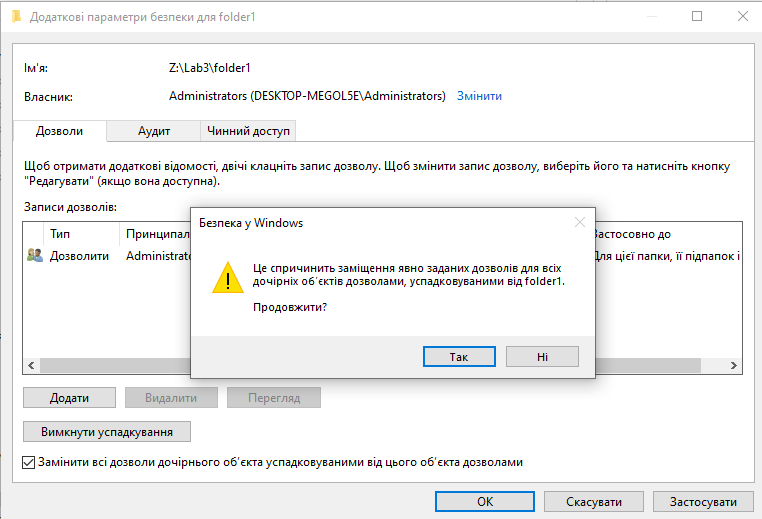


Рис. 14. Заміна дозволів

5. Користувачем з адміністративними правами перейти на вкладку "Квота" (рис. 15) властивостей NTFS тому (за необхідності конвертувати існуючий FAT том, або створити новий). Включити управління квотами у "м’якому" режимі. У вікні "Записи квоти" (рис. 16) скориставшись меню "Квота" створити індивідуальний запис квоти для певного користувача (рис. 18).

Увійти до системи під іншим користувачем. Записати на том з квотами файли сумарним обсягом більшим від порогу попереджень, але меншим за розмір квоти.

Увійти до системи під третім користувачем. Записати на том з квотами файли сумарним обсягом більшим за розмір квоти.

Користувачем з адміністративними правами переглянути записи квот для цього тому. Включити квоти у "жорсткому" режимі (для цього поставити відмітку «Заборонити користувачам перевищувати квоту місця на диску»).

Увійти до системи під іншим користувачем. Спробувати записати на том з квотами файли сумарним обсягом більшим за розмір квоти. Переконатись у неможливості такої операції.

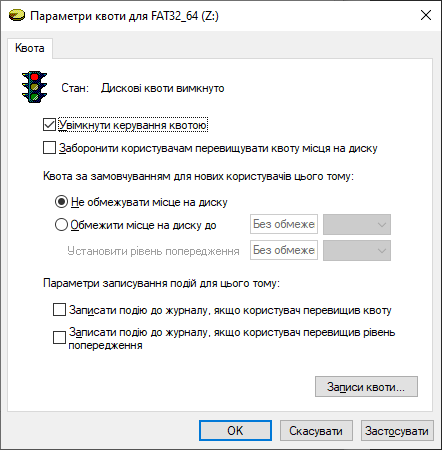
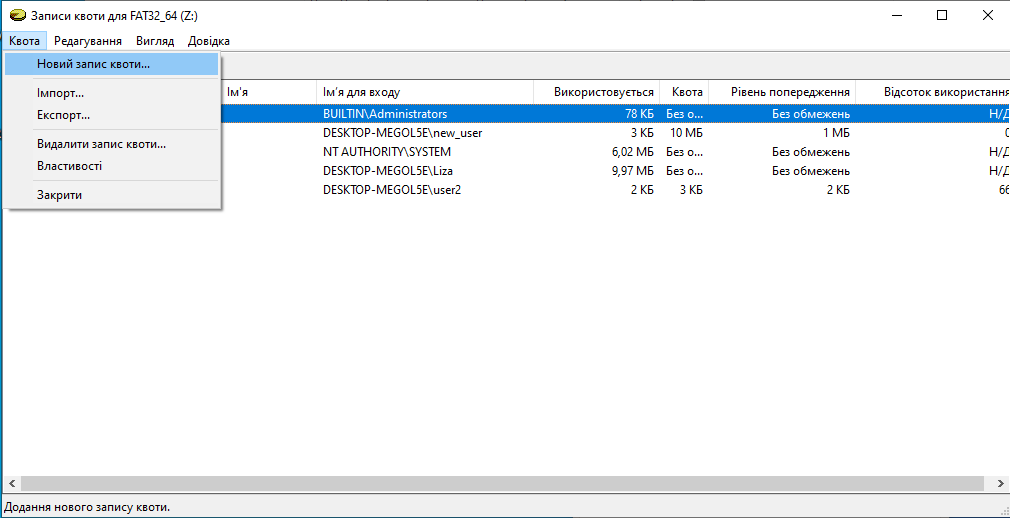


Рис. 15. Вкладка квот у властивостях дискового тому

 Рис. 16. Вікно записів квот для дискового тому.

Додамо користувача, якому необхідно встановити квоту.

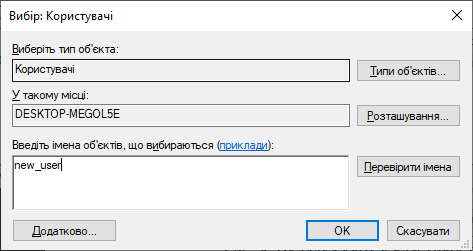


Рис. 17. Додавання користувача

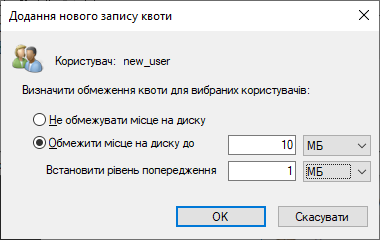


Рис. 18. Додавання квоти

Після цього увійдемо під іншими користувачами і запишемо на одному томі файл менший за встановлену квоту, але більший за поріг попередженя, а від іншого кристувача – більший за встановлену квоту.

Бачимо наступні записи.

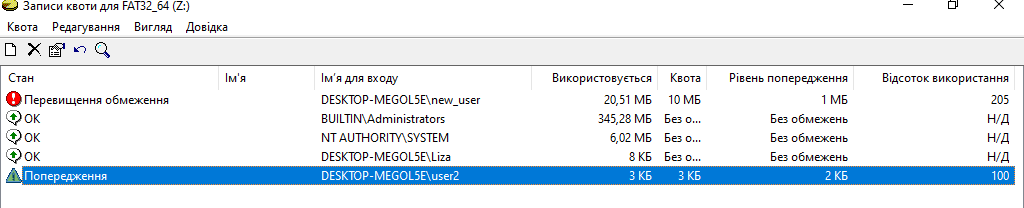


Рис. 19. Вікно записів квот для дискового тому (один користувач перевищив поріг квоти, а один – поріг попереджень)

Включимо квоту в жорсткомі режимі, поставивши галочку у відповідному пункті налаштувань («Заборонити користувачам перевищувати квоту місця на диску»).

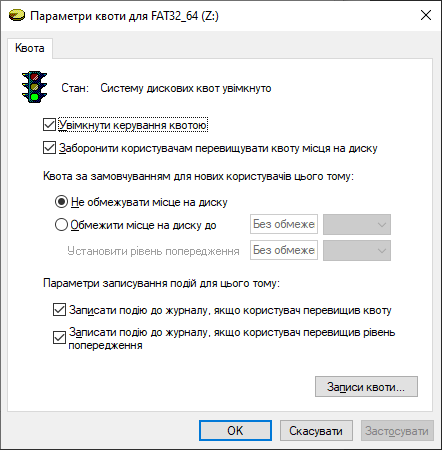


Рис. 20. Заборона перевищення квоти місця

Спробувавши створити текстовий файл від користувача, який перебільшив квоту, переконаємося, що це неможливо.



Рис. 21. Заборона операції

6. Створити агента відновлення шифрованих даних. Для цього виконати наступні кроки:

І. Створення сертифікату агента відновлення:

* Увійти в систему як адміністратор.
* У вікні консолі ввести команду cipher /R:Ім’яФайлу – без розширення (рис. 22).
* Ввести і підтвердити пароль, що захищає приватний ключ.

В поточному каталозі будуть створені два файли: з розширенням сer (містить тільки згенерований ключ) і з розширенням pfx (містить і ключ, і сертифікат агента відновлення).

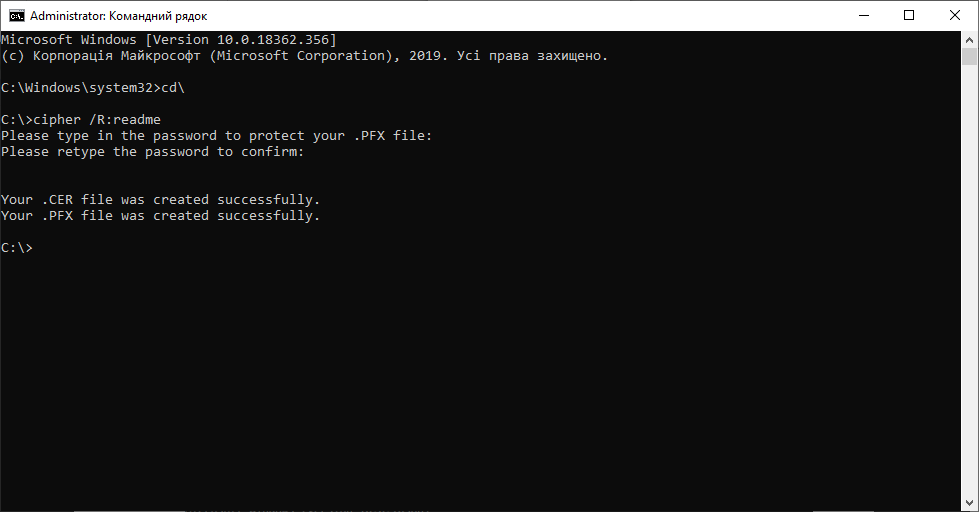


Рис. 22. Створення сертифікату агента відновлення

Бачимо, що створилися 2 файли.

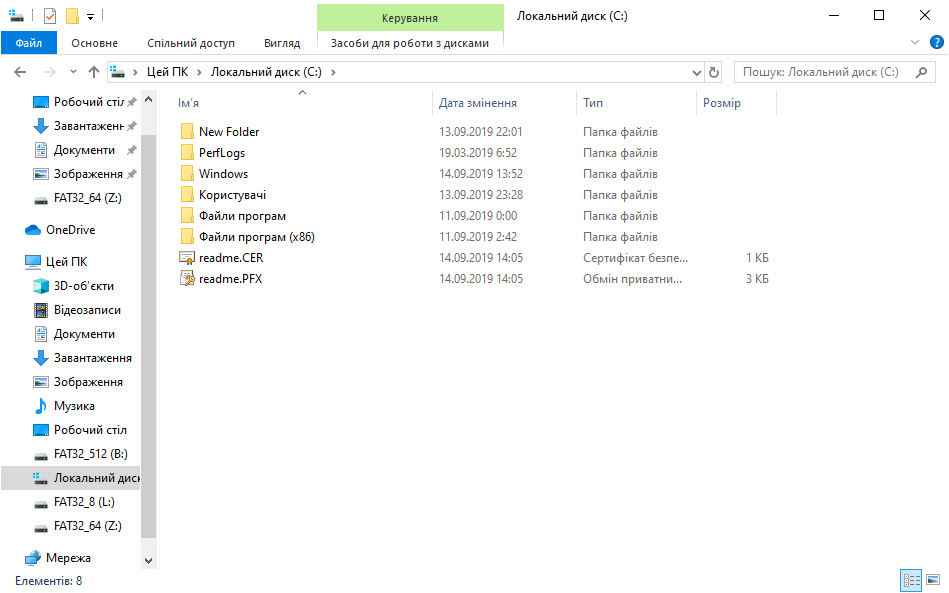


Рис. 23. Створені файли

ІІ. Імпорт сертифікату, за допомогою якого можна відновлювати індивідуальні файли користувачів:

* Відкрийте оснащення Certificates, вузол Personal (рис. 25).
* Імпортуйте створений РFХ-файл (зверніть увагу на розширення сертифікату!).

