Інформатика, 9 клас _____ (дата)

Урок №8

Тема: Загрози безпеці та пошкодження даних у комп'ютерних системах

Мета :

- **навчальна:** сформувати поняття про загрози безпеці та пошкодження даних у комп'ютерних системах;
- **розвиваюча:** розвивати логічне мислення, планувати свою діяльність, аналізувати і робити висновки, вміння висловлювати свою точку зору;
- **виховна:** виховувати інформаційну культуру учнів, уважність, дисциплінованість

Обладнання: роздатковий матеріал, підручники, бланки оцінювання.

Тип уроку: засвоєння нових знань.

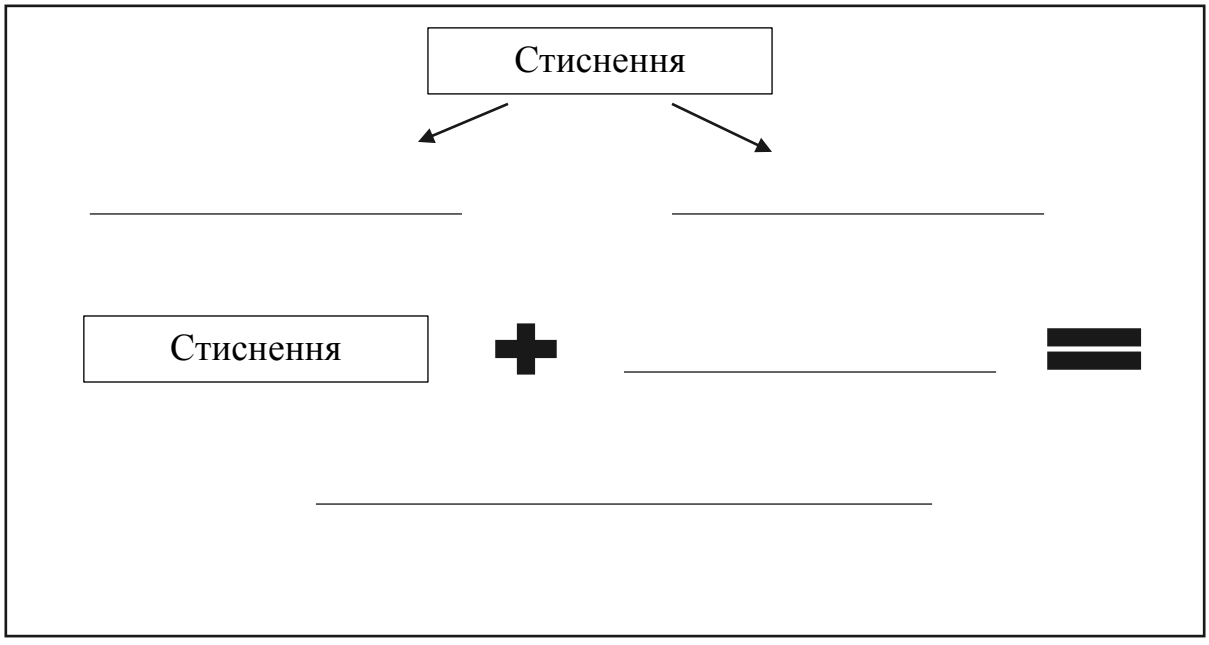
Хід уроку

І. Організаційний етап

- Привітання.
- Відмічання відсутніх.
- Перевірка готовності до уроку.

ІІ. Перевірка домашнього завдання.

Заповнити пропущені місця:



ІІІ. Актуалізація опорних знань

Фронтальне опитування

- Правила безпечного пошуку матеріалів в Інтернеті.

- Що таке критичне оцінювання матеріалів з Інтернету?

IV. Повідомлення теми і мети уроку

V. Вивчення нового матеріалу

Робота в групах

(Учні об’єднуються в 3 групи та опрацбовують матеріал. Їх завдання скласти асоціативний кущ за матеріалом та донести найголовніше учням з інфших груп.)

1 група: Загрози інформаційної безпеки.

2 група: Етичні та правові основи захисту даних.

3 група: Шкідливі програми та комп’ютерні віруси.

Приклади асоціативних кущів:

