10.10.24 **9 клас** **Вчитель: Артемюк Н.А.**

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

Очікувані результати заняття

Після цього заняття потрібно вміти:

- дотримуватися принципів інформаційної безпеки під час роботи з інформаційними технологіями та системами.

Поміркуйте

- Назвіть можливі загрози для особистих даних.
- Як можна захистити комп’ютер від загроз?

Ознайомтеся з інформацією

Механізми проникнення з Інтернету на локальний комп’ютер і в локальну мережу

- веб-сторінки, що завантажуються в браузер, можуть містити активні елементи, здатні виконувати деструктивні дії на локальному комп’ютері;
- деякі веб-сервери розміщують на локальному комп’ютері текстові файли *cookie,* використовуючи які, можна отримати конфіденційну інформацію про користувача локального комп’ютера;
- електронні листи або дописи в соціальних мережах можуть містити шкідливі посилання;
- за допомогою спеціальних програм можна отримати доступ до дисків і файлів локального комп’ютера тощо.

Для захисту даних під час роботи в Інтернеті доцільно використовувати підключення, захищене шифруванням. Наприклад, за замовчуванням *Google* шифрує з’єднання з *Gmail,* а також при виборі інших сервісів *Google,* наприклад *Google Диск,* активується протокол шифрування *SSL,* який використовується до завершення сеансу роботи.

Щоб визначити, що сайти захищені, слід звернути увагу на їхню URL-адресу — вона починається з *https://.* Це, на відміну від протоколу *http,* — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка https — це означає, що з’єднання захищене й більш безпечне.

Загальний захист мережевого під’єднання здійснюють за допомогою брандмауерів (або міжмережевих екранів) — окремих пристроїв чи спеціальних програм, які для захисту створюють бар’єр між комп’ютером і мережею. За допомогою програм-брандмауерів відслідковуються всі під’єднання й за необхідності дозволяється чи блокується доступ до комп’ютера. Брандмауер може блокувати доступ до комп’ютера вірусів і хробаків, однак він не в змозі знайти їх і знищити. Перш ніж під’єднати комп’ютер до Інтернету, бажано підключити брандмауер.

Виконайте вправу

https://learningapps.org/watch?v=p1f6yddic20

Перегляньте відео

https://youtu.be/uaj86TlQwZI

Запитання до відео

- Які системи є критичними для ураження інформації про їхню діяльність?
- Назвіть причини пошкодження інформації
- Які наслідки можуть мати такі пошкодження?
- Які заходи входять у галузь кібербезпеки?
- Що таке vpn, і як варто його використовувати?
- Що повинен включати в себе надійний пароль?

Завдання

- Придумайте 3 надійних пароля для особистого використання. (8 балів)
- Підготуйте історію про різноманітні загрози безпеці комп'ютерів та даних у них. Це може бути текст, комікс, презентація, ролик. Спробуйте в одній історії поєднати якомога більше загроз безпеці: апаратний збій, програмний збій, помилка людини, зловмисні дії, природні лиха тощо. Можна скористатись ресурсом https://www.storyboardthat.com/storyboard-creator для створення коміксу. Як створювати комікс, показано у відео. (12 балів)

Фото домашньої роботи надішліть на HUMAN або на електронну пошту nataliartemiuk.55@gmail.com

Джерело
Дистосвіта