Відкрити оснащення можна, скориставшись пошуком.

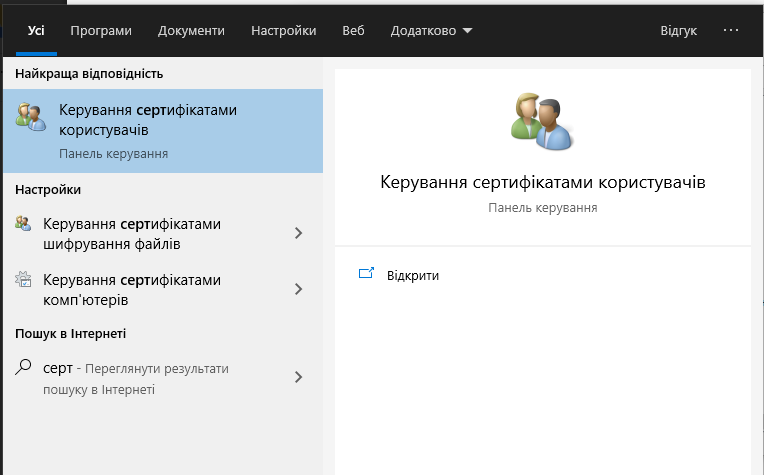


Рис. 24. Пошук оснащення

Відкриємо оснащення і, натиснувши правою кнопкою миші, викликаємо контекстне меню для імпорту файлу.

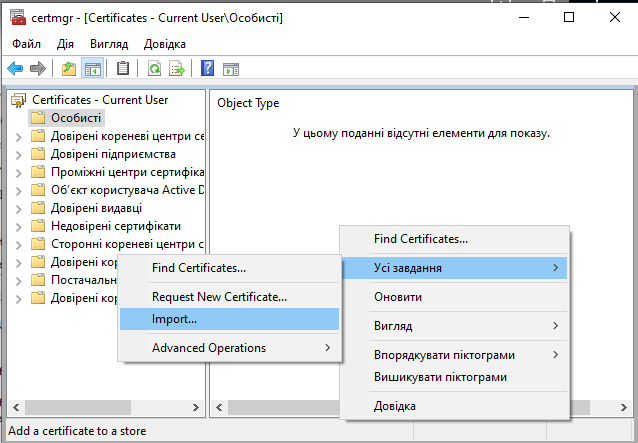


Рис. 25. Меню імпорту

Відкриється майстер імпорту сертифікатів.

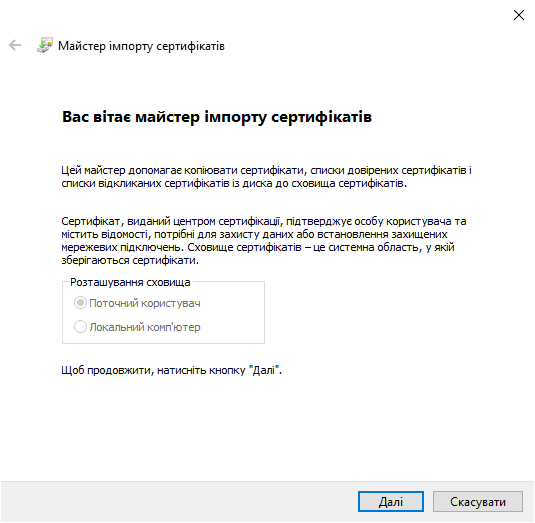


Рис. 26. Майстер імпорту сертифікатів

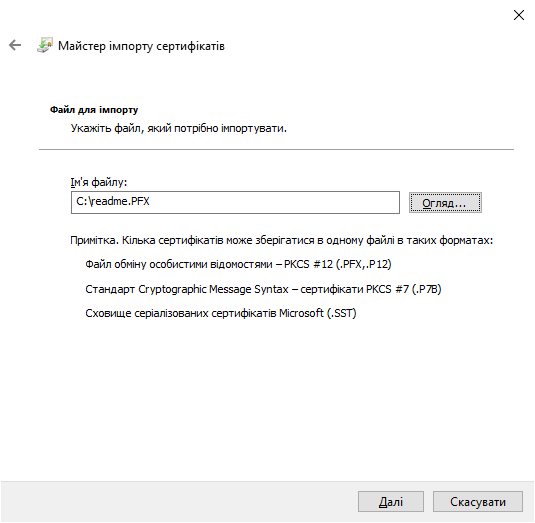


Рис. 27. Вибір файлу

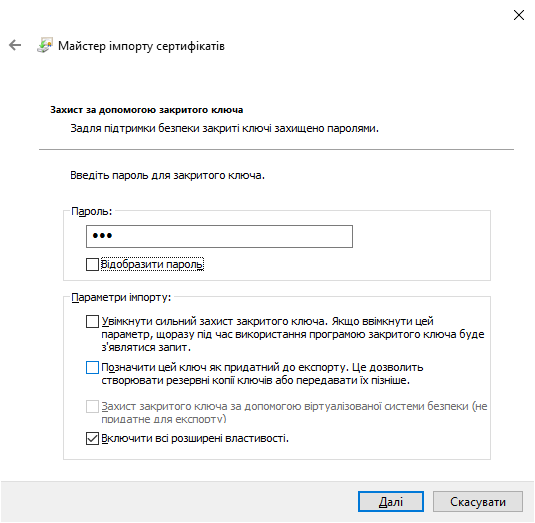


Рис. 28. Захист за допомогою паролю

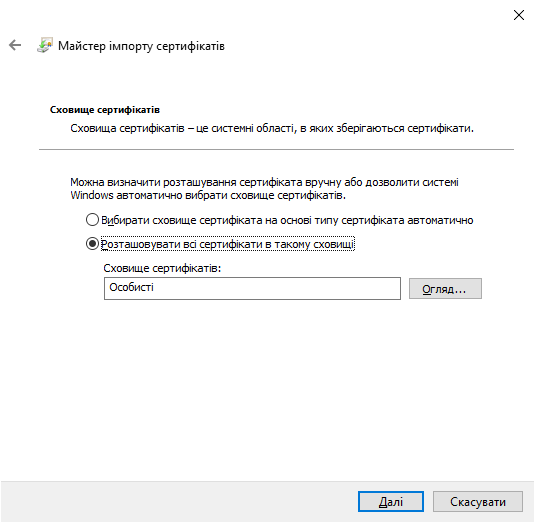


Рис. 29. Сховище сертифікатів

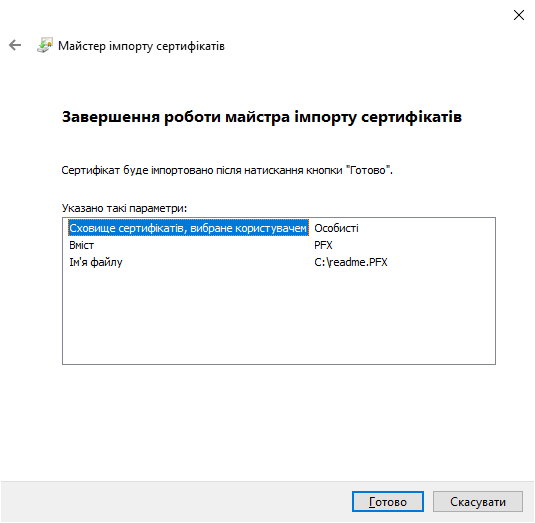


Рис. 30. Завершення роботи майстра імпорту сертифікатів

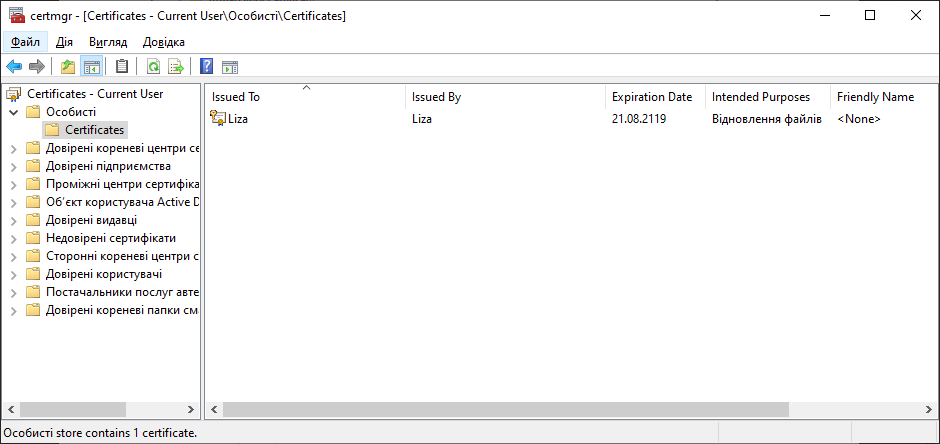


Рис. 31. Імпортований сертифікат

ІІІ. Призначення політики агента відновлення для операцій шифрування:

* Запустіть оснащення Group Policy.
* Виберіть вузол Public Key Policies | Encrypting File System.
* В контекстному меню виконайте команду Add Data Recovery Agent.
* У вікні майстра Welcome to the Add Data Recovery Agent Wizard.
* Натисніть кнопку Browse Folders і вкажіть шлях до створеного раніше файлу з розширенням сеr.
* Завершіть роботу майстра натиснувши кнопки Next та, на наступній сторінці, Finish.

Сертифікат буде імпортовано, а його власник стане агентом відновлення шифрованих даних на цьому комп’ютері. (Зверніть увагу, що в стовпчику Intendend Purposes імпортованого сертифікату вказано File Recovery).

Оснащення Групових політик можна знайти за допомогою пошуку.

