Урок №5

Тема: Інформаційна безпека. Шкідливе програмне забезпечення та боротьба з ним.

➥На цьому уроці ти дізнаєшся про види шкідливого забезпечення та заходи протидії.

! Під час роботи за комп'ютером дотримуйся вимог безпеки життєдіяльності та санітарно-гігієнічних норм.

Докладніше про тему…

Правові аспекти.

Для кожного з нас питання інформаційної безпеки стало невід'ємною частиною життя, починаючи з елементарних речей – встановлення блокування на телефон, конфіденційністю під час листування в чаті, безпечними транзакціями через банківську картку тощо.

➦ **Інформаційна безпека** – *це комплекс заходів щодо запобігання несанкціонованому доступу та використання конфіденційної інформації сторонніми особами.* Інформаційна безпека надає інструменти для захисту фізичних осіб, підприємств, організацій, державних установ, держави тощо.

> Визначення терміну, який надається у Вікіпедії, розкриває повноту напрямків, які входять до сфери безпеки: *«Це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення».*

! Законами України та іншими правовими актами встановлено відповідальність за злочини в галузі інформаційної безпеки. Кримінальним кодексом України передбачено кримінальну відповідальність, наприклад, за:

«Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»	«Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»
«Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, … їх незаконне тиражування та розповсюдження на… носіях інформації»	«Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення»

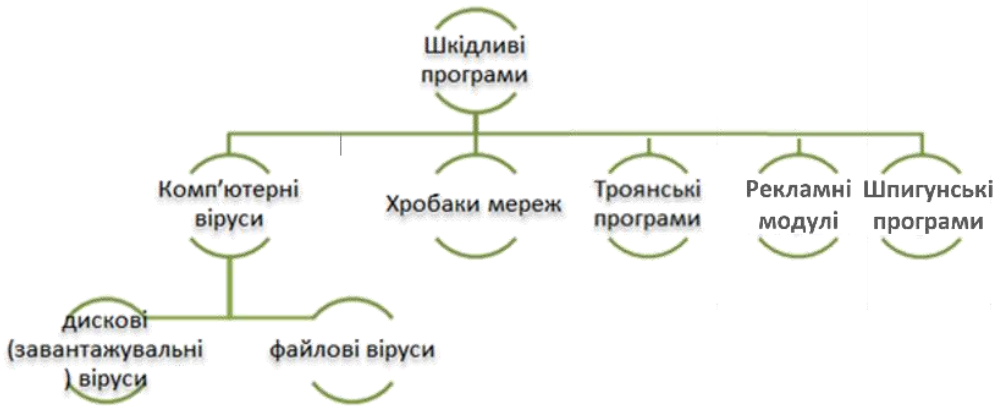
Технічні аспекти.

➦ Залежно від обсягів завданих збитків *загрози інформаційній безпеці поділяють на*:

- нешкідливі – не завдають збитків;
- шкідливі – завдають значних збитків;
- дуже шкідливі – завдають критичних збитків

➦ **Шкідливе програмне забезпечення** — *програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем*. Для шкідливих програм характерно:

- швидке розмноження різними способами;
- автоматичне виконання деструктивних дій.



✓ *Віруси* – програми, здатні саморозмножуватися і виконувати несанкціоновані деструктивні дії.

✓ *Хробаки мереж* – пересилають свої копії комп'ютерними мережами з метою проникнення на віддалені комп'ютери.

✓ *Троянські програми* – програми, що збирають інформацію, модифікують та пошкоджують її, порушують роботу комп'ютера чи використовують його ресурси у зловмисних цілях

У сучасному житті великі збитки і шкоду наносять *шпигунські програми*. Їх основні види:

- програми для зчитування натиснень клавіатури дозволяють зловмисникам отримати паролі та логіни для доступу до особистих акаунтів жертви;
- програмне забезпечення для сканування жорсткого диску дає можливість отримати доступ до встановлених програм на пристрої жертви;
- екранні шпигуни збирають інформацію про діяльність користувача (знімки екрану відвіданих веб-сайтів);
- поштові шпигуни дозволяють збирати дані про контакти жертви з електронної пошти з метою розсилки спам-повідомлень;
- рекламне програмне забезпечення у вигляді небажаних спливаючих вікон використовується для збору особистої інформації користувача, відстеження його дій, а також нанесення шкоди системі безпеки пристрою;
- банківські трояни, маскуючись під легітимні ресурси, можуть отримати доступ до банківських рахунків жертви.

Як розпізнати шпигунську програму?

Найпоширенішими ознаками наявності шкідливого коду на пристрої користувача є *зниження продуктивності* або *збої в роботі* комп'ютера, *масові спливаючі вікна*, а також *підозрілі дії на жорсткому диску*.

➦ Докладніше про шкідливе програмне забезпечення:
- підручник с.34-40
- або подивившись відео: https://youtu.be/Ic7RgwANz1k.