Урок 3. Тема: Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення.

Вправа «Незакінчене речення». Перевір свої знань за попередньою темою. Закінчи подані нижче речення.

1. Технології здійснення операцій над текстами, графічними зображеннями, презентаціями, числовими, мультимедійними та іншими даними з використанням комп'ютерів називають… .
2. Мета застосування інформаційних технологій — … .
3. Для реалізації окремих інформаційних технологій, а особливо їх комплексу, створюються… .
4. Інформаційна система — це сукупність взаємопов'язаних елементів, яка призначена для… .
5. Апаратна складова інформаційної системи — це комплекс технічних засобів, який включає наступні пристрої: … .
6. До програмної складової інформаційної системи відносять системні програми, … .

Поміркуй!

1) Які правила захисту даних у комп'ютерних системах ти знаєш?
2) Які загрози можуть виникнути під час роботи в Інтернеті?
3) Які особисті дані потрібно захищати? Які загрози із цим пов'язані?

На уроці ти дізнаєшся:

- ✔ що таке інформаційна безпека та на яких принципах вона базується;
- ✔ які існують види загроз інформаційній безпеці;
- ✔ про загрози для мобільних пристроїв;
- ✔ що таке соціальна інженерія;
- ✔ правила безпечної роботи в Інтернеті.

Вивчи новий матеріал!

У зв'язку зі зростаючою роллю інформаційно-комунікаційних технологій у сучасному суспільстві проблема захисту даних від втрати, викрадення, спотворення або пошкодження потребує посиленої уваги.

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

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

Зверни увагу на указ Президента України про Доктрину інформаційної безпеки України, яку було затверджено у лютому 2017 року (див. стор. 10).

Загрози інформаційній безпеці

З технічної точки зору, залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

Значна частина загроз інформаційній безпеці виникає внаслідок користування ресурсами Інтернету. Серед них основними загрозами є:

- ✔ потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем;
- ✔ інтернет-шахрайство, наприклад фішинг;
- ✔ хакерські атаки;
- ✔ потрапляння комп'ютера до ботнет-мережі;
- ✔ «крадіжка особистості» (Читай подробиці на стор. 11)

Загрози для мобільних пристроїв

Для смартфонів характерні ті самі загрози, що і для стаціонарних комп'ютерів: віруси, троянські програми, мережеві хробаки, рекламні модулі та ін., орієнтовані на різні типи мобільних пристроїв. Як і стаціонарні комп'ютери, смартфони можуть потрапити до ботнет-мережі.

Соціальна інженерія

Соціальна інженерія — це наука, що вивчає людську поведінку та фактори, які на неї впливають. За даними української антивірусної лабораторії Zillya! Антивірус (zillya.ua), наразі більшість заражень шкідливими програмами комп'ютерів і мереж відбувається шляхом обману користувачів з використанням методів соціальної інженерії. Розглянь найбільш поширені прийоми, які використовують зловмисники: (див. стор. 12)

Правила безпечної роботи в інтернеті

Для того щоб максимально уникнути загроз під час роботи в Інтернеті, варто дотримуватися певних правил. Вивчи поради, які надає CERT-UA (див. стор. 12)

Рефлексія. «ПОПС-формула». (Як ти усвідомив зміст пройденого матеріалу?)

Вона розшифровується так:
П – позиція,
О – обґрунтування,
П – приклад,
С – судження.

Кожна з цих позицій – це відповідне речення: "Я вважаю, що…", "Тому що…", "Я можу довести це на прикладі…", "Виходячи з цього, я роблю висновок про те, що…".

Закріпи вивчений матеріал. Виконай інтерактивні вправи:
https://learningapps.org/view5531816, https://learningapps.org/4586421

Д/з § 1.2 стор. - 10-13.