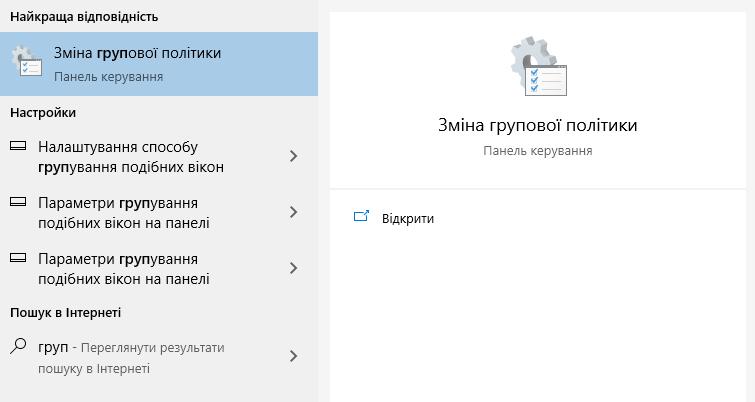


Рис. 32. Пошук групових політик

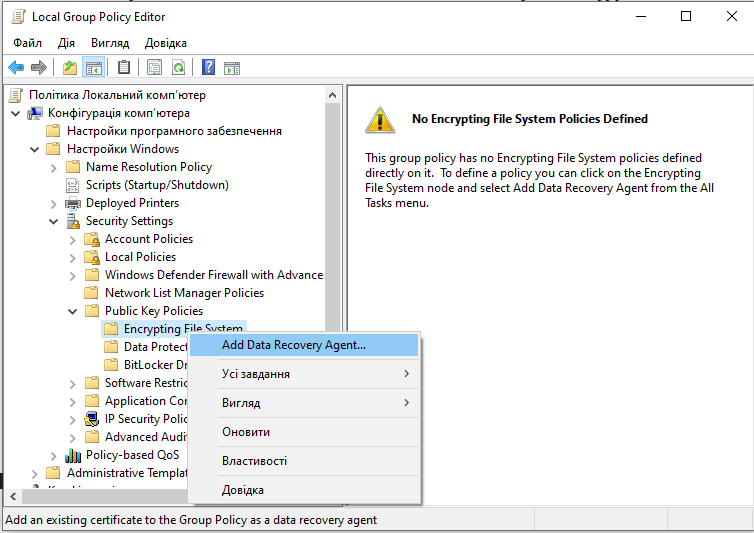
****

Рис. 33. Створення політики агента відновлення шифрованих даних

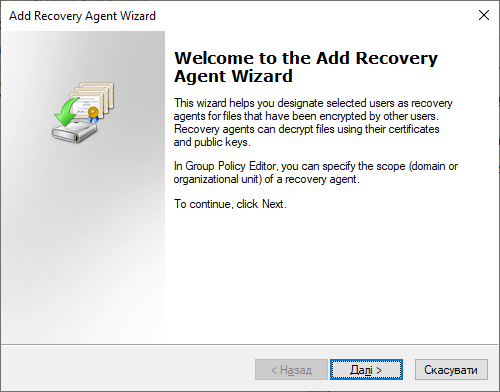


Рис. 34. Агент відновлення шифрованих даних

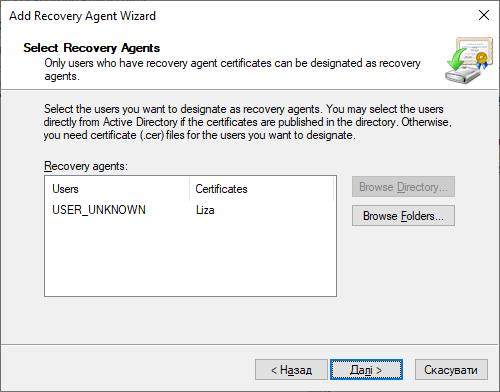


Рис. 35. Вибір файлу

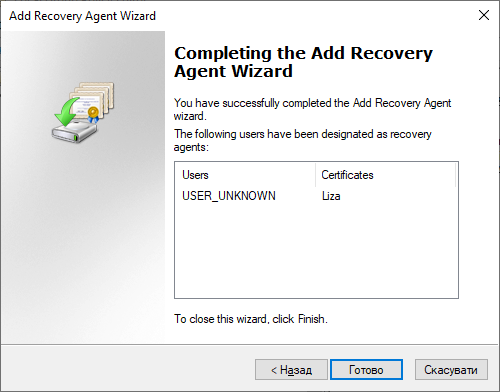


Рис. 36. Завершення роботи агента

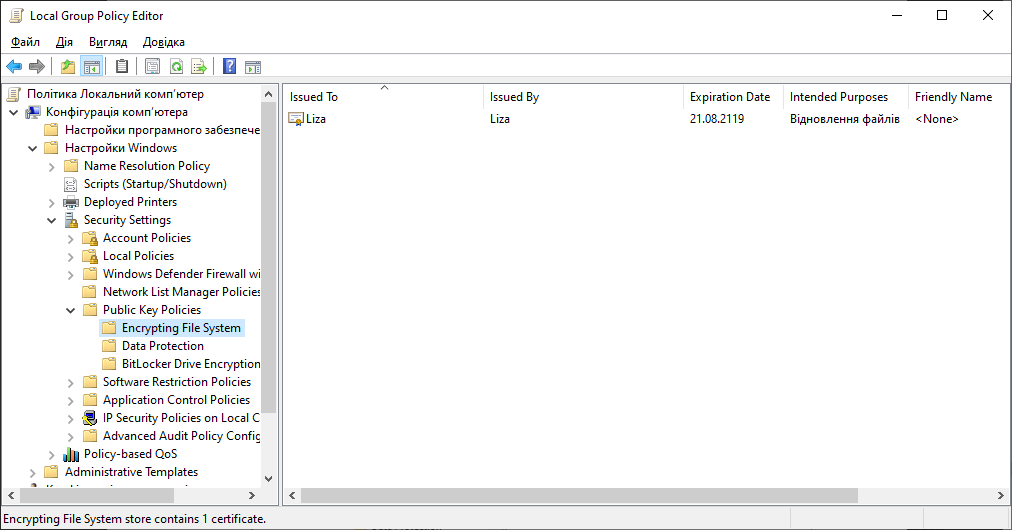


Рис. 37. Сертифікат

7. Увійшовши до системи під декількома користувачами зашифруйте по одному файлу для кожного користувача. Для цього у властивостях файлу (вкладка "General") натисніть кнопку "Додатково" і поставте відмітку "Шифрувати вміст для захисту даних". Переконайтесь, що кожен користувач може розшифрувати тільки свої файли, а після шифрування першого файлу створюється сертифікат з призначенням EFS (перевірити за допомогою оснащення Certificates).

Створюємо новий файл і шифруємо його.

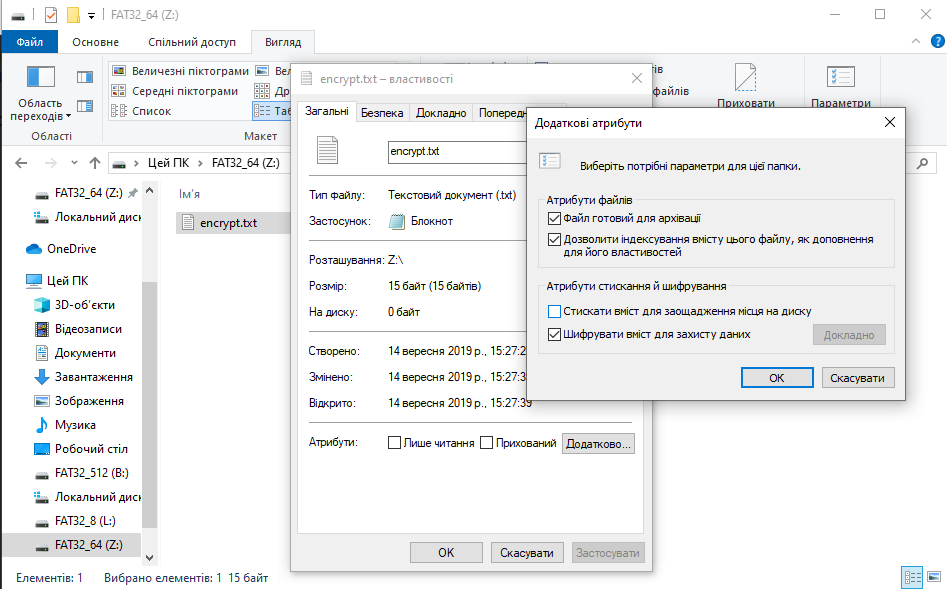


Рис. 38. Встановлення додаткових атрибутів файлу

За потреби спільного доступу декількох користувачів до одного шифрованого файлу у вікні додаткових атрибутів файлу оберіть кнопку «Додатково». Після цього у вікні «Користувачі, які мають доступ до цього файлу» можна додати користувачів, яким дозволено розшифровувати цей файл (основною умовою є наявність в системі сертифікатів цих користувачів). Крім того, зверніть увагу, що після призначення політики агента відновлення шифрованих даних у вікні деталей щодо шифрування кожного файлу міститься ім’я агента відновлення. Переконайтесь, що користувачі, яким дозволили спільний доступ, можуть читати (тобто розшифровувати) цей файл, в той як інші – ні.

(Якщо треба надати певному користувачу доступ до ВСІХ шифрованих файлів іншого користувача, можна експортувати сертифікат користувача, що надає свої файли – але обов’язково у pfx форматі – і імпортувати цей файл іншому користувачу для надання доступу).

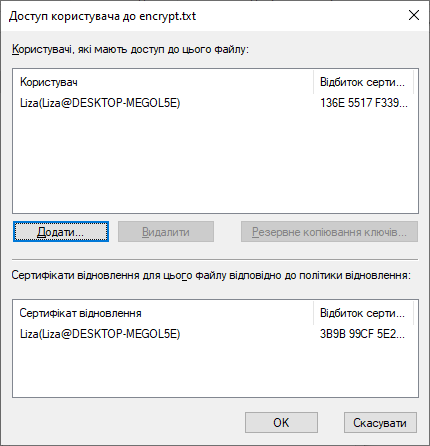


Рис. 39. Налаштування шифрованого файлу на спільний доступ декількох користувачів при діючій політиці агента відновлення

У звіті до лабораторних робіт описати та пояснити отримані результати.

**КОНТРОЛЬНІ ЗАПИТАННЯ**

1. Чим відрізняються дозволи «Modify» та «Write»?

2. Чи можна заборонити доступ до об’єктів файлової системи адміністратору комп’ютера?

3. Хто може брати об’єкти у власність?

4. Об’єкт файлової системи може брати у власність група «Administratos». Яке призначення такої можливості?

5. Чи можна призначити індивідуальний розмір квот для кожного користувача, групи?

6. Призначення файлової системи EFS.

7. Хто може розшифрувати файл, зашифрований іншим користувачем?

**ЛАБОРАТОРНА РОБОТА № 4**

**Тема роботи:** Реалізація механізму групових політик у Windows 10. Аналіз і налаштування безпеки.

**Мета роботи:** Ознайомлення зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері під управлінням ОС Windows 10. Навчитись використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.

**ТЕОРЕТИЧНІ ВІДОМОСТІ**

Групова політика – це технологія управління, що використовується для налаштування параметрів конфігурації робочих столів для груп комп’ютерів і користувачів. Групові політики можуть включати в себе параметри безпеки, параметри установки та підтримки програмного забезпечення і параметри для скриптів (сценаріїв), що управляють процесами завантаження і завершення роботи з системою. Групові політики зберігаються у вигляді об’єктів Group Policy (GPO), які, своєю чергою, зв’язуються з об’єктами Active Directory – сайтами, доменами чи організаційними одиницями (OU), крім того існує об’єкт локальної групової політики комп’ютера[[5]](#footnote-5).

Численні параметри, що визначаються в рамках об'єкту групової політики, розділено на дві частини. Одна частина параметрів використовується для конфігурації комп'ютера (computer configuration), інша частина параметрів використовується для конфігурації середовища користувача (user configuration). Конфігурація комп'ютера припускає визначення значень для параметрів, що впливають на формування оточення будь-яких користувачів, що реєструються на заданому комп'ютері. Конфігурація середовища користувача дає можливість управляти процесом формування оточення конкретного користувача, незалежно від того, на якому комп'ютері він реєструється в мережі.

Незалежно від типу конфігурації, параметри групової політики організовані в спеціальні категорії (рис. 1). Кожна з категорій параметрів групової політики визначає окрему область оточення користувача. Доступні категорії параметрів перераховані в табл. 1. Перераховані в таблиці категорії параметрів надають адміністратору доступ до різних механізмів конфігурації робочих станцій. У свою чергу категорії параметрів групової політики організовані в три контейнери відповідно до свого призначення:

* Software Settings (Конфігурація програм). У контейнері розміщуються категорії параметрів групової політики, за допомогою яких можна управляти переліком додатків, доступних користувачам;
* Windows Settings (Конфігурація Windows). У контейнері розміщуються категорії параметрів групової політики, що визначають налаштування безпосередньо самої операційної системи. Вміст цього контейнера може бути різним, залежно від того, на якому рівні визначаються параметри групової політики (для користувача або комп'ютера);
* Administrative Templates (Адміністративні шаблони). Цей контейнер містить категорії параметрів групової політики, які встановлюють правила на основі системного реєстру[[6]](#footnote-6).

Всі компоненти групової політики можна редагувати за допомогою Group Policy Editor.

