05.10, 07.10.2022 9 клас

Тема. Основні дії для захисту від шкідливого програмного забезпечення. Загрози безпеці та пошкодження даних у комп'ютерних системах

Мета: ознайомитися з основними методами захисту від інформаційних загроз та навчитися пояснювати принцип їх дії; навчитися дотримуватися принципів інформаційної безпеки під час роботи з інформаційними технологіями та системами.

Повторюємо

дайте відповіді на запитання (усно)

- що таке комп'ютерний вірус?
- що таке антивірусна програма? Наведіть приклади.
- які засоби захисту від комп'ютерних вірусів ви знаєте?

Перегляньте відеоролик за посиланням:

https://youtu.be/DjjYSRNAJgI

Ознайомтеся з інформацією

Шляхи захисту даних

- *Захист доступу до комп'ютера.* Для запобігання несанкціоновано-му доступу до даних, що зберігаються на комп'ютері, використовують облікові записи. Комп'ютер надає доступ до своїх ресурсів тільки тим користувачам, які зареєстровані та ввели правильний пароль. Кожному конкретному користувачеві може бути наданий доступ тільки до певних інформаційних ресурсів. При цьому може проводитися реєстрація всіх спроб несанкціонованого доступу.

- *Захист даних на дисках*. Кожний диск, папка та файл локального комп'ютера, а також комп'ютера, підключеного до локальної мережі, мо-жуть бути захищені від несанкціонованого доступу. Для них встановлю-ються певні права доступу (повний, тільки читання, доступ за паролем), причому права можуть бути різними для різних користувачів.

- *Захист даних в Інтернеті.* Якщо комп'ютер підключений до Інтернету, то будь-який користувач, також підключений до Інтернету, може отри-мати доступ до інформаційних ресурсів цього комп'ютера.

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

- веб-сторінки, що завантажуються в браузер, можуть містити ак-тивні елементи, здатні виконувати деструктивні дії на локальному комп'ютері;

- деякі веб-сервери розміщують на локальному комп'ютері текстові файли *cookie,* використовуючи які, можна отримати конфіденцій-ну інформацію про користувача локального комп'ютера;
- електронні листи або дописи в соціальних мережах можуть міс-ти-ти 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 використову-вати підключення, захищене шифруванням. Наприклад, за замовчуван-ням *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 протоко-лу *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 захи-щене й більш безпечне.

Загальний захист мережевого під'єднання здійснюють за допомогою **брандмауерів** (або міжмережевих екранів) — окремих пристроїв чи спе-ціальних 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.

Перегляньте навчальне відео за посиланням:
https://youtu.be/uaj86TlQwZI

Завдання

- переглянувши навчальне відео, дайте відповіді на запитання (усно):
  1. які системи є критичними для ураження інформації про їхню діяльність?
  2. назвіть причини пошкодження інформації
  3. які наслідки можуть мати такі пошкодження?
  4. які заходи входять у галузь кібербезпеки?
  5. що таке VPN, і як варто його використовувати?
  6. що повинен включати в себе надійний пароль?
- придумайте 3 надійних пароля для особистого використання
- виконайте вправу за посиланням: https://learningapps.org/watch?v=p1f6yddic20

УВАГА!

З травня 2022 року за ініціативи Міжнародним Благодійним Фондом «Допомоги постраждалим внаслідок дорожньо-транспортних пригод» у рамках національного

проєкту «Безпечна країна» серед учнів та вихованців закладів освіти в Україні триває щорічний Всеукраїнський конкурс фото- та відеоробіт «Безпечна країна».

У цьому році він охоплює такі теми:

1) Безбар'єрне освітнє середовище;

2) Безпека життєдіяльності: знаємо та діємо (висвітлення практичних навичок поведінки у разі надзвичайних ситуацій, виявлення мінновибухових предметів, надання домедичної допомоги потерпілим тощо);

3) Молодь за безпеку дорожнього руху;

4) Моя безпечна країна: майбутнє (тема пов'язана із війною в Україні, патріотичними настроями, вільною інтерпретацією бачення безпеки своєї країни та її майбутнього).

Конкурс у цьому році є п'ятим, ювілейним. Щороку до участі долучаються сотні освітніх закладів по усій Україні, переможці нагороджуються цінними призами, а їхні роботи стають базою для формування соціальної реклами «Безпечна країна очима дітей». Згідно умов конкурсу, прийом робіт триватиме до 21 жовтня 2022 року включно. Фото- та відеороботи подаються учасниками в електронному вигляді. Ознайомитися з умовами конкурсу, вимогами до конкурсних робіт та безпосередньо завантажити роботи можна за посиланням https://dopomogadtp.com/konkurs_2022/ Незалежну оцінку фото-та відеоматеріалів проведе повноважне журі, у т.ч. за участю представників МОН, а підведення підсумків та нагородження переможців конкурсу відбудеться у листопаді 2022 року під час проведення IIго етапу Тижня безпеки дорожнього руху в Україні.