Лабораторна робота №3

Відновлення даних на жорсткому диску

Ціль роботи: ознайомлення з методами відновлення даних на жорсткому диску.

1. Короткі теоретичні відомості

Пошкодження даних може виникнути як через помилки при обробці таблиці файлів. Це може трапитися, наприклад, після некоректного відключення пристрою, збоїв в роботі програмного і апаратного забезпечення або в результаті зараження вірусами. Також однією з поширених причин виникнення такого роду помилок є частковий вихід з ладу поверхні диска – поява «*bad*-секторів». На жаль, зараз це явище не рідкість навіть для нових жорстких дисків, що експлуатуються протягом декількох тижнів або навіть днів.

Якщо запис в сектори, що містять файли не проводилася, то дані фізично залишилися на своїх місцях, але загубилися або спотворилися відомості про їх розташування. Таким чином, потрібно визначити, де саме знаходяться сектора, містять потрібну інформацію, і зчитати їх у правильній послідовності.

У разі, коли проводився запис на диск, наприклад, підчас форматування диску з подальшою установкою операційної системи, ймовірність фізичного знищення потрібної інформації може бути досить велика. У подібних ситуаціях можливість успішного відновлення даних залежить від везіння і співвідношення обсягів втраченої і записаної інформації. Скажімо, якщо Ви випадково видалили 1Гб бухгалтерських баз і після цього записали на цей же логічний розділ 70Гб цікавих фільмів, ймовірність відновлення хоч чогось близька до нуля.

Також варто взяти до відома, що при втраті даних через помилки в файлової системі, запуск програм типу *ScanDisk* істотно зменшує ймовірність успішного відновлення. Основне завдання цих утиліт – приведення в порядок службових структур файлової системи, що вони і

роблять, не особливо піклуючись про долю користувача даних. При цьому знищуються дані, за якими можна було б реконструювати структуру файлової системи до пошкодження і врятувати дані.

У загальному випадку, програма для відновлення даних спочатку сканує всі носії. За результатами сканування, на основі виявлених службових записів, складається карта розташування фрагментів відновлюваних файлів і будується дерево каталогів. У карті містяться відомості про те, який кластер до якогось файлу відноситься, розміри, назви та інші атрибути елементів файлової системи, що сканується, тобто все, що вдалося дізнатися на підставі залишків службової інформації. Якщо отриманих в результаті сканування відомостей не достатньо, то використовуються певні методи екстраполяції. Потім файли і папки, які потрібно відновити, вибираються відповідно до складеної карти і переносяться на інший носій.

Найчастіше все, що в принципі можливо відновити за справного носія інформації, дістається за допомогою програм, згаданих нижче. І лише в меншій частині випадків, висококваліфікований фахівець, працюючи на більш низькому рівні, здатний відновити інформацію в більшому обсязі.

Перед тим, як приступити до самостійного відновлення даних, слід взяти до уваги можливість фізичної несправності пристрою. Особливо це ймовірно у випадках, коли дані пропали без видимих причин, або при спробі відкриття файлів видається повідомлення про помилку. І хоча нижчезгаданих програми самі по собі не роблять деструктивних дій (вони взагалі нічого не пишуть на розділ, з яким працюють), подальша робота з несправним накопичувачем без спеціального обладнання може привести до посилювання ситуації, аж до повної неможливості відновлення даних.

Значний досвід використання різних програм для відновлення даних показує, що жодна з них не дає кращий результат у всіх випадках втрати інформації. Вони використовують різні алгоритми, які мають свої

переваги і недоліки. Тому, в залежності від характеру пошкодження, на одній і тій же файлової системі кращий результат можуть показати різні утиліти.

Цей факт добре відомий, тому в процесі роботи фахівцями використовуються добірки програм від різних виробників, і в кожній ситуації застосовується утиліта, найкращим чином підходить під конкретний випадок. Або використовується декілька різних програм послідовно.

