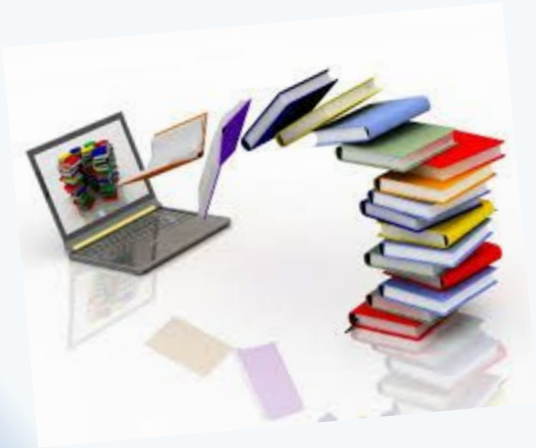
Тема: Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення

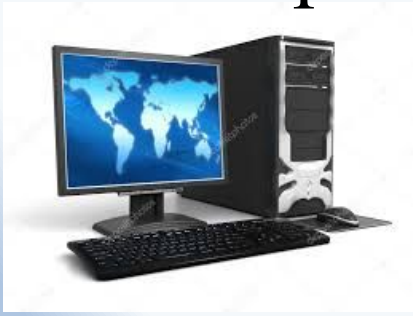
Хочу побажати вам гарного уроку,
Щоб було цікаво всім нам працювати,
Щоб хотіли всі відповідати.
Щоб допомагало вам вміння міркувати
І дванадцять балів легко зароблять.



Актуалізація опорних знань

Запитання

1. Які правила захисту даних у комп’ютерних системах ви знаєте?
2. Які загрози можуть виникнути під час роботи в Інтернеті?
3. Які особисті дані потрібно захищати? Які загрози із цим пов’язані?



Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Конфіденційність - забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення.

Доступність - забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками.

Цілісність - захист даних від їх зловмисного або випадкового знищення чи спотворення.

Залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

- отримання несанкціонованого доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп'ютерної інформаційної системи;
- отримання несанкціонованого доступу до керування роботою комп'ютерної інформаційної системи;
- знищення та спотворення даних.

Загрози інформаційній безпеці, що виникають внаслідок користування ресурсами Інтернету:

- потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем;
- інтернет-шахрайство, наприклад фішинг;
- несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем;
- потрапляння комп’ютера до ботнетмережі;
- «крадіжка особистості» — несанкціоноване заволодіння персональними даними особи.

Для того щоб максимально уникнути загроз під час роботи в Інтернеті, варто дотримуватися правил:

1.Використовуйте тільки ліцензійне програмне забезпечення.

2. Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп’ютери.

3. Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.

4. Використовуйте надійні паролі.

5. Приєднуйтеся тільки до перевірених Wi-Fi-мереж.

6. Установіть фільтр спливаючих вікон у браузері.

7. Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера та URL-адреси веб-сайтів.

8. Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли.

9. Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет.

10. Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.

Надіслати фото домашнього завдання **(обов'язково вказати Прізвище та номер групи)** на поштову скриньку: 31051988fwika@gmail.com

Домашнє завдання

Дайте відповіді на запитання (оформіть письмово)

1. Що таке інформаційна безпека?
2. Які основні складові має інформаційна безпека? Охарактеризуйте їх.
3. На які види поділяються загрози інформаційній безпеці залежно від результату шкідливих дій?
4. Які загрози інформаційній безпеці виникають унаслідок користування ресурсами Інтернету?
5. Яких правил потрібно дотримуватися, щоб уникнути загроз інформаційній безпеці під час роботи в Інтернеті