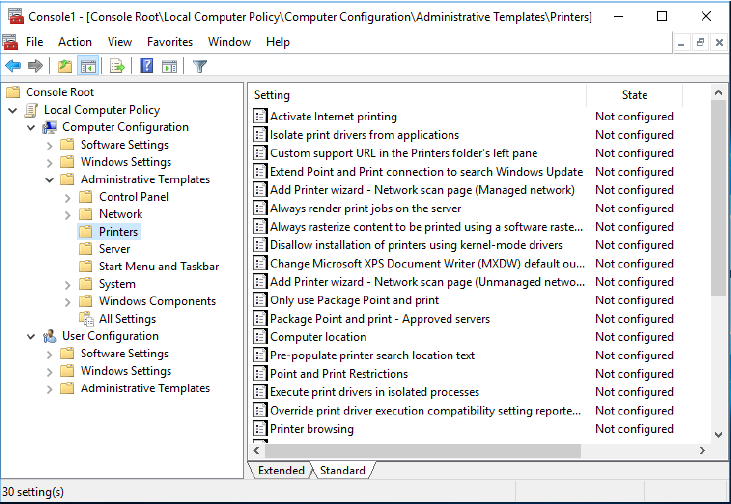


Рис. 1. Структура об'єкту групової політики

Таблиця 1. Категорії параметрів групової політики

|  |  |  |
| --- | --- | --- |
| **Категорія** | **Контейнер** | **Опис** |
| Software Installation | Software Settings | Ця категорія параметрів використовується для централізованого управління додатками, доступними на певному комп'ютері, або для певного [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. При цьому залежно від параметрів групової політики додатки можуть або встановлюватися примусово, або рекомендуватися для установки. |
| Remote Installation Service | Windows Settings | Ця категорія параметрів використовується для управління процесом віддаленої установки на клієнтському комп'ютері. Ця категорія параметрів доступна тільки у випадку конфігурації на рівні [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| Scripts | Windows Settings | Категорія використовується для визначення сценаріїв, які виконуватимуться при включенні/виключенні комп'ютера (Startup/Shutdown Scripts), або при реєстрації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а в системі чи його виході з неї (Logon/Logoff Scripts). |
| Security Settings | Windows Settings | Параметри цієї категорії використовуються для управління налаштуваннями безпеки клієнтського комп'ютера. Крім групової політики, адміністратор може також використовувати інші механізми для управління налаштуваннями безпеки. |
| Folder Redirection | Windows Settings | За допомогою параметрів цієї категорії адміністратор може налаштовувати процес перенаправлення папок з призначеного для [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а профілю (таких, наприклад, як My Documents) на деякий мережний ресурс. Ця категорія параметрів доступна тільки для конфігурації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| [Internet Explorer](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19618&displayformat=dictionary) Maintenance | Windows Settings | Параметри цієї категорії використовуються для налаштування [браузер](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19617&displayformat=dictionary)а [Internet Explorer](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19618&displayformat=dictionary" \o "Словник основних термінів: Internet Explorer). Ця категорія параметрів доступна тільки для конфігурації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| Windows Components | Administrative Templates | У цій категорії представлені параметри, за допомогою яких адміністратор може здійснювати управління налаштуваннями Windows-компонентів, встановлених на системі, що налаштовується. |
| Start Menu and Taskbar | Administrative Templates | Параметри цієї категорії дозволяють адміністратору налаштовувати головне меню і панель завдань клієнтського комп'ютера (насамперед, обмежувати доступну функціональність). Ця категорія параметрів доступна тільки для конфігурації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| Desktop | Administrative Templates | Параметри цієї категорії дозволяють адміністратору налаштовувати вигляд робочого столу клієнтського комп'ютера і його функціональність. Ця категорія параметрів доступна тільки для конфігурації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| Control Panel | Administrative Templates | Параметри цієї категорії дозволяють адміністратору управляти відображенням окремих компонентів панелі управління на клієнтському комп'ютері. Ця категорія параметрів доступна тільки для конфігурації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| Shared Folders | Administrative Templates | Параметри цієї категорії дозволяють управляти процесом публікації загальних папок. Ця категорія параметрів доступна тільки для конфігурації [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)а. |
| Networks | Administrative Templates | Ця категорія параметрів використовується для управління конфігурацією мережних компонентів системи. |
| System | Administrative Templates | У даній категорії представлені параметри, що дозволяють управляти настройками реєстру, що впливають на поведінку системи в цілому |
| Printers | Administrative Templates | Параметри цієї категорії використовуються для управління процесом публікації [принтер](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19635&displayformat=dictionary)ів. Ця категорія параметрів доступна тільки для конфігурації комп'ютера. |

**Побудова ієрархії об'єктів групової політики.** Параметри, визначені в рамках об'єкту групової політики, впливають тільки на ті об'єкти каталога, до яких вони застосовані. Щоб визначити множину об'єктів каталога, що підпадають під дію того або іншого об'єкту групової політики, необхідно виконати прив'язку останнього до одного або декількох контейнерів каталога. Для будь-якого об'єкту групової політики (за винятком локальних) дозволяється прив'язка до будь-якого з трьох класів об'єктів каталога – сайту, домена або підрозділу. Будь-які об'єкти, асоційовані з обліковими записами користувачів і комп'ютерів, що розташовуються всередині цих контейнерів, підпадають під дію прив'язаного об'єкту групової політики.

У випадку, коли в рамках дерева каталога є прив'язка декількох об'єктів групової політики, цілком можлива ситуація, коли деякі об'єкти каталога (або навіть всі) можуть підпадати під дію відразу декількох об'єктів групової політики. При цьому параметри, визначені в них, застосовуються до об'єктів каталога відповідно до певного порядку:

* спочатку застосовуються об'єкти групової політики, прив'язані до сайту, в якому знаходиться об'єкт каталога;
* після цього застосовуються об'єкти, прив'язані на рівні домена;
* останніми застосовуються об'єкти групової політики, прив'язані до організаційних одиниць.

Якщо є декілька вкладених організаційних одиниць, об'єкти групової політики застосовуються відповідно до рівнів вкладеності. В такому випадку йдеться про успадкування параметрів об'єктів вищого рівня групової політики (group policy inheritance).

Об'єкти групової політики, прив'язані до дочірніх контейнерів, можуть перевизначати параметри об'єктів групової політики, прив'язаних до об'єктів вищого рівня. В цьому випадку прийнято говорити про перевизначення (group policy overriding) параметрів об'єкту групової політики. При цьому успадковуються тільки ті параметри об'єктів групової політики, що були визначені для батьківського контейнера, але не визначені для дочірнього. Інакше значення параметрів, визначені в об'єкті групової політики, прив'язаному до об'єкту нижчого рівня групової політики, перевизначатимуть значення аналогічних параметрів об'єкту групової політики, прив'язаної до контейнера вищого рівня. Якщо деякий параметр об'єкту групової політики допускає безліч значень, значення параметра об'єкту групової політики батьківського контейнера доповнюють значення аналогічного параметра, визначеного в рамках об'єкту групової політики дочірнього контейнера.

**Оснащення "Security Templates".** За допомогою оснащення "Security Templates" можна створити політику безпеки для комп'ютера або мережі. Використовуючи це єдине оснащення, можна управляти всією безпекою системи. Оснащення "Security Templates" не надає нових параметрів безпеки, а просто впорядковує і надає зручний доступ до всіх наявних атрибутів безпеки для спрощення адміністрування.

При імпорті шаблону безпеки в об'єкт групової політики полегшується адміністрування домена, оскільки безпека настроюється для домена або підрозділу тільки один раз.

Щоб застосувати шаблон безпеки на локальному комп'ютері, можна використовувати засіб "Security Configuration and Analysis".

Шаблони безпеки можна використовувати, щоб визначити перелічені в табл. 2 елементи.

Таблиця 2. Елементи шаблонів безпеки

|  |  |
| --- | --- |
| **Область безпеки** | **Опис** |
| Політики облікових записів | [Політика](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=4385&displayformat=dictionary) паролів, [політика](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=4385&displayformat=dictionary) блокування облікового запису і [політика](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=4385&displayformat=dictionary) Kerberos |
| Локальні політики | [Політика](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=4385&displayformat=dictionary) аудиту, призначення прав [користувач](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19623&displayformat=dictionary)ів і параметри безпеки |
| Журнал подій | Параметри журналів подій додатків, системних подій і подій безпеки |
| Групи з обмеженим доступом | Участь в групах безпеки |
| Системні служби | Запуск і дозволи для системних служб |
| Реєстр | Дозволи для розділів реєстру |
| [Файлова система](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19639&displayformat=dictionary) | Дозволи для [файл](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8652&eid=19626&displayformat=dictionary)ів і папок |

Всі шаблони зберігаються в текстових файлах з розширенням .inf. Це дозволяє копіювати, вставляти, імпортувати і експортувати будь-які атрибути шаблону. У шаблоні безпеки можуть зберігатися всі атрибути безпеки, за виключенням політик безпеки IP і політик відкритого ключа.

**Нові і готові шаблони**

Можна створювати шаблони безпеки, що відповідають вимогам користувача, або використовувати готові шаблони. Перед зміною параметрів безпеки необхідно визначити параметри безпеки системи, що використовуються за умовчанням, а також їх призначення.

У Windows XP існувало декілька готових шаблонів, які рекомендується використовувати для захисту системи залежно від потреб конкретного користувача. Ці шаблони використовуються для виконання наступних дій:

* Відновлення параметрів за умовчанням (Setup security.inf);
* Впровадження середовища підвищеного захисту (Hisecws.inf);
* Впровадження середовища з нижчим рівнем захисту, але з більшою сумісністю (Compatws.inf);
* Захист кореневого каталога системи (Rootsec.inf).

**Готові шаблони безпеки**

Готові шаблони безпек[[7]](#footnote-7)и є відправною точкою в створенні політик безпеки, які налаштовуються для задоволення вимог організації. Після налаштування готових шаблонів безпеки ці шаблони можна використовувати для зміни конфігурації одного комп'ютера або безлічі комп'ютерів[[8]](#footnote-8). Змінити конфігурацію комп'ютерів можна за допомогою оснащення "Security Configuration and Analysis", утиліти командного рядка Secedit.exe, а також за допомогою імпорту шаблону в оснащення "Local Computer Policy". Можна змінювати конфігурацію декількох комп'ютерів, імпортувавши шаблон в компонент "Security Configuration", що є розширенням оснащення "Group Policy". На основі шаблонів безпеки можна також виконувати аналіз можливих слабких місць безпеки і порушень політики системи за допомогою оснащення "Security Configuration and Analysis" За умовчанням готові шаблони безпеки збережені в розташуванні: %systemroot%\Security\Templates.

* **Безпека за умовчанням (Setup security.inf)**

Шаблон Setup security.inf є шаблоном для конкретного комп'ютера і містить параметри безпеки, використовувані за умовчанням, які застосовуються під час установки операційної системи, включаючи дозволи для файлів кореневого каталога системного диска. Цей шаблон можна використовувати повністю або частково з метою аварійного відновлення. Шаблон Setup security.inf не можна застосовувати за допомогою оснащення "Групова політика".

* **Сумісний (Compatws.inf)**

Дозволи за умовчанням для робочих станцій і серверів спочатку створюються для їх локальних груп: "Administrators", "Power Users" і "Users". Члени групи "Administrators" володіють найбільшими правами тоді як члени групи "Users" – якнайменшими. З цієї причини можна значно підвищити безпеку, надійність і понизити загальну вартість володіння системою, якщо дотримуватися наступних правил:

* переконатися, що кінцеві користувачі є членами групи "Users";
* упровадити додатки, які можуть успішно запускатися і виконуватися членами групи "Users".

