

Опорний конспект

Тема уроку: ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Після вивчення цієї теми учень повинен:

- дотримуватися правил безпечної роботи в Інтернеті;
- розуміти принципи інформаційної безпеки;
- дотримуватися правил безпечної поведінки в Інтернеті;
- усвідомлювати комунікаційну роль ІТ та тенденції розвитку цифрового суспільства та вплив інформаційних технологій на життя людей.

Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних. Також під інформаційною безпекою розуміють комплекс заходів, спрямованих на забезпечення захищеності даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення. Останнім часом до питань інформаційної безпеки включено питання інформаційного впливу на особистість і суспільство.

З технічної точки зору, 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.

Для **смартфонів** характерні ті самі загрози, що й для стаціонарних комп'ютерів: віруси, троянські програми, мережеві хробаки, рекламні модулі та ін., орієнтовані на різні типи мобільних пристроїв.

Соціальна інженерія — це наука, що вивчає людську поведінку та фактори, які на неї впливають. Зловмисники для маніпуляції, щоб спонукати людину виконати певні дії чи розголосити конфіденційну інформацію, часто використовують результати досліджень із соціальної інженерії.

Для того щоб максимально уникнути загроз під час роботи в Інтернеті, варто дотримуватися певних правил: установлювати тільки ліцензійне програмне забезпечення, установлювати програмні продукти тільки з офіційних джерел, установлювати та оновлювати антивірусне програмне забезпечення, установлювати оновлення операційної системи та

іншого програмного забезпечення, використовувати надійні паролі, приєднуватися тільки до перевірених Wi-Fi-мереж, не відкривати повідомлення з електронної пошти та прикріплені до них файли від невідомих осіб, перевіряти URL-адреси веб-сайтів і сертифікат безпеки та ін.

Робота з комп'ютером

Увага! Під час роботи з комп'ютером дотримуйтеся вимог безпеки життєдіяльності та санітарно-гігієнічних норм.

Налаштуйте двохетапну перевірку для вашого облікового запису Google. Для цього:

1. Відкрийте браузер, увійдіть до свого облікового запису.
2. Виберіть кнопку **Додатки Google**  і додаток **Мій обліковий запис** .
3. Виконайте **Вхід і безпека** $\Rightarrow$ **Вхід в обліковий запис Google** $\Rightarrow$ **Двохетапна перевірка**.
4. Виберіть кнопку **Розпочати**.
5. Уведіть повторно пароль від облікового запису.
6. Погодьтеся або змініть номер телефона на сторінці **Налаштуйте свій телефон**, виберіть гіперпосилання **Далі**.
7. Уведіть код, що надійде на мобільний телефон, та виберіть гіперпосилання **Далі**.
8. Виберіть гіперпосилання **Увімкнути**.
9. Виберіть у групі **Резервні коди** гіперпосилання **Згенерувати**.
10. Виберіть гіперпосилання **Завантаження** та збережіть згенеровані коди у вашій папці. Ними можна скористатися для входу в обліковий запис, якщо телефона немає поруч.
11. Закрийте вікно **Збережіть резервні коди**.
12. Вийдіть з вашого облікового запису.
13. Увійдіть повторно до облікового запису. Для цього:
 1. Уведіть логін і пароль.
 2. На сторінці **Двохетапна перевірка** введіть код, що надійде на телефон, або виконайте **Більше варіантів** $\Rightarrow$ **Ввести один з восьмицифрових резервних кодів** і введіть один з кодів, що містяться у збереженому файлі.
 3. Виберіть кнопку **Далі**.
14. Ознайомтеся з порадами для безпеки в Інтернеті від сервісу Google. Для цього:
 1. Виконайте **Додатки Google** $\Rightarrow$ **Мій обліковий запис** $\Rightarrow$ **Вхід і безпека** $\Rightarrow$ **Вхід в обліковий запис Google**.
 2. Виберіть у нижній частині сторінки **Вхід і безпека** гіперпосилання **Ваша безпека понад усе в усіх наших починаннях**.
 3. Ознайомтеся на сторінці **Конфіденційність** з порадами в рубриці **Найкращі поради для безпеки в Інтернеті**.
15. Закрийте вікно браузера.

Складіть карту знань із класифікацією загроз інформаційній безпеці користувача Інтернету. Збережіть карту як зображення та надайте доступ друзям і учителю.