UFS Explorer - найбільш універсальний з відомих пакетів програм для відновлення даних. *UFS Explorer Standard Recovery* зручний для професіоналів, підтримує відновлення інформації з різних типів накопичувачів і всіх поширених на даниц момент файлових систем. Є версії під *Windows*, *Linux*, *BSD*, *Mac OS*. Редакція *Raise Data Recovery* являє собою набір утиліт для користувачів, яким потрібна разове відновлення даних. Функціонал кожної з них обмежений підтримкою однієї конкретної файлової системою, працюють тільки під *Windows*.

Безкоштовна програма для відновлення даних *R.saver* допоможе врятувати дані з *FAT* або *NTFS*. Вона призначена для користувачів, не знайомих з пристроєм файлових систем і принципами відновлення даних, тому інтерфейс максимально спрощений. Налаштування виконуються автоматично, для запуску сканування достатньо натиснути всього одну кнопку. Це робить програму менш зручною для професіоналів, але значно спрощує її застосування звичайними користувачами.

Якщо алгоритми зазначених вище програм виявилися не оптимальними для конкретного випадку, рекомендується спробувати *R-studio* або *GetDataBack*.

Послідовність дій при відновлені даних:

1) Встановлення або розпакування завантаженої програми. Перш ніж приступити до цих дій, переконайтеся, що плануєте виконувати їх на диску або розділі відмінному від того, де втрачена інформація.

2) Запуск і попереднє сканування, яке виконується автоматично. Утиліти використовують для цього різні алгоритми, через що у них відрізняються час запуску і списки виявлених файлових систем. Деякі програми можуть відразу показати пошкоджені розділи, які не видно засобами операційної системи, а деякі не покажуть навіть пристрій, з якого планується відновити дані. Якщо все, що потрібно, відобразилося, то переходите до третього пункту. Якщо ні, то можливі наступні варіанти:

• Пристрій відображається у списку, але потрібний розділ на ньому не знайдений:

a. Якщо такий функціонал програмою підтримується, то можна скористатися поглибленим варіантом первинного сканування. Наприклад, в *UFS Explorer* для цієї мети є функція «Знайти розділ».

b. Запустити сканування по всьому пристрою відразу. Деякі програми, наприклад *R-studio*, дозволяють це зробити, показуючи в результатах сканування можливі знайдені розділи з приблизною файловими структурами.

c. Скористатися іншою програмою.

• Пристрою немає у списку, але при цьому визначається засобами операційної системи. В *Windows* це можна перевірити, подивившись список пристроїв Пуск->Панель_управления->Администрирование->Управление компьютером-> Управління дисками. Якщо накопичувач був підключений після запуску програми, то перезапустите її або поновіть список пристроїв. Якщо не допомогло – спробуйте іншу програму.

• Пристрій не визначається засобами операційної системи. Перевірте правильність підключення і подачу живлення. Якщо все підключено вірно, а накопичувач все одно в системі не видно, то, найімовірніше, ви зіткнулися з фізичною несправністю.

3) Налаштування параметрів сканування зазвичай виконується після вибору накопичувача або розділу і натиснення кнопки запуску,

безпосередньо перед початком самого процесу. Деякі програми, в тому числі *R.saver*, виконують попереднє налаштування автоматично. Утиліта може запросити:

- Межі сканування. Якщо відомо, в якій саме області пам'яті слід шукати потрібні дані, то налаштування цих параметрів може заощадити час. Якщо не знаєте - залиште значення за замовчуванням.
- Тип файлової системи. Деякі програми пропонують вибрати один тип зі списку, підказуючи при цьому оптимальний вибір, інші можуть запропонувати виключити зі списку файлові системи, яких на накопичувачі точно не може бути.
- Для певних типів файлових систем багатомовна програма може запросити передбачувану кодування. Наприклад, для російськомовної *FAT*32 слід вибирати *cp*866.
- Крім перерахованих вище налаштувань, утиліти часто пропонують вибрати один або кілька алгоритмів, які будуть використовуватися в процесі сканування. Їх можна умовно розділити на три типи, в залежності від призначення і особливостей роботи:

a. Відновлення видалених файлів на справній файловій системі. Повне сканування для більшості типів файлових систем в таких випадках НЕ потрібно. Використовується виключно для відновлення видалених файлів. Деякі програми запускають його автоматично, в процесі попереднього сканування.

