

## Урок 12

**Тема: Захист даних. Безпечне зберігання даних. Резервне копіювання та відновлення даних.**

### Мета:

- ✓ **навчальна:** навчити безпечно користуватись мережею, створювати резервні копії файлів та правильно чистити кластери на носіях пам'яті;
- ✓ **розвивальна:** розвивати логічне мислення; формувати вміння діяти за інструкцією, планувати свою діяльність, аналізувати і робити висновки;
- ✓ **виховна:** виховувати інформаційну культуру учнів, уважність, акуратність, дисциплінованість.

**Тип уроку:** засвоєння нових знань;

### Хід уроку

#### I. Організаційний етап

- привітання
- перевірка присутніх
- перевірка готовності учнів до уроку

#### II. Актуалізація опорних знань

Дайте відповіді на запитання:

- Назвіть види ризиків, з якими стикається користувач в Інтернеті.
- Чому ризики в Інтернеті особливо небезпечні для дітей підліткового віку? Поясніть свою думку.
- Як зменшити ризики під час користування сервісами Інтернету?

#### III. Оголошення теми та мети уроку . Мотивація навчальної діяльності

На сьогоднішньому уроці ви дізнаєтесь:

- чому потрібно робити резервне копіювання даних
- як безпечно видаляти дані
- які правила необхідно знати при роботі в Інтернеті

#### IV. Вивчення нового матеріалу

**Як виконувати резервне копіювання та відновлення даних?**

На жаль, неможливо абсолютно надійно зберігати дані в комп'ютері. Відмова апаратної частини (жорсткий диск), вірусна атака чи неакуратність самого користувача (випадкове видалення даних) можуть призвести до втрати важливих даних. Щоб запобігти цьому, необхідно періодично робити резервне копіювання даних.

**Резервна копія** — копія окремих файлів, групи файлів або всього диска, що збережена на іншому носії, для наступного відновлення в разі руйнувань, псування або втрати даних на основному носії.

Розрізняють такі типи резервних копій:

- **резервна копія операційної системи.** Дуже корисна річ, якою часто нехтують навіть досвідчені користувачі. Потрібно встановити операційну систему, драйвери та необхідні програми. Потім зробити резервну копію налагодженої операційної системи й за потреби (вірусна атака або просто захаращення системи) відновити резервну копію. Це займає набагато менше часу, ніж нова установка й налаштування операційної системи. Здебільшого для резервного копіювання операційної системи використовують спеціальні програми або засоби;
- **резервна копія логічного диска (розділу);**
- **резервна копія окремих файлів і папок — найпоширеніший спосіб резервного копіювання.**

Резервне копіювання та відновлення даних є різновидом операцій збереження даних зі своїми особливостями.

- При збереженні даних ми найчастіше маємо справу з одним або декількома файлами. При резервному копіюванні зазвичай об'єктом копіювання є набір великої кількості файлів, папки або диски.
- Резервне копіювання завжди проводять на інші носії — на DVD-диск, флеш-накопичувач, мережеві ресурси, відмінні від тих, з яких копіюють. Не можна розмішувати резервну копію файлів на тому самому диску або диску, де встановлена операційна система.
- При резервному копіюванні збереження даних для користувача комп'ютера є більш важливим, ніж у випадку окремого файла чи файлів. Тому для таких випадків використовують спеціальні засоби — програми для резервного копіювання даних.

Під час резервного копіювання файлів ОС *Windows* створює на відповідному носії папку з іменем *Set [data] [час]*. У разі першого створення резервної копії *Windows* виконує повне резервне копіювання всіх файлів визначеного типу. Після цього здійснюється оновлення резервної копії файлами, що створені чи змінені з моменту запису останньої резервної копії. Можна

періодично створювати нову повну резервну копію, щоб починати роботу «з чистого аркуша».

Резервне копіювання та відновлення файлів і дисків виконується за допомогою вказівки *Пуск/Усі програми/Обслуговування/Резервне копіювання та відновлення*. У вікні, що відкриється слід налаштувати параметри резервного копіювання — вибрати потрібні файли або папки та вказати місце для відновлення даних.

Доцільно дотримуватися таких рекомендацій щодо резервного копіювання даних.

- **Робити періодично резервні копії.** Залежно від типу даних — кожного дня, тижня, місяця тощо або хоча б після істотного оновлення даних. Інакше в разі втрати даних можна відновити лише застарілу версію резервної копії, у якій не вистачатиме нещодавно змінених даних.
- **Тиражувати копії.** Зробивши резервну копію важливих даних, розмножити цю копію на фізично різних носіях: флеш-накопичувачах, зовнішньому жорсткому диску, CD/DVD-диску, хмарному сховищі тощо. Що більше є копій, то більша ймовірність не втратити потрібні дані.
- **Захистити резервну копію** від сторонніх. Краще поєднати кілька способів захисту. Наприклад, захист даних паролем і шифрування.
- **Зберігати резервні копії в різних місцях**, навіть якщо їх зроблено на різних носіях. Інакше в разі крадіжки, пожежі чи стихійного лиха всі копії можна втратити.