Особи, що мають права групи "Users", можуть успішно працювати із додатками, сертифікованими для Windows. Проте такі користувачі швидше за все не зможуть запускати не сертифіковані для Windows додатки. Якщо необхідно забезпечити підтримку не сертифікованих додатків, існують дві можливості:

* Всі члени групи "Users" повинні також бути членами групи "Power Users".
* Використовувати додаткові дозволи за умовчанням, створені для групи "Users".

Оскільки члени групи "Power Users" володіють успадкованими можливостями, такими як створення користувачів, груп, принтерів і загальних ресурсів, деякі адміністратори вважають за краще надати додаткові дозволи групі "Users", замість зарахування кінцевих користувачів в групу "Power Users". Для цих цілей служить "Сумісний" шаблон. За допомогою цього шаблону змінюються дозволи для файлів і реєстру, використовувані за умовчанням, створені для групи "Users", які відповідають вимогам більшості не сертифікованих застосувань. Крім того, оскільки після застосування сумісного шаблону користувачі не повинні приєднуватися до групи "Power Users", всі члени групи "Power Users" віддаляються.

Сумісний шаблон не слід застосовувати до комп'ютерів, які є контролерами домена. Наприклад, не слід імпортувати сумісний шаблон в стандартний домен або в об'єкт групової політики стандартного контролера домена.

* **Захист (Secure\*.inf)**

У шаблоні "Security" визначаються параметри підвищеної безпеки. Найменш імовірно, що вони впливають на сумісність. Наприклад, в шаблоні "Захист" визначаються параметри надійних паролів, блокування і аудиту.

Крім цього, шаблоном "Захист" обмежується використання LAN Manager і протоколів перевірки достовірності NTLM шляхом налаштування клієнтів на відправку відповідей у форматі NTLMv2.

Шаблони безпеки також визначають додаткові обмеження для анонімних користувачів та включають підписування пакетів SMB на сервері, яке за умовчанням відключено для робочих станцій і серверів.

* **Підвищений захист (hisec\*.inf)**

Група шаблонів підвищеного захисту включає шаблони, що накладають додаткові обмеження на рівні шифрування і підпису, необхідні для перевірки достовірності і для даних, що передаються по безпечним каналам між клієнтами SMB і серверами. Наприклад, тоді як параметри шаблонів безпеки визначають відмову серверів від відповідей LAN Manager, параметри шаблонів підвищеного захисту визначають відмову серверів як від відповідей LAN Manager, так і від відповідей NTLM. Шаблон захисту включає підписання пакетів SMB на сервері, а для шаблону підвищеного захисту таке підписання є необхідним. Для шаблонів підвищеного захисту є необхідним надійне кодування і підпис для даних, що передаються по безпечному каналу між доменом і членом домена і між двома доменами, між якими встановлені довірчі відносини.

Крім обмежень на використання протоколів LAN Manager і вимог шифрування і підпису даних SMB і потоку даних безпечного каналу шаблони підвищеного захисту також обмежують використання кешованих даних входу в систему, таких як дані, збережені за допомогою Winlogon і засобу "Збереження імен користувачів і паролів".

Крім цього, в шаблоні Hisecws параметри групи обмеженого доступу використовуються для виконання наступних дій:

* Видалення всіх членів групи "Power Users".
* Перевірка того, що тільки адміністратори домена і локальні облікові записи адміністратора є членами локальної групи "Administrators".

Шаблоном Hisecws визначаються ці обмеження для груп при виконанні тільки сертифікованих для Windows 2000 додатків. При роботі тільки з сертифікованими додатками ані небезпечні сумісні шаблони, ані небезпечна група "Power Users" не є необхідними. Користувачі можуть успішно працювати з сертифікованими додатками в безпечному контексті звичного користувача, який визначається параметрами безпеки за умовчанням файлової системи і реєстру.

* **Безпека системного кореневого каталога (Rootsec.inf)**

Шаблоном Rootsec.inf визначаються нові дозволи для кореневого каталога Windows 10. За умовчанням ці дозволи визначаються шаблоном Rootsec.inf для кореневого каталога системного диска. Цей шаблон можна використовувати, щоб повторно застосувати дозволи для кореневого каталога, якщо вони були випадково змінені. Шаблон також може бути змінений для застосування цих дозволів для кореневого каталога до інших томів. Шаблоном не перевизначаються явні дозволи, визначені для всіх дочірніх об'єктів. Шаблоном розповсюджуються тільки успадковані дочірніми об'єктами дозволи.

* **Відсутність SID користувача серверу терміналів (Notssid.inf)**

Стандартні таблиці управління доступом до файлової системи і реєстру, розташовані на серверах, надають дозволи для SID (Secuity ID) сервера терміналів. SID сервера терміналів використовується, тільки якщо цей сервер запущений в режимі сумісності додатків. Якщо сервер терміналів не використовується, цей шаблон може бути застосований для видалення непотрібних SID сервера терміналів з файлової системи і реєстру. Проте, видалення запису управління доступом для SID сервера терміналів з файлової системи і реєстру не підвищує безпеку системи. Замість видалення SID сервера терміналів слід запустити сервер терміналів в режимі повної безпеки. При роботі в режимі повної безпеки SID сервера терміналів не використовується.

**Щоб імпортувати[[9]](#footnote-9) шаблон безпеки:**

1. Відкрийте оснащення "Security Configuration and Analysis". У дереві консолі клацніть правою кнопкою миші вузол "Security Configuration and Analysis".

2. Виберіть команду "Import Template".

3. (Необов'язково) Для видалення з бази даних від всіх збережених раніше шаблонів встановіть відмітку "Clear this database before importing".

4. Клацніть файл шаблону і натисніть кнопку "Open".

5. Повторіть попередній крок для всіх шаблонів, для яких вимагається виконати злиття з базою даних.

**Щоб виконати аналіз безпеки системи:**

1. Відкрийте оснащення "Security Configuration and Analysis"

2. У дереві консолі клацніть правою кнопкою миші вузол " Security Configuration and Analysis " і виберіть команду "Open database".

3. У діалоговому вікні "Open database" даних виконайте одну з наступних дій:

* щоб створити нову базу даних, введіть ім'я в полі "Name file" і натисніть кнопку "Open";
* щоб відкрити існуючу базу даних, виберіть базу даних і натисніть кнопку "Open".

4. Якщо створюється нова база даних, в діалоговому вікні "Import Template " виберіть шаблон і натисніть кнопку "Open".

5. У області відомостей клацніть правою кнопкою миші вузол " Security Configuration and Analysis " і виберіть команду "Analyze Computer".

6. Виконайте одну з наступних дій:

* для використання стандартного журналу в групі "The path of the log file errors" натисніть кнопку "OK";
* для вибору іншого журналу введіть в полі " The path of the log file errors " допустимі шлях і ім'я файлу.

**Щоб налаштувати безпеку системи:**

1. Відкрийте оснащення "Security Configuration and Analysis"

2. У дереві консолі клацніть правою кнопкою миші вузол "Security Configuration and Analysis" і виберіть команду "Open database".

3. У діалоговому вікні "Open database" виконайте одну з наступних дій:

* щоб створити нову базу даних, введіть ім'я в полі "Name file" і натисніть кнопку "Open";
* щоб відкрити існуючу базу даних, виберіть базу даних і натисніть кнопку "Open".

4. Якщо створюється нова база даних, в діалоговому вікні "Import Template" виберіть шаблон і натисніть кнопку "Open".

5. У дереві консолі клацніть правою кнопкою миші вузол "Security Configuration and Analysis" і виберіть команду "Configure Computer".

6. Виконайте одну з наступних дій:

* для використання стандартного журналу в групі "The path of the log file errors" натисніть кнопку "OK";
* для вибору іншого журналу введіть в полі "The path of the log file errors" допустимі шлях і ім'я файлу.

**ЗАВДАННЯ ДО ВИКОНАННЯ РОБОТИ\***

**\*Використовувати своє ім’я або будь-який інакший ідентифікатор при іменуванні папок, файлів і т.д.**

1. Відкрити оснащення mmc "Group Policy". Перейти в гілку "Password Policy" (рис. 2), задати мінімальну довжину пароля (рис. 3). Після цього спробувати змінити власний пароль на такий, довжина якого менша за вказану в політиці, переконатись в неможливості такої дії (рис. 5). Повторити такі дії з параметрами "Password must meet complexity requirements" та "Store passwords using reversible encryption".

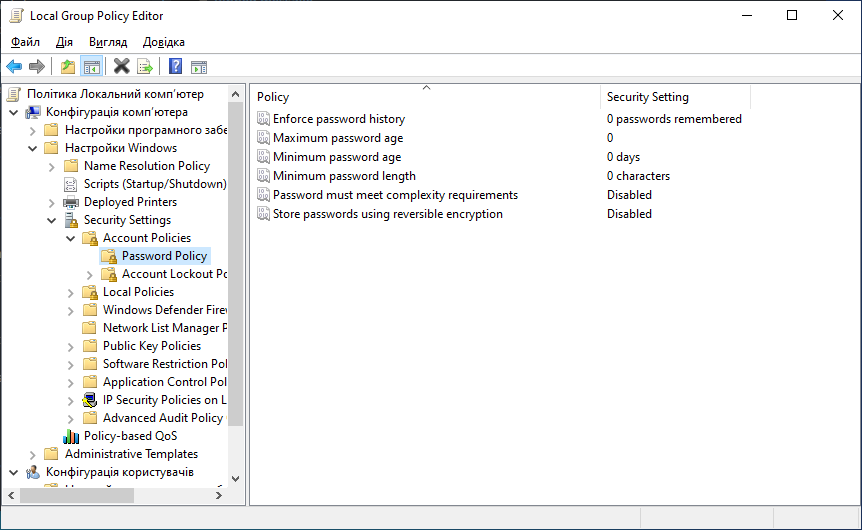


Рис. 2. Оснащення "Group Policy"

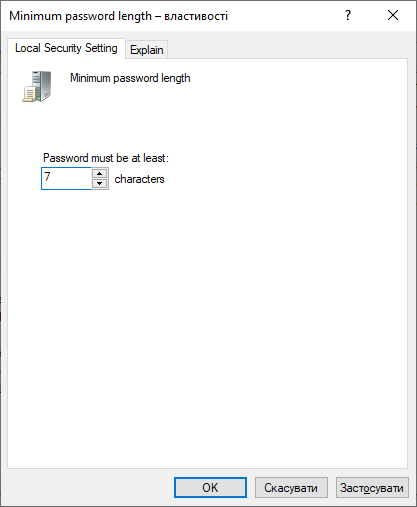


Рис. 3. Властивості параметру безпеки

Змінимо або створимо новий пароль для користувача в системі.