b. Реконструкція файлової системи після пошкоджень або форматування. Мета – створення віртуального дерева каталогів, що відображає вміст файлової системи, що була сканована в вихідному стані, без пошкоджень. В випадку успіху звідти можна зберегти потрібні дані на інший розділ.

c. Відновлення даних по сигнатурам, так зване «Чорнове» відновлення або «*Raw recovery*». Сигнатура – це характерна послідовність символів, по якої можна зрозуміти, що знайдений фрагмент даних відноситься до файлу певного типу. Використовується в тих випадках,

коли інші методи НЕ допомогли. Результатом застосування будуть файли без назв, розсортовані по папкам в залежності від типу містяться в них даних.

Кожен тип носія інформації, файлова система і особливості експлуатації, вносять свої критерії у вибір оптимального методу відновлення даних. Наприклад, не дивлячись на те, що відновлення по сигнатурам рекомендується використовувати як крайній захід, в одному з найпоширеніших випадків втрати даних його можна запустити відразу і отримати відмінні результати. Цей випадок – випадкове видалення, форматування або пошкодження структури *FAT* флешки фотоапарата. Імена файлів і структура папок в таких випадках не важливі. Крім того, фотографії звичайно пишуться послідовно на порожню флешку, тому дані кожного файлу зберігаються разом у вигляді одного ланцюжка. Це і створює ідеальні умови для використання «чорнового» відновлення.

4) Сканування може займати від декількох хвилин до декількох годин і більше в залежності від характеристик накопичувача, способу його підключення до комп'ютера і використовуваних алгоритмів. Після завершення процесу утиліта відобразить вміст віртуальних каталогів із знайденими файлами.

5) Вивчення результату сканування, вибір файлів для збереження. У багатьох програмах для оцінки стану знайдених файлів передбачена функція попереднього перегляду. Потрібні файли помічаємо або виділяємо. Якщо в процесі перевірки частину шуканих даних виявити не вдалося, саме час скористатися відновленням по сигнатурам, якщо це ще не було зроблено.

6) Збереження файлів – по суті це і є саме відновлення даних, оскільки в процесі сканування програма просто визначає розташування їх фрагментів. Натискаємо відповідну кнопку на панелі інструментів або вибираємо розділ в випадаючому меню. Потім вибираємо місце для збереження. Переконайтеся, що папка, в яку буде зберігатися результат,

знаходиться на розділі або носіях відмінному від того, який сканувався. Далі тиснемо підтвердження і очікуємо на відновлені дані.

Перед закриттям програми переконайтеся, що коректно відновилося все, що потрібно, або збережіть результат сканування. Інакше, якщо виявиться, що вам потрібно щось ще, доведеться сканувати заново. Це може погіршити результат в тих випадках, коли поверхня жорсткого диска починає виходити з ладу.

7) Помилки читання, «зависання» програм під час сканування жорсткого диска або збереження результату можуть означати наявність секторів, що не читаються. Цілком імовірно, втрата даних і була викликана їх появою. Чим їх більше, тим повільніше буде йти процес. Для перевірки припущення, можна скористатися *HDDScan*.

У подібних випадках рекомендується зняти посекторного копію на справний накопичувач і відновлювати дані з неї. Пам'ятайте, робота *с* подібним диском погіршує його стан. Якщо не впевнені в тому, що робите, і на диску важлива інформація – краще зверніться в спеціалізовану організацію. Там при відновленні даних з пошкоджених дисків використовують програмно-апаратні комплекси, спеціально призначені для таких робіт.