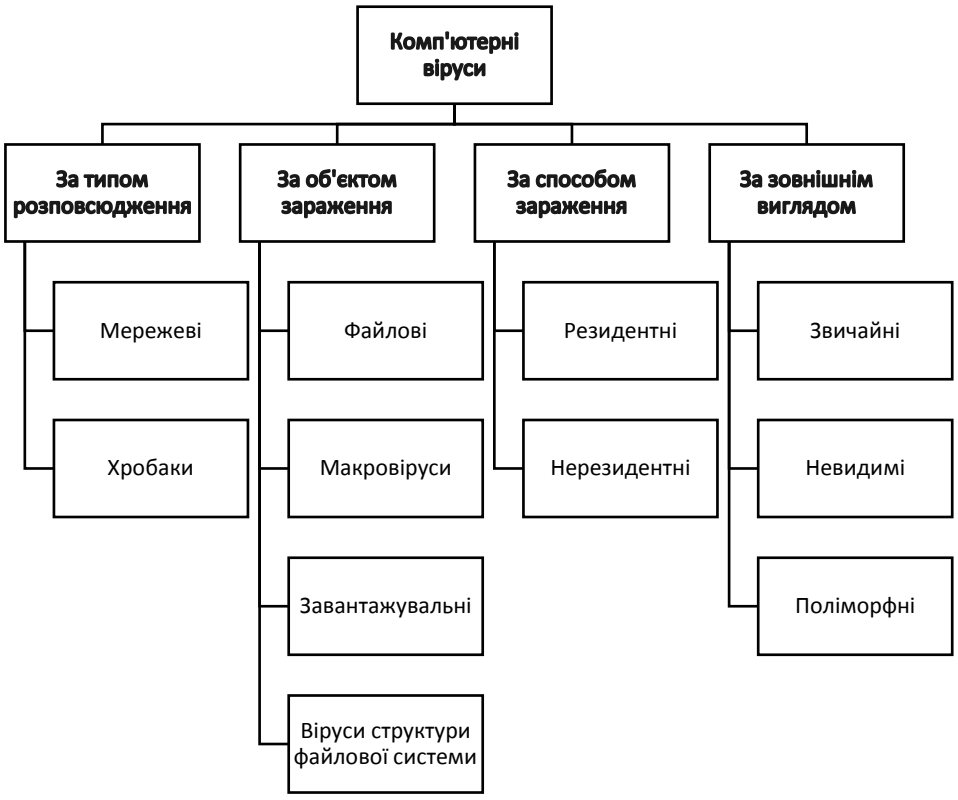
1 група:

2 група:


Базові права
Загальнодоступність
Таємниця приватного життя
Недоторканість приватної власності


Правовий захист інформації
Наявність прав на інформацію
Реалізація прав
Контроль за процедурами реалізації прав

3 група:


Комп'ютерні віруси
За типом розповсюдження
За об'єктом зараження
За способом зараження
За зовнішнім виглядом
Мережеві
Хробаки
Файлові
Макровіруси
Завантажувальні
Віруси структури файлової системи
Резидентні
Нерезидентні
Звичайні
Невидимі
Поліморфні

VI. Формування умінь і навичок

Завдання 1. Класифікація джерел загроз

Ознайомтеся з іншою класифікацією джерел загроз інформаційній безпеці (мал. 9.3) та поставте у відповідність загрози, вказані на малюнку 9.2, категоріям запропонованої класифікації.

Завдання на с. 74 підручника

Завдання 2. Працюємо в парах

Чи може Інтернет бути небезпечним для користувача, а не лише для його комп'ютера? Обговоріть у парах. Наведіть приклади, коли користування Інтернетом є небезпечним для дітей, молоді, дорослих.

Завдання на с. 79 підручника

VII. Підбиття підсумків

Фронтальне опитування

1. Які є джерела загроз комп'ютерної небезпеки?
2. Які шляхи поширення загроз комп'ютерної небезпеки?
3. У яких випадках програму називають комп'ютерним вірусом?
4. Як може проявлятись зараження комп'ютера вірусом?

Оцінювання

Бланк оцінювання:

№	*Тип роботи*	*Бали*
1	Домашнє завдання	**0-2**
2	Фронтальне опитування	**0-2**
3	Робота в групах	
	Читав	**1**
	Розрповідав, підглядаючи	**2**
	Розповідав сам	**3**
4	Робота над асоціативним кущем	**0-2**
5	Нотування асоціативних кущів	**0-2**
6	Робота на уроці	**0-1**

Рефлексія

- Що нового сьогодні дізналися?
- Чого навчилися?
- Що сподобалось на уроці, а що ні?
- Чи виникали труднощі?

VIII. Домашнє завдання

Опрацювати **п.9.1-9.5**

Роздатковий матеріал

1 група
Загрози інформаційної безпеки

Інформаційна загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

Під *інформаційною безпекою* розуміють захищеність даних та інфраструктури, що її підтримує, від будь-яких випадкових або зловмисницьких дій, результатом яких може стати нанесення шкоди безпосередньо даним, їхнім власникам або інфраструктурі, що підтримує інформаційну безпеку.

Стандартною моделлю безпеки даних може слугувати модель із трьох категорій:

Конфіденційність – стан даних, за якого доступ до них здійснюють тільки ті особи, що мають на нього право.

Цілісність – уникнення несанкціонованої зміни даних та існування даних у неспотвореному вигляді.

Доступність – уникнення тимчасового або постійного приховування даних від користувачів, котрі мають права доступу.

Відповідно до розглянутої моделі безпеки даних є три різновиди загроз:

Загроза порушення конфіденційності полягає у тому, що дані стають відомими тому, хто не має права доступу до них.