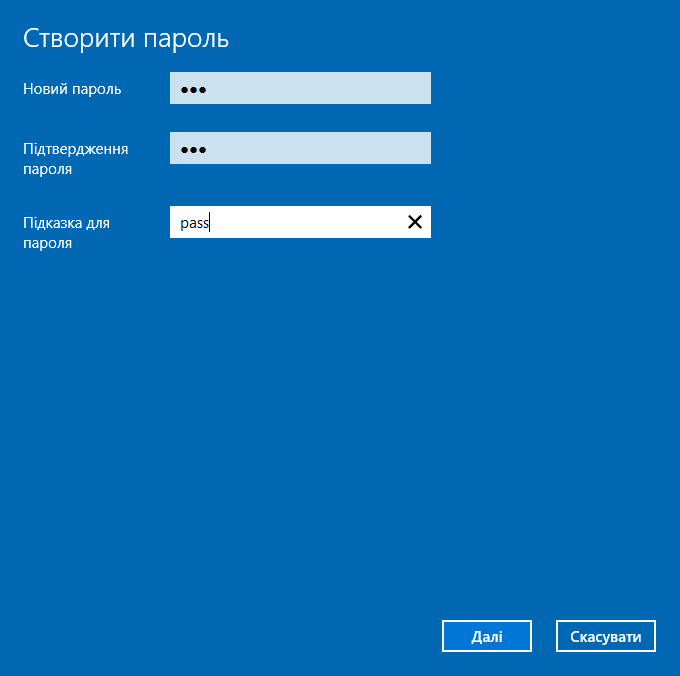


Рис. 4. Зміна паролю

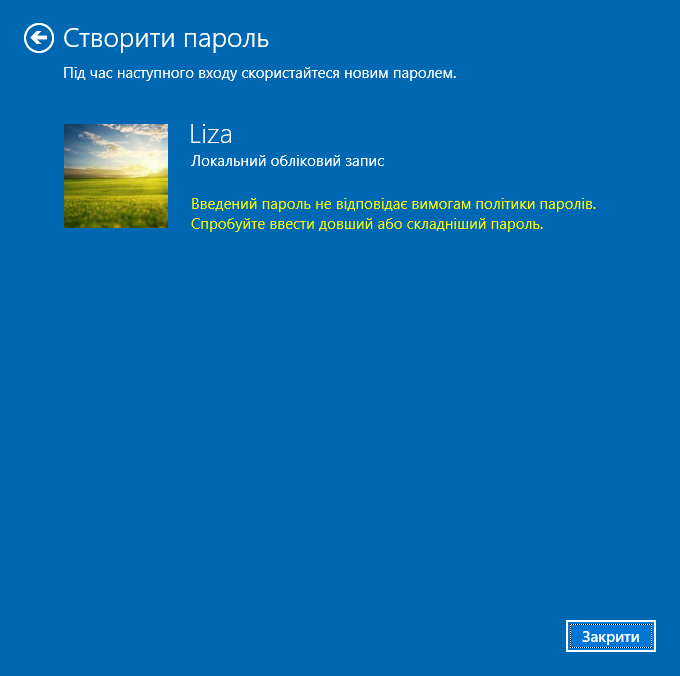


Рис. 5. Повідомлення системи про невідповідність параметру значенню політики

1. Перейти в гілку "Account lockout threshold" (рис. 6), задати граничне значення блокування (рис. 7). Після цього спробувати декілька разів зайти в систему з неправильним вводом пароля – переконатись у спрацюванні блокування (рис. 8). Увійти в систему як адміністратор – зняти блокування вручну з оснастки "Local Users and Groups" у властивостях заблокованого облікового запису (рис. 10).

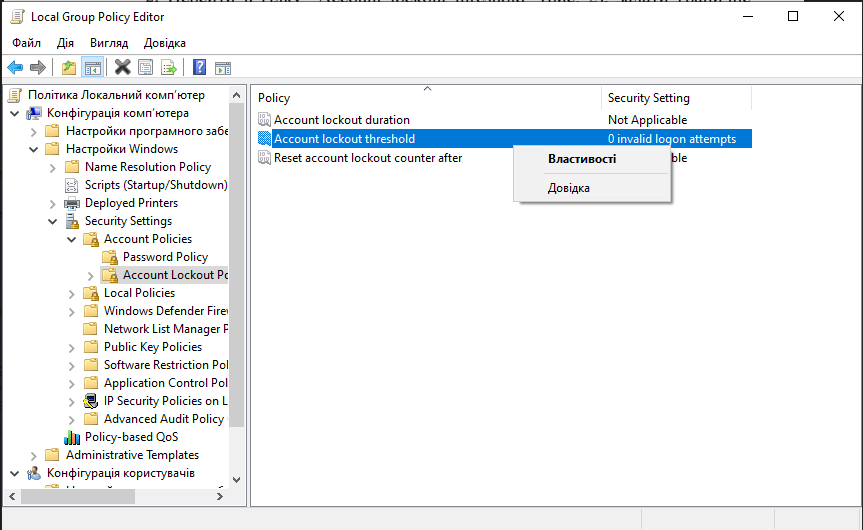


Рис. 6. Account lockout threshold



Рис. 7. Встановлення граничного значення блокування облікового запису

Введемо неправильний пароль для користувача 3 рази.

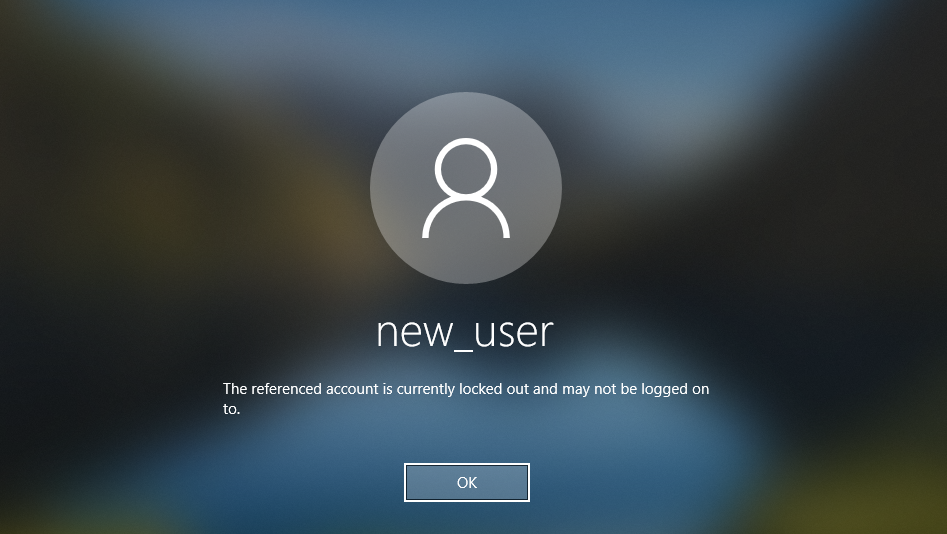


Рис. 8. Повідомлення системи про блокування облікового запису

Перейдемо у властивості заблокованого користувача.

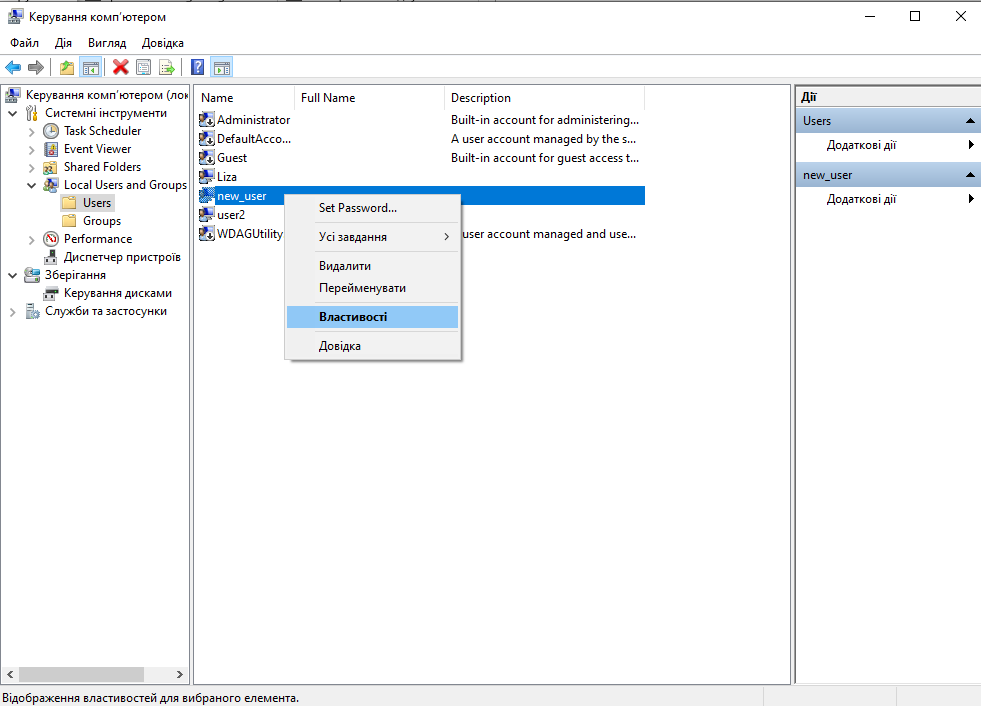


Рис. 9. Перехід у властивості користувача

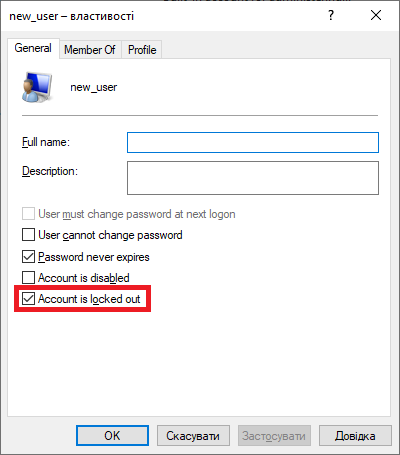


Рис. 10. Властивості заблокованого облікового запису

1. Налаштування привілеїв користувачів. Перейти в гілку "Local Policies | User Rights Assignment" (рис. 11), задати привілей на вимкнення комп’ютера тільки для групи адміністраторів (рис. 12). За необхідності перезавантажте комп’ютер. Увійти до системи як користувач без адміністративних привілеїв; переконатись, що пункт "Shut down" зник з меню "Start", крім того завершення роботи системи з командного рядка теж неможливе (рис. 13).

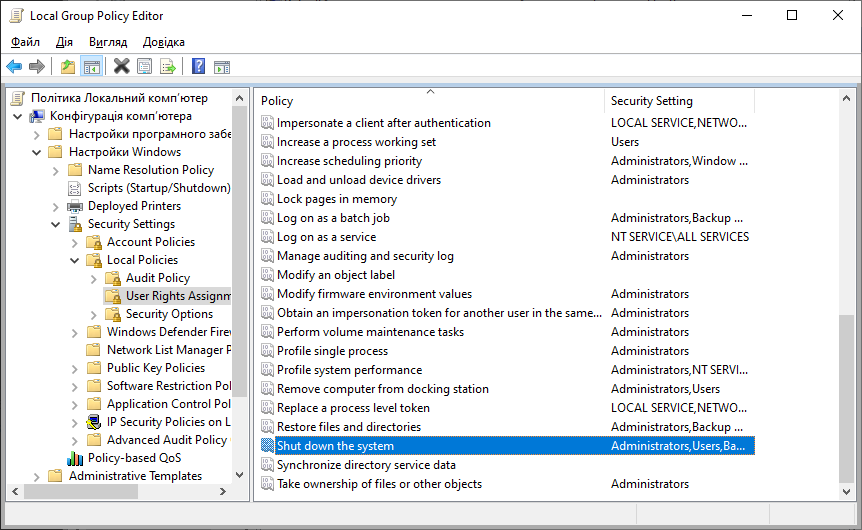


Рис. 11. Призначення прав користувачів за допомогою групової політики

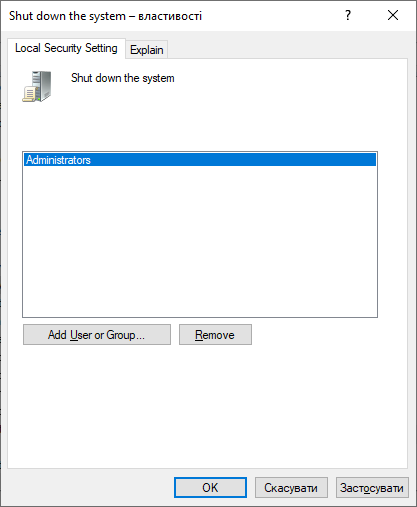


Рис. 12. Властивості параметру прав користувачів на завершення роботи системи

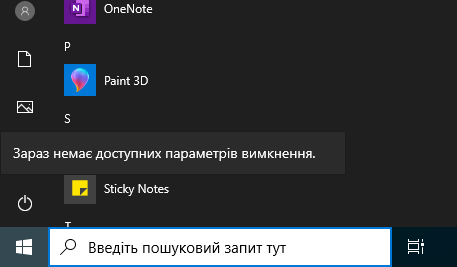


Рис. 13. Результат виконання політики стосовно заборони користувачу завершення роботи системи

1. Оглянути вміст гілки "Administrative Templates" як для частини "Computer Configuration", так і "User Configuration". В гілці "Control Panel | Display" увімкнути політику видалення значка "Display" з панелі управління (рис. 14). За необхідності перезавантажити комп’ютер. Спробувати змінити параметри екрану (рис. 15). Переконатись, що політики діють на усіх користувачів локальної системи.