2. Виконання роботи

2.1. Вимоги до обладнання та програмного забезпечення

Лабораторна робота виконується на ПК з використанням программ *VMware player*, *R-Studio*, *Zero Assumption Recovery*.

2.2. **Порядок виконання роботи**

2.2.1. Створення нового жорсткого диску.

2.2.1.1. Зайти у налаштування віртуальної машини (*Player -> Manage -> Virtual Machine Settings*… або *Ctrl+D*, Рис. 1).

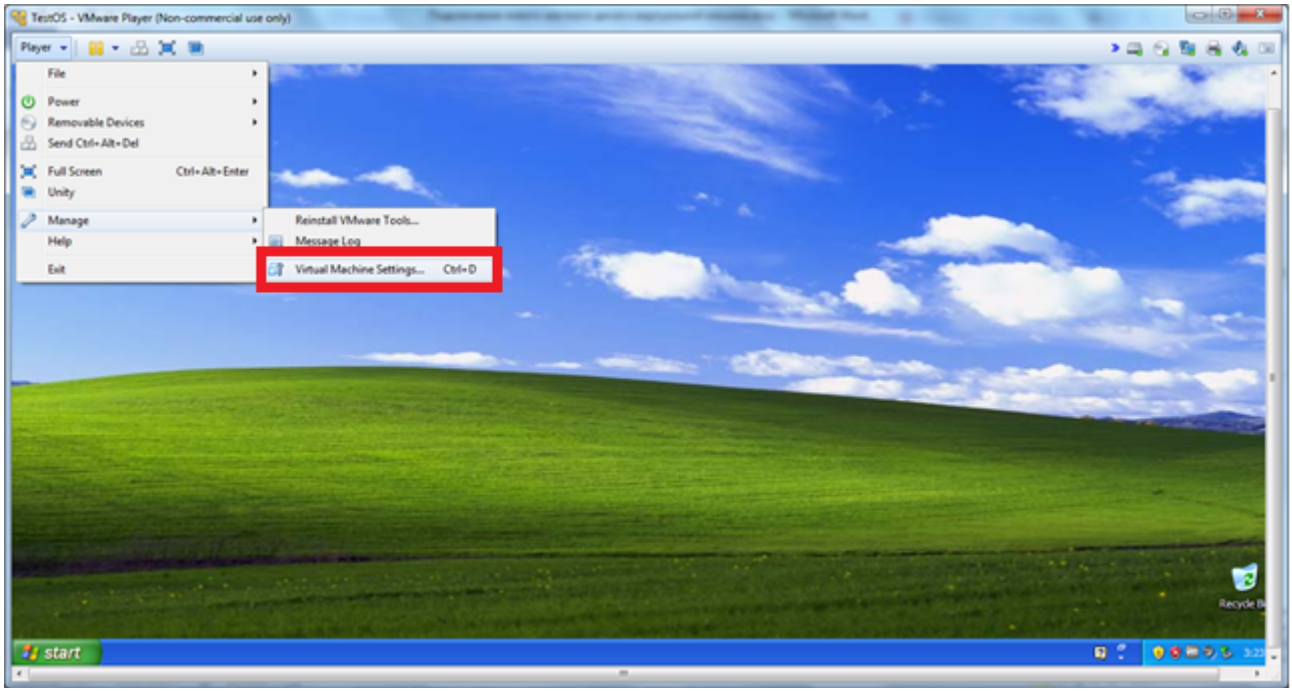

Рис. 1 Доступ до налаштування віртуальної машини

2.2.1.2. Обрати пункт *Hard Disk* (*IDE*) та натиснути кнопку *Add* (Рис. 2):