### **Як безпечно видаляти дані?**

Файли, які видаляються в *Кошик*, можуть за необхідності бути відновлені. Навіть після очищення *Кошика* видалені файли все одно залишаються на диску, поки на їхнє місце не буде записано інші файли. При видаленні особистих і конфіденційних даних слід передбачити захист від небажаного відновлення видалених файлів іншими особами.

Для безпечного видалення даних без можливості відновлення використовують спеціальні програми. Наприклад, програми *Eraser* та *File Shredder* призначені для безповоротного видалення даних із дисків шляхом неодноразового перезапису.

Популярною програмою для безпечного видалення й очистки комп'ютера від невживаних і тимчасових файлів є *CCleaner* ([www.piriform.com/ccleaner](http://www.piriform.com/ccleaner)). Програма має базову безкоштовну версію та платні версії з додатковими можливостями.

За допомогою *CCleaner* можна швидко й безпечно видаляти:

- тимчасові файли, історію відвідувань браузерів;
- вміст *Кошика*, буфера обміну, тимчасових файлів, файлів журналів, переліку нещодавно відкритих документів в операційній системі *Windows*;
- тимчасові та інші непотрібні файли багатьох програм. Видалення непотрібних файлів за допомогою *CCleaner* звільняє місце на жорстких дисках і забезпечує швидшу роботу операційної системи. Після вибору типів даних, що підлягають очищенню, слід натиснути кнопку *Аналіз*. У вікні буде відображено деталі про файли, які будуть видалені, зокрема вказано їхній обсяг. Для їх видалення натискають кнопку *Запустити очищення*.

Безпечне видалення файлів з диска шляхом неодноразового перезапису забезпечують додаткові засоби, зокрема *Обтирач диска*.

### **Яких правил доцільно дотримуватися для безпечної роботи в інтернеті?**

Жодні найнадійніші засоби не зможуть гарантувати стовідсотковий захист від комп'ютерних вірусів і троянських програм, але, дотримуючись певних правил, ви істотно знизите імовірність вірусної атаки і ступінь

можливих збитків. Одним з основних методів боротьби з вірусами є, як і в медицині, своєчасна профілактика. Комп'ютерна профілактика передбачає невелику кількість правил, дотримання яких значно знижує імовірність зараження вірусом і втрати даних.

З метою профілактики зараження комп'ютерними вірусами користувачеві слід дотримуватися певних рекомендацій.

А саме:

- необхідно використовувати надійні джерела програмного забезпечення для свого комп'ютера, купувати його лише в офіційних продавців;
- перевіряти за допомогою антивірусних програм файли,
- які надходять ззовні (з дисків, Інтернету) до вашого комп'ютера; обмежити доступ сторонніх осіб до комп'ютера; регулярно створювати резервні копії важливих даних; періодично перевіряти комп'ютер на наявність вірусів з використанням нових версій антивірусних програм;
- не відкривати вкладення електронної пошти, які були надіслані від невідомих вам адресатів;
- не завантажувати з Інтернету файли з розширенням *exe* з неперевічених сайтів.

Часто шкідливі програми можуть потрапляти на комп'ютер через спам. Найнадійніший спосіб боротьби зі спамом — не дати можливості спамерам дізнатися вашу електронну адресу. Для цього доцільно дотримуватися таких правил.

- Не варто без необхідності публікувати адресу електронної пошти на веб-сайтах чи в групах новин.
- Не потрібно реєструватися на підозрілих сайтах. Якщо деякий корисний сайт вимагає реєстрації, можна вказати спеціально для цього створену адресу.
- Ніколи не відповідати на спам і не переходити за посиланнями, які містяться в ньому. Цим ви тільки підтвердите, що користуєтеся своєю електронною адресою й будете одержувати ще більше спаму.
- Вибираючи ім'я для своєї електронної пошти, варто, за можливості, щоб воно було довгим й незручним для вгадування.

## **V. Інструктаж з ТБ**

## **VI. Засвоєння нових знань, формування вмінь**

Практичне завдання .

1. Виконати резервне копіювання даних локального диску C та зберегти на локальний носій диску D
2. Результат виконання продемонструйте вчителю

## **VII. Підсумки уроку**

### ***Рефлексія***

- ***Що ми навчились на уроці***
- ***Що виявилось занадто важким***

## **VIII. Домашнє завдання**

Підручник п. 10.4-10.6 ст. 84- 87

## **IX. Оцінювання роботи учнів**