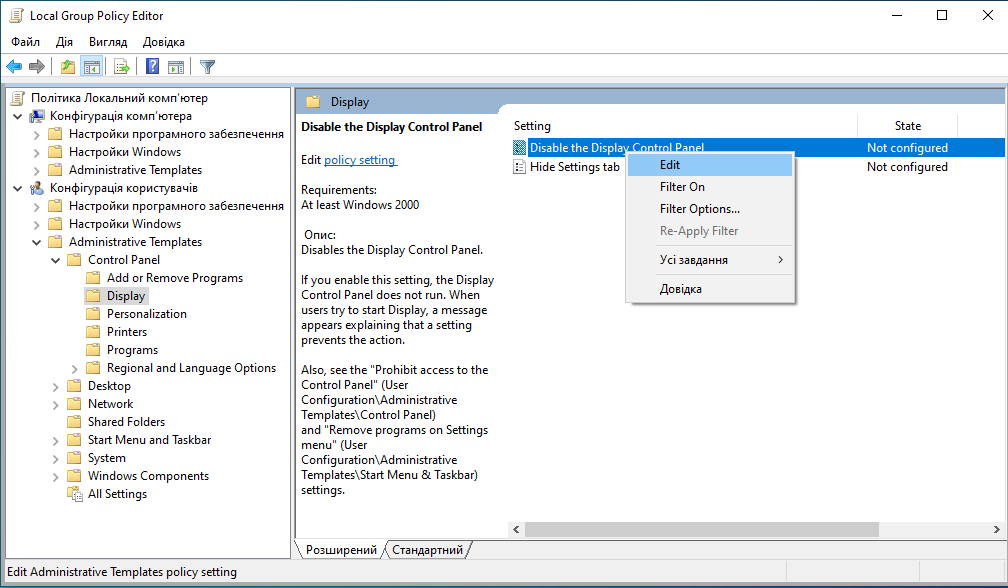


Рис. 14. Налаштування адміністративних шаблонів

Бачимо, що деякі параметри змінити неможливо.

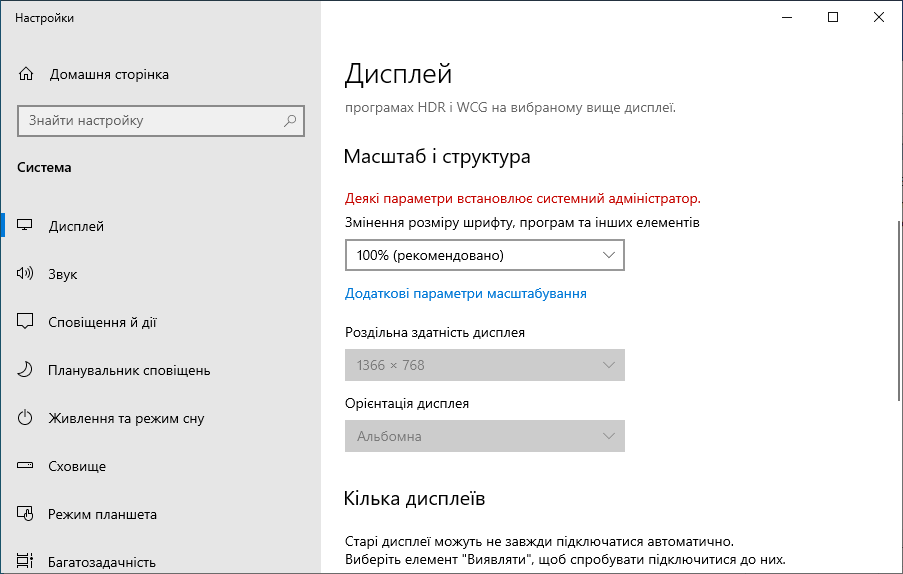


Рис. 15. Повідомлення системи щодо заборони виконання певних налаштувань робочого середовища

1. Перейти в гілку "Software Restriction Policies" (рис. 16). Створити нову політику. Не змінюючи політики за замовчуванням створити нове правило (правила), що забороняє виконання програм з будь-якого тому крім "С:" (при потребі створити логічні диски або розділи) – рис. 18. Спробувати виконати будь-який файл з цього тому (рис. 19). Створити нове правило для хешу програми, яке дозволить виконувати саме цей вказаний файл (рис. 21). Спробувати запустити на виконання цей файл. Для яких потреб можуть використовуватись правила такого типу?

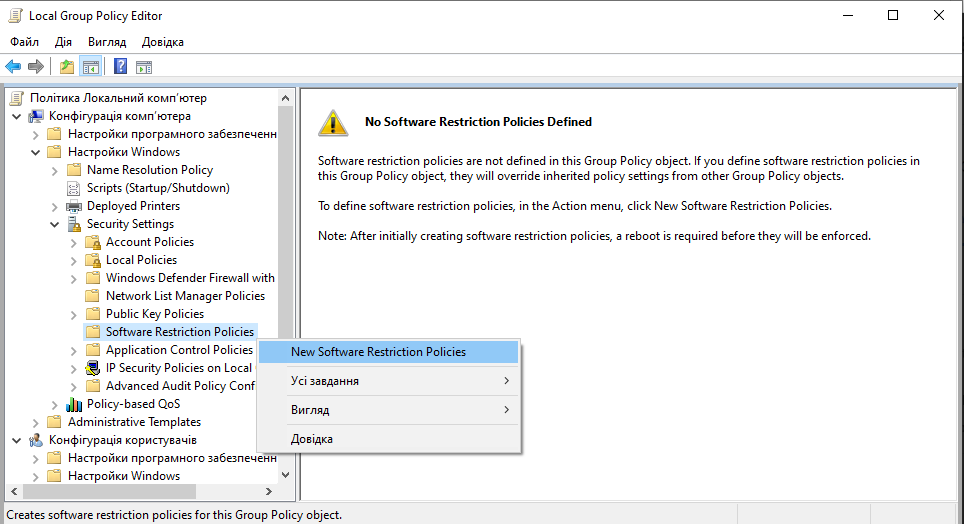


Рис. 16. Software Restriction Policies

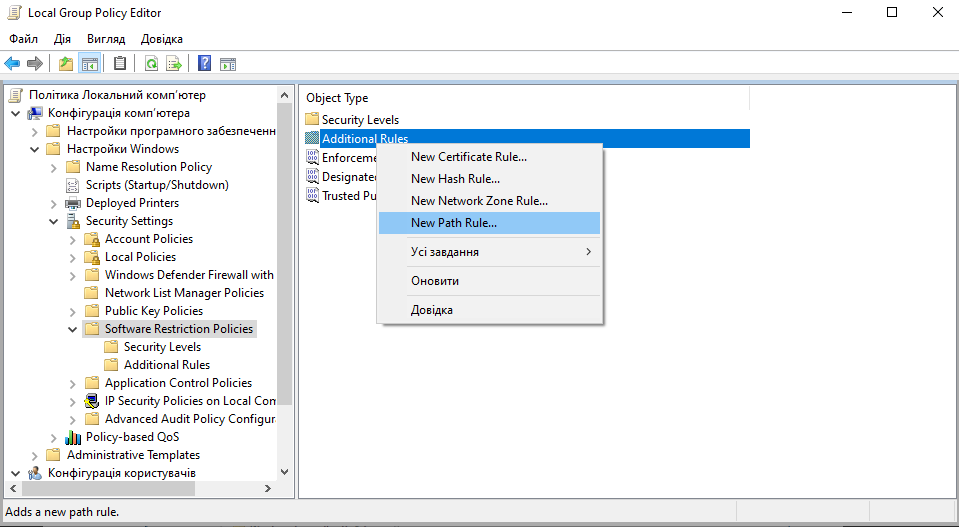


Рис. 17. Створення нового правила

Заборонимо виконання файлів на томі Z, перезавантажимо комп’ютер і спробуємо виконати файл.

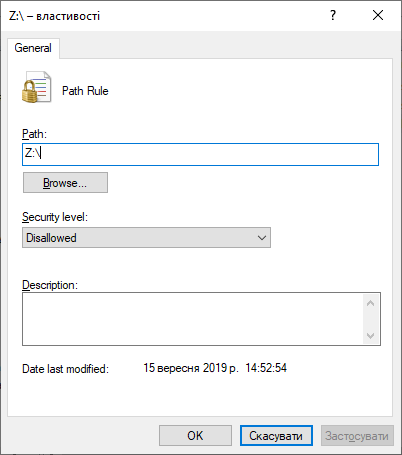


Рис. 18. Властивості правила обмеженого використання програм

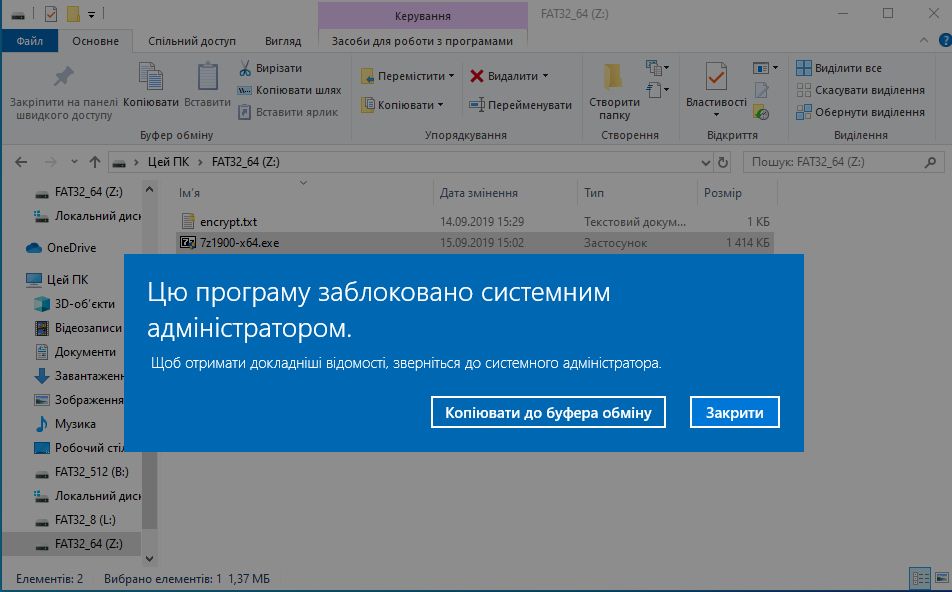


Рис. 19. Повідомлення системи про заборону виконання програми

Створимо правило для хешу програми.