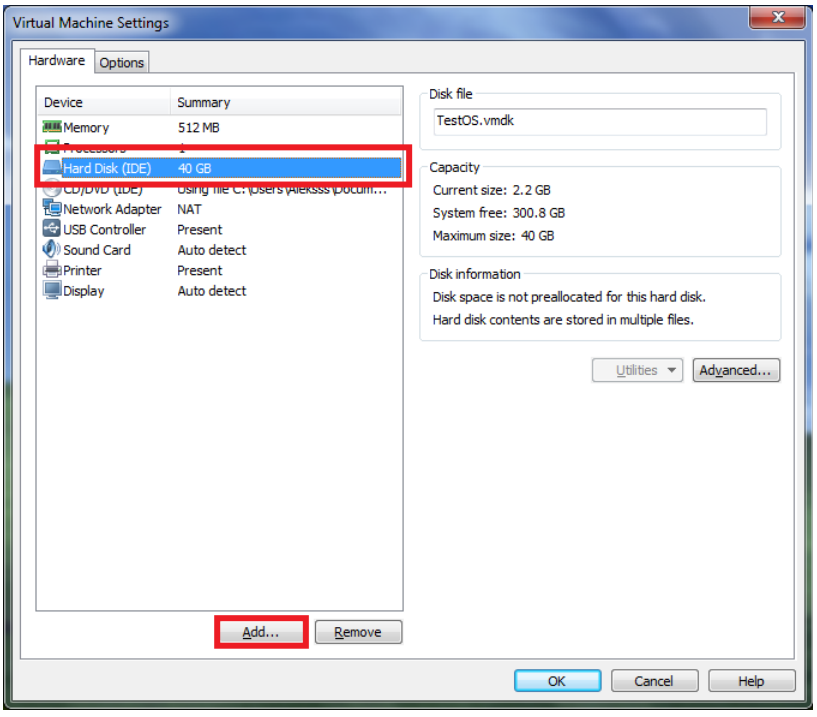

Рис. 2 Додавання нового пристрою до віртуальної машини

2.2.1.3. Обрати пункт *Hard Disk* та натиснути кнопку *Next* (Рис. 3)

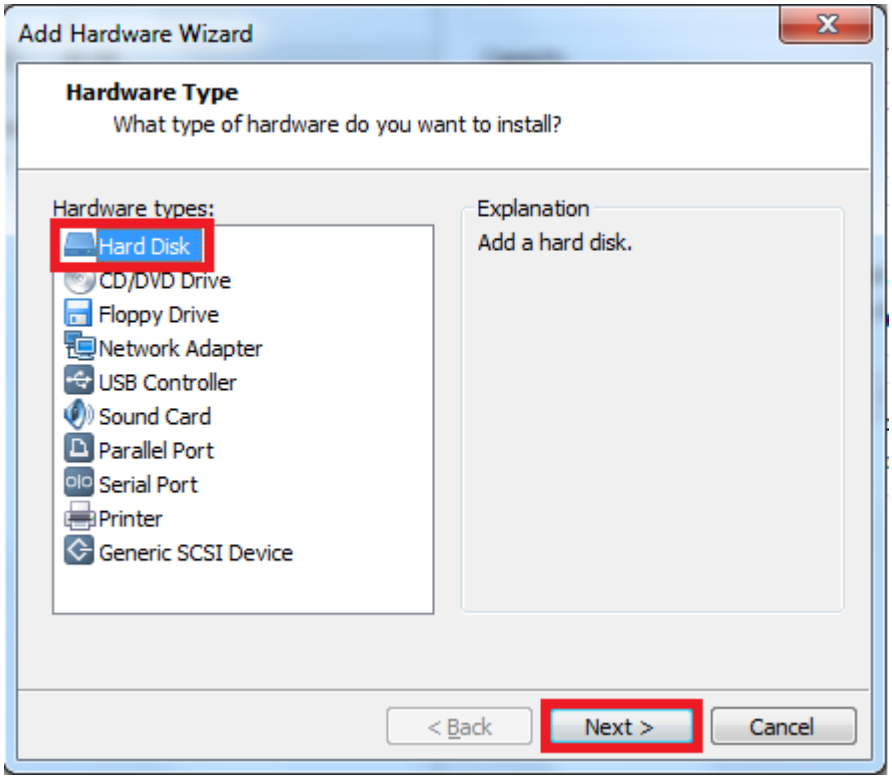

Рис. 3 Вибір типу нового пристрою

2.2.1.4. Обрати тип нового жорсткого диску *IDE* та натиснути кнопку *Next* (Рис. 4):