Загроза порушення цілісності передбачає будь-яку умисну зміну даних, що зберігаються в комп'ютерній системі чи передаються з однієї системи в іншу.

Загроза відмови служб виникає щоразу, коли в результаті навмисних дій, які виконує інший користувач або зловмисник, блокується доступ до деякого ресурсу комп'ютерної системи.

Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій.

До категорій дій, що здійснюються *авторизованими користувачами*, належить: цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачами в результаті необережних дій.

Хакер – кваліфікований IT-фахівець, який знається на комп'ютерних системах і втручається в роботу комп'ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері.

Окрема категорія електронних методів впливу – комп'ютерні віруси та інші шкідливі програми. Вони становлять реальну небезпеку, широко використовуючи комп'ютерні мережі, Інтернет і електронну пошту.

Спам – небажані рекламні електронні листи, повідомлення на форумах, телефонні дзвінки чи текстові повідомлення, що надходять без згоди користувача.

Фішинг – один з найпопулярніших і прибуткових (для тих, хто його реалізує) видів атак. Зловмисник створює сайт, який у точності копіює дизайн і можливості сайта будь-якого банку, інтернет-магазину або платіжної системи. Мета – збір конфіденційної інформації – паролі, коди тощо.

2 група
Етичні та правові основи захисту даних

Морально-етичні основи захисту даних передбачають норми поведінки, які традиційно склались або складаються з поширенням комп'ютерів та мереж: соціальна й персональна відповідальність, рівноправність партнерів по комунікації, точне й сумлінне виконання обов'язків тощо.

Поряд із загальнолюдськими етичними нормами є такі базові права, як:

- загальнодоступність – гарантує право на комунікацію й передбачає доступність державних інформаційних ресурсів;
- таємниця приватного життя – дотримання конфіденційності довірених даних;
- недоторканість приватної власності – основа майнового порядку, дотримання права власності на дані й норм авторського права.

У прийнятих в Україні законодавчих нормах, зазначено, зокрема, що захисту підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрити інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;
- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України «Про доступ до публічної інформації»;
- службова інформація;
- інформація, яка становить державну або іншу передбачену законом таємницю;
- інформація, вимога щодо захисту якої встановлена законом.

Правовий захист інформації передбачає:

- наявність прав на інформацію – сертифікацію, ліцензування, патентування;
- реалізацію прав – захист інтелектуальної власності, захист авторських прав;
- контроль за процедурами реалізації прав – систему адміністративного, програмного, фізико-технічного захисту інформації.

Власник авторських прав може використовувати знак охорони авторського права, що складається з трьох елементів:

- латинської літери «С» (початкова буква англійського слова copyright – авторське право), взятої в коло ©;
- імені власника виключних авторських прав;
- року першого опублікування твору.

3 група

Шкідливі програми та комп'ютерні віруси

Шкідлива програма – комп'ютерна програма або переносний код, призначений для реалізації загроз даним, що зберігаються в інформаційній системі, або для прихованого нецільового використання ресурсів системи, або іншої дії, що перешкоджає нормальному функціонуванню інформаційної системи.

Комп'ютерні віруси – це спеціальні програми в машинних кодах або фрагменти програм, здатні без відома та згоди користувача розмножуватися й розповсюджуватися на інші програми шляхом копіювання свого коду у файли, що зберігаються в системі.

Як можна класифікувати комп'ютерні віруси?

Мережеві віруси для свого розповсюдження використовують можливості комп'ютерних мереж.

Хробаки – це один з різновидів шкідливих вірусів, що розмножуються та псують дані, збережені на комп'ютері. Часто хробаки розповсюджуються через файли, вкладені в електронні листи, або через деякі веб-сторінки, проте можуть також завантажуватися під час спільного користування файлами або програмами миттєвого обміну повідомленнями.

Файлові – уражають програми (основні й допоміжні, тобто ті, що завантажуються лише під час виконання основних).

Макровіруси – це файлові віруси, які використовують файли документів текстових процесорів та електронних таблиць, зокрема Microsoft Office.

Завантажувальні – уражають завантажувальні сектори дисків.

Віруси структури файлової системи – здатні вносити зміни в службові структури файлової системи таким чином, що вірус включається у файли, призначені для виконання, явно не вкорінюючи в них свій код.

За способом зараження середовища мешкання віруси можна поділити на резидентні та нерезидентні.

Так, завантажувальні віруси найчастіше є резидентними. Це означає, що під час завантаження системи вірус потрапляє в оперативну пам'ять і перебуває там постійно.

Є також класифікація за зовнішнім виглядом:

- звичайні – код вірусу видно на диску;
- невидимі (Stealth-віруси) – використовують особливі методи маскування, при перегляді код вірусу не видно. Мають резидентний модуль, який постійно перебуває в оперативній пам'яті;
- поліморфні – код вірусу змінний.