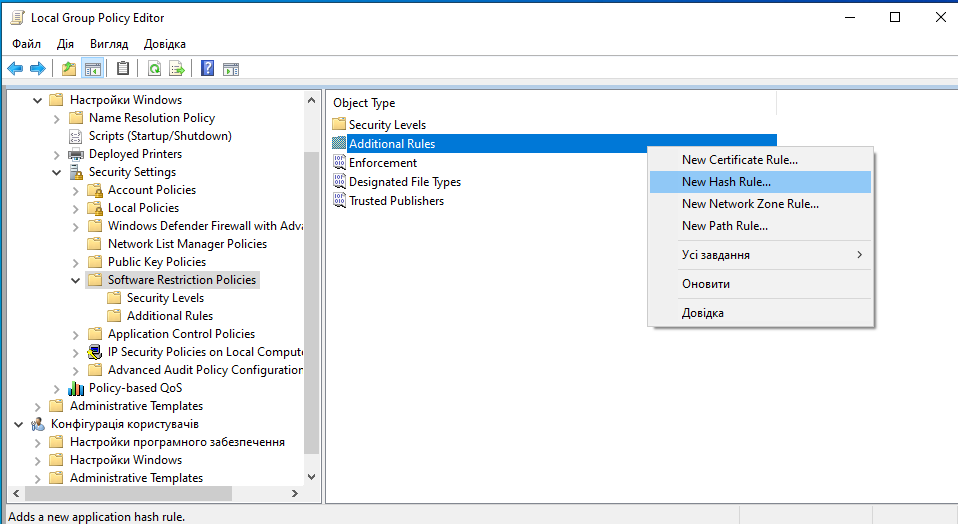


Рис. 20. Software Restriction Policies

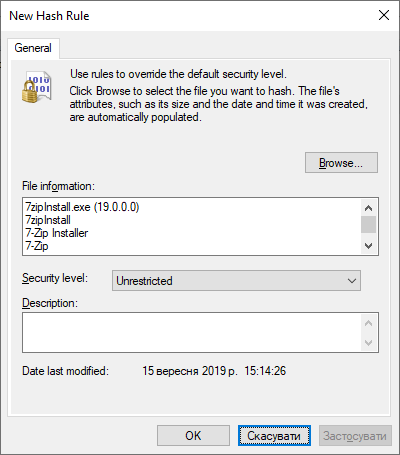


Рис. 21. Створення правила для хешу

Переконаємося, що тепер файл виконується.

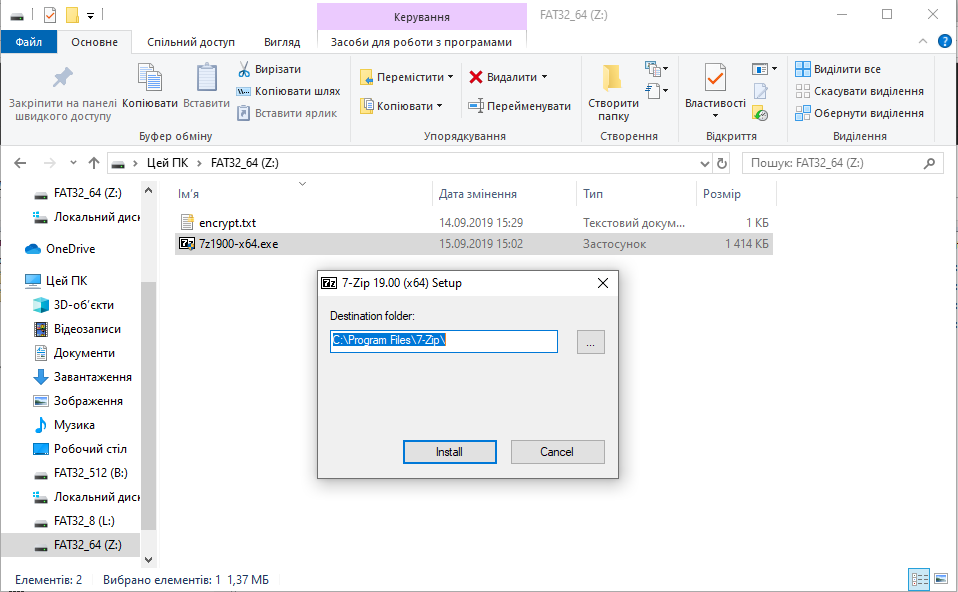


Рис. 22. Виконання файлу

1. Відкрити оснастку mmc "Security Configuration and Analysis" (рис. 23). Створити нову базу даних, яка буде відображати стан налаштування політик комп’ютера за певним шаблоном.



Рис. 23. Оснащення "Security Configuration and Analysis"

Власні шаблони створюються за допомогою оснастки "Security Templates" (рис. 24). Проаналізувати параметри безпеки комп’ютера (рис. 25). Результати аналізу відображаються як порівняння параметрів комп’ютера з параметрами шаблону (створеної бази даних) – рис. 26. Базу даних можна редагувати в цьому ж вікні, а потім вибрати пункт контекстного меню "Save" та, при потребі, експортувати відредагований шаблон безпеки.

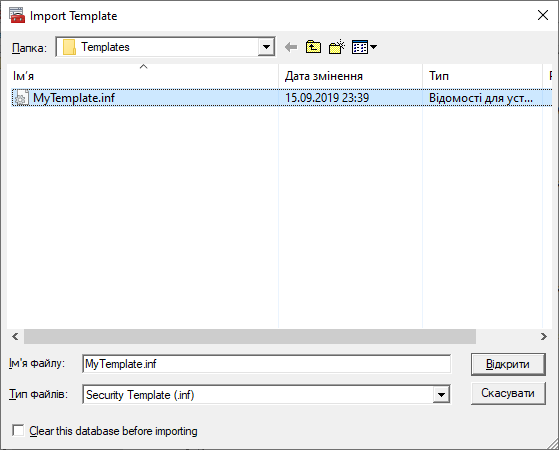


Рис. 24. Створення власних шаблонів.

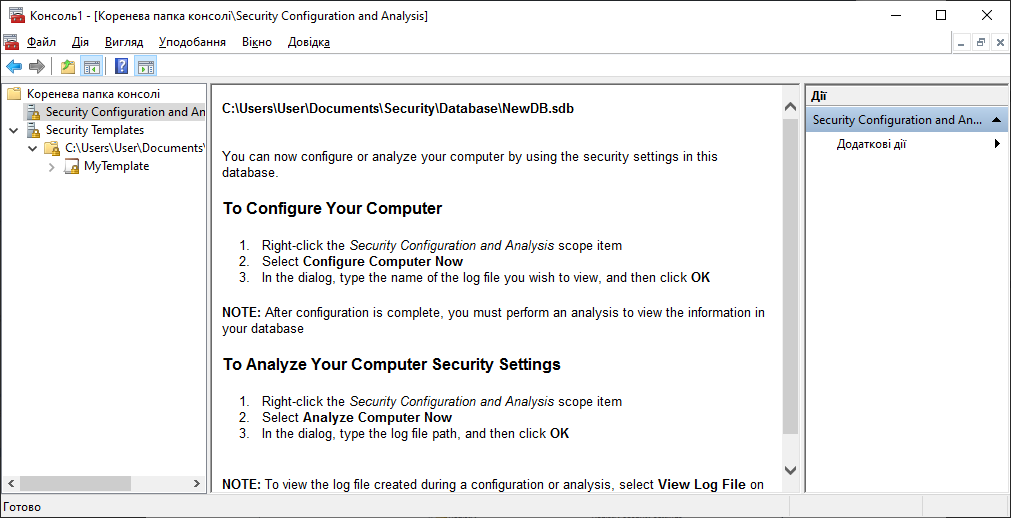


Рис. 25. Використання оснащення "Security Configuration and Analysis"

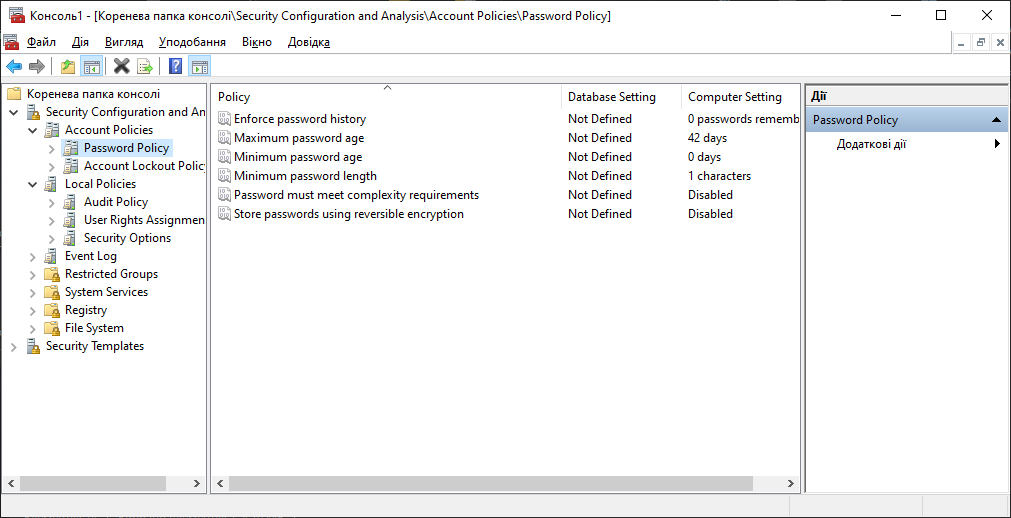


Рис. 26. Результат аналізу безпеки системи

Налаштувати комп’ютер за певним, власним, шаблоном безпеки (привести у відповідність параметри бази даних і поточні налаштування комп’ютера), виконавши необхідні дії.

У звіті до лабораторної роботи описати та пояснити отримані результати.

**КОНТРОЛЬНІ ЗАПИТАННЯ**

1. Призначення групових політик.

2. Чим відрізняються гілки політики "Computer Configuration" та "User Configuration"?

3. Хто має привілей брати об’єкти у власність?

4. Порядок застосування групових політик в Active Directory.

5. Для чого використовуються шаблони безпеки?

6. Чи можна (і як) за допомогою політик бути впевненим у відсутності модифікацій програмного забезпечення після його встановлення на комп’ютер?

1. Нагадаємо, що дозволи підтримуються тільки на файловій системі NTFS, тому не дивуйтеся, якщо ви не побачите вкладку Security (Безпека) у властивостях дискових томів, що відформатовані для FAT або FAT32. [↑](#footnote-ref-1)
2. У Windows 10 і Windows Server 2008 для виконання будь-яких операцій з квотами можна також використовувати утиліту командного рядка Fsutil.exe. [↑](#footnote-ref-2)
3. З вищесказаного випливає принцип відновлення дозволів для будь-якого об'єкту (зокрема для об'єктів, у яких помилково видалені всі дозволи): потрібно стати його власником, а потім встановити потрібні дозволи для інших користувачів і груп. [↑](#footnote-ref-3)
4. Політики відновлення в Windows 10/2008 працюють інакше, ніж в Windows 2000. За умовчанням на комп'ютерах під управлінням Windows Server 2008 агенти відновлення не створюються і політика відновлення не перешкоджає роботі EFS. Це означає, що відновити зашифровану інформацію можуть тільки ті користувачі, які її зашифрували. [↑](#footnote-ref-4)
5. GPO, який застосовується локально, зберігається в локальній папці комп’ютера %systemroot%\system32\GroupPolicy. Комп’ютер може мати тільки одну локальну групову політику. [↑](#footnote-ref-5)
6. Адміністративний шаблон є текстовим файлом у форматі Unicode, який містить перелік ключів і параметрів реєстру. Такі файли мають розширення .adm і зберігаються в папці %SystemRoot%\inf. [↑](#footnote-ref-6)
7. Ці шаблони призначені для комп'ютерів, на яких використовуються параметри безпеки за умовчанням. Іншими словами, будучи встановленими на комп'ютері, ці шаблони значно змінюють стандартні параметри безпеки. Але вони ***не*** встановлюють стандартні параметри безпеки, перш ніж змінити їх. [↑](#footnote-ref-7)
8. Забезпечення безпеки неможливе в системах Windows XP Professional, встановлених на дисках з файловою системою FAT. [↑](#footnote-ref-8)
9. Імпорт шаблонів в особисту базу даних впливає тільки на базу даних аналізу і не змінює параметри системи. [↑](#footnote-ref-9)