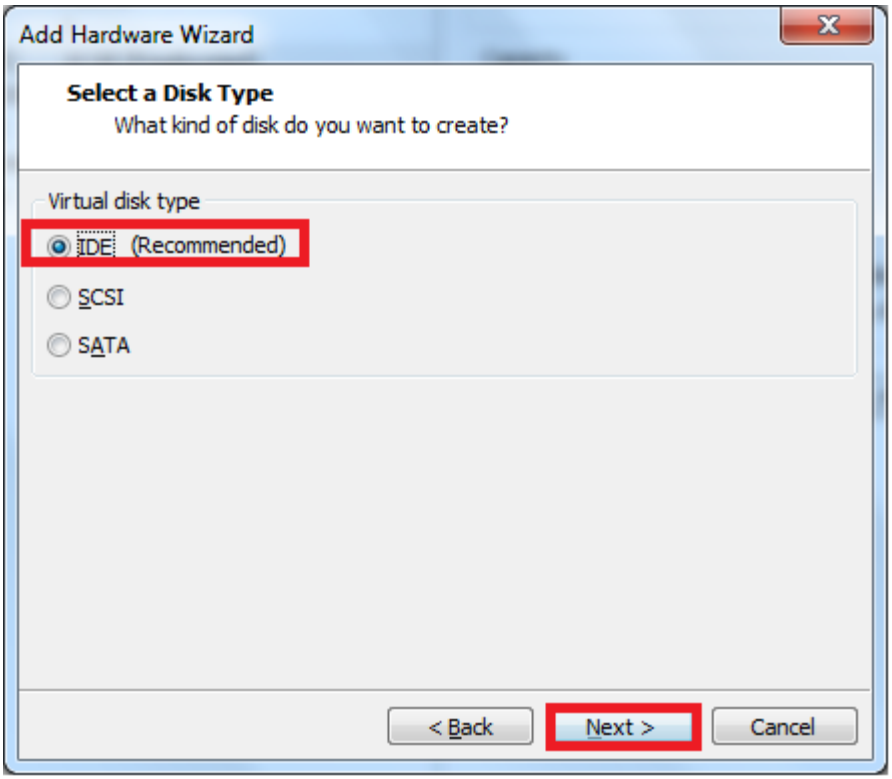

Рис. 4 Вибір типу жорсткого диску

2.2.1.5. Обрати пункт, який дозволить створити новий віртуальний жорсткий диск та натиснути кнопку *Next*(Рис. 5):

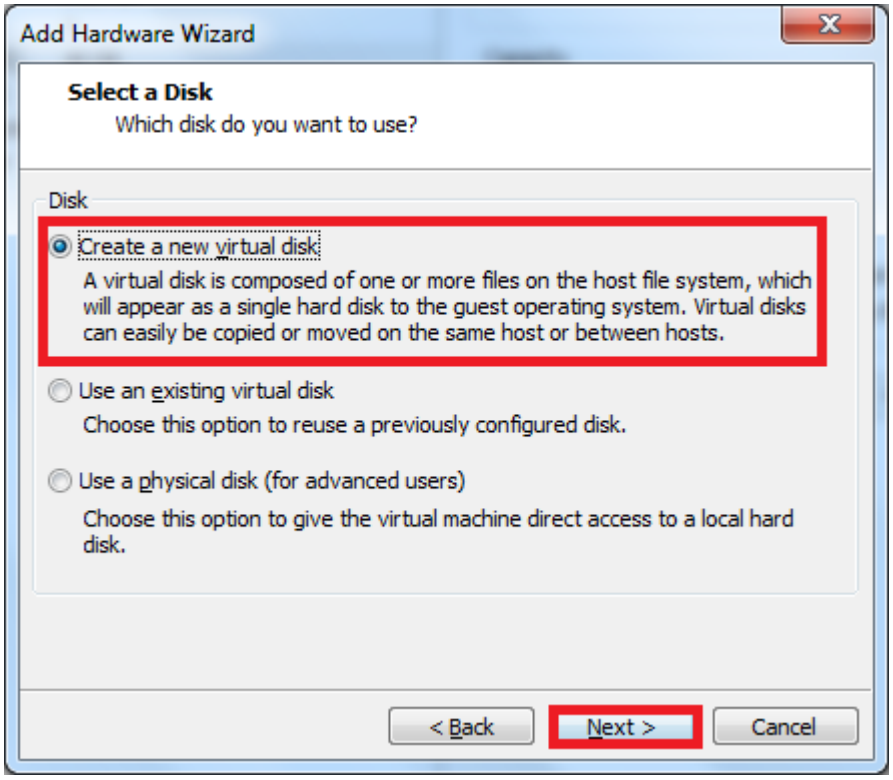

Рис. 5 Визначення джерела нового жорсткого диску

2.2.1.6. Встановити налаштування для жорсткого диску. Потрібно виділити для нього 5 *Gb* вільного простору, виділити пункт, що робить доступним весь дисковий простір одразу, а потім вибрати пункт, що зберігає весь жорсткий диск в одному фалій. Після встановлення налаштуваннь потрібно натиснути кнопку *Next* (рис. 6).

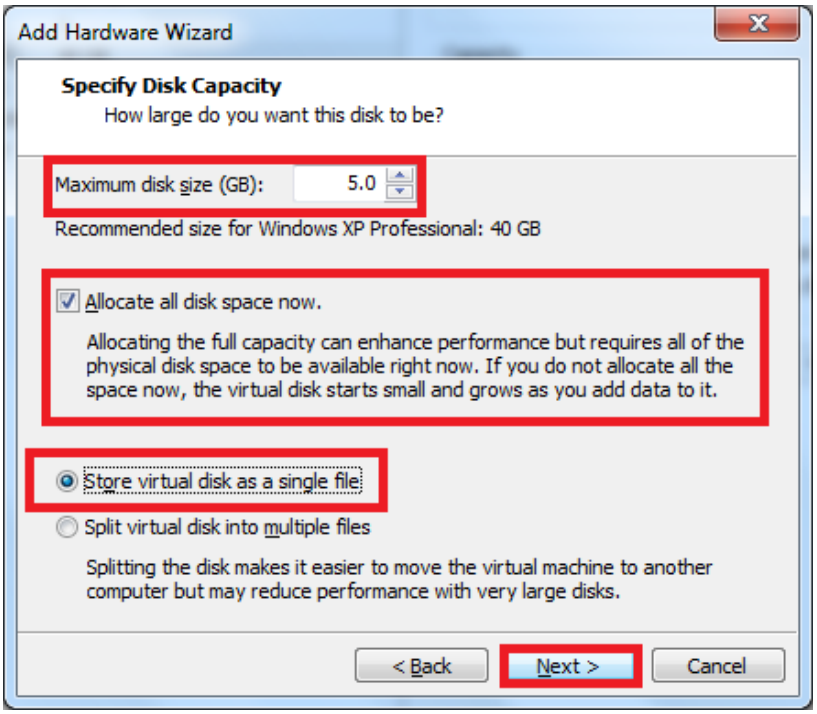

Рис. 6 Налаштування нового жорсткого диску

2.2.1.7. Потрібно дати назву файлу нового жорсткого диску та вказати місце розташування, а потім натиснути кнопку *Finish* (рис. 7):

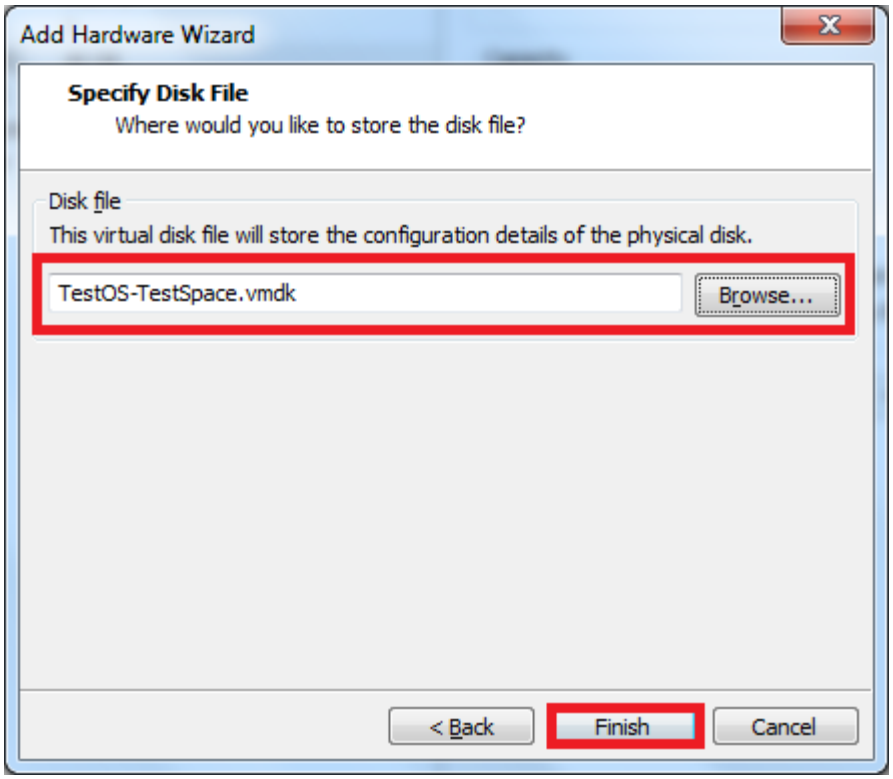

Рис. 7 Визначення ім'я файлу та місця його розташування

2.2.1.8. Далі необхідно встановити новий диск в операційну систему. Потрібно перейти до *Control Panel ->Administrative Tools ->Computer Management -> Storage -> Disk Management*. Там потрібно встановити новий розділ та відформатувати його.

2.2.1.9. На новому розділі потрібно створити файли різного типу та вмісту. Кількість файлів повинна бути в діапазоні від 150 до 200. Знімки екрану з переліком файлів повинні бути в звіті.

2.2.1.10. **Скопіювати (!!!)** програми з образу диску, який є в комплекті з лабораторною роботою, а потім встановити програми та використати їх для відновлення даних. Для кожної програми потрібно виконувати пункт 2.2.1.9 спочатку.

3. Вимоги до вмісту і оформлення звіту

Звіт з лабораторної роботи повинен містити:

— титульний лист;

— короткі теоретичні відомості;

— опис ходу роботи;

— отримані в ході виконання роботи знімки вікон програм;

— результати виконання домашнього завдання;

— висновки.

4. Вимоги до оформлення звіту:

— сторінки А4, відступ зліва – 20, зправа – 10, зверху – 15, знизу – 15;

— шрифт *Times New Roman* 14, відступ першого рядку – 1,25, інтервал – полуторний, вирівнювання – по ширині, вирівнювання малюнків – по центру;

— сторінки нумеровані.

5. Контрольні питання

5.1. Які причини пошкодження даних на жорсткому диску?

5.2. Від чого залежить шанс відновлення даних на жорсткому диску?

5.3. Які програми для відновлення даних ви знаєте?

5.4. Які кроки потрібно виконати для відновлення даних?

5.5. Опишіть програми, які ви використовували при виконанні лабораторної роботи. Перелічіть їх особливості.