**12, 13.05.25 9 клас Вчитель: Куроп’ятников А. О.**

**Тема. Повторення. Програмне забезпечення та інформаційна безпека**

**Очікувані результати заняття:**

# після цього заняття потрібно вміти

# називати типи програмного забезпечення; пояснювати відмінності між ними та наводити приклади.

# називати різні типи ліцензій на програмне забезпечення, пояснювати відмінності між ними.

# називати основні типи шкідливих програм та пояснювати принцип їх дії.

# пояснювати принципи і методи захисту від інформаційних загроз.

**Виконайте вправу**

<https://wordwall.net/resource/60565700>

**Поміркуйте**

* Що таке програмне забезпечення комп’ютера?
* Для чого служить прикладне програмне забезпечення?
* Яке призначення службового програмного забезпечення?
* Який правовий документ визначає правила використання та поширення програмного забезпечення?
* Які чинники можуть спричинити пошкодження даних комп’ютерними вірусами?
* У чому полягає відмінність комп’ютерного вірусу від решти шкідливих програм?

**Перегляньте відео**

[Класифікація програмного забезпечення](https://www.google.com/search?q=%D0%BB%D1%96%D1%86%D0%B5%D0%BD%D0%B7%D1%96%D1%97+%D0%BD%D0%B0+%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5+%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F+%D1%97%D1%85+%D1%82%D0%B8%D0%BF%D0%B8+%D0%BF%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D1%96%D1%8F&sca_esv=6b5001a3b62373fd&rlz=1C1GCEA_enUA1014UA1014&sxsrf=AHTn8zoiaNUYSrJFtdi9ojfDUScG-D8Ppw%3A1746977828816&ei=JMQgaIDPMYyowPAPnOn_6AU&oq=%D0%9B%D1%96%D1%86%D0%B5%D0%BD%D0%B7%D1%96%D1%97+%D0%BD%D0%B0+%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5+%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%2C+%D1%97%D1%85+%D1%82%D0%B8%D0%BF%D0%B8&gs_lp=Egxnd3Mtd2l6LXNlcnAiUNCb0ZbRhtC10L3Qt9GW0Zcg0L3QsCDQv9GA0L7Qs9GA0LDQvNC90LUg0LfQsNCx0LXQt9C_0LXRh9C10L3QvdGPLCDRl9GFINGC0LjQv9C4KgIIAzIFEAAYgAQyBhAAGBYYHjIGEAAYFhgeMgYQABgWGB4yBhAAGBYYHjIIEAAYFhgKGB4yCBAAGKIEGIkFSI0bUABYAHAAeACQAQCYAXKgAXKqAQMwLjG4AQHIAQD4AQL4AQGYAgGgAn2YAwCSBwMwLjGgB_MIsgcDMC4xuAd9&sclient=gws-wiz-serp#fpstate=ive&vld=cid:a8fd1a86,vid:aZ4tPfNQJZM,st:0)

**Ознайомтеся з інформацією**

**Інформаційна безпека**– розділ інформатики, що вивчає закономірності забезпечення захисту інформаційних ресурсів від втрати, порушення функціонування, пошкодження, спотворення, несанкціонованого копіювання та використання.

**Основні складові інформаційної безпеки:**

* **Доступність**– забезпечення доступу до загальнодоступних даних усім користувачам, захист цих даних від спотворення та блокування зловмисниками.
* **Конфіденційність**– забезпечення доступу до даних на основі розподілу прав доступу.
* **Цілісність** – захист даних від зловмисного або випадкового видалення чи спотворення.

**Класифікація загроз інформаційної безпеки**

**В залежності від**обсягів**збитків:**

* **нешкідливі**– не завдають збитків;
* **шкідливі** - завдають значних збитків;
* **дуже шкідливі** - завдають критичних збитків інформаційній системі, що призводить до повного або тривалого в часі припинення роботи інформаційної системи.

**За метою:**

* зловмисні;
* випадкові.

**За місцем виникнення:**

* зовнішні;
* внутрішні.

**За походженням:**

* природні
* техногенні;
* зумовлені людиною.

**Основні загрози інформаційної безпеки**

* знищення та спотворення даних;
* отримання доступу до секретних або конфіденційних даних;
* пошкодження пристроїв інформаційної системи;
* отримання прав на виконання дій, що передбачені тільки для окремих керівних осіб;
* отримання доступу до здійснення фінансових операцій замість власників рахунків;
* отримання повного доступу до керування інформаційною системою.

**Етичні та правові основи захисту даних**

**Етичні норми**– не використовувати комп’ютерну техніку та програмне забезпечення на шкоду іншим людям, не порушувати авторських прав.

**Правова основа захисту даних**– правові акти.

**Акти, що утверджують права та свободи людини:**

* **Загальна декларація прав людини**(прийнята Генеральною Асамблеєю ООН 10.12.1948 року): *«Стаття 19. Кожна людина має право на ... свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів»;*
* **Конвенція про захист прав людини і основоположних свобод**(прийнята Радою Європи 04.11.1950 року) проголошує, що *свобода вираження поглядів може обмежуватися законодавством «...для запобігання розголошенню конфіденційної інформації»;*
* **Конституція України:***«Стаття 32.... Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом...». «Стаття 54. Громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав...».*

**Кримінальним кодексом України передбачено кримінальну відповідальність за:**

* Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер;
* Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації;
* Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення;
* Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
* Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;
* Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації тощо.

**Заходи реалізації організаційних принципів захисту даних**

|  |  |
| --- | --- |
| **Цілі захисту даних** | **Заходи** |
| Захист від втрати даних внаслідок стихійних явищ, збоїв у роботі елек­тричних мереж, некомпетентності працівників тощо | Використання додаткових пристроїв автономного електроживлення, ство­рення копій особливо важливих даних і зберігання їх у захищених місцях |
| Захист від умисного пошкодження комп’ютерного та мережевого обладнання, викрадення даних безпосередньо з пристроїв | Створення системи охорони з розмежуванням доступу до особливо важливо­го обладнання |
| Захист від викрадення даних власними працівниками | Введення різних рівнів доступу до даних, використання персональних за­хищених паролів, контроль за діяльністю працівників |
| Захист від викрадення, спотворення чи знищення даних з використанням спеціальних комп'ютерних програм | Використання спеціального антишпигунського та антивірусного програмного забезпечення, шифрування даних, що передаються мережами, використання паролів доступу та обов'язкового дублювання даних |

**Перегляньте відео**

<https://youtu.be/cuCIU0RBL60>

**Запитання до відео**

* Що означає інсталювати програму?
* Назвіть етапи інсталяції операційної системи.

**Поміркуйте**

* Які антивірусні програми вам відомі?
* Які з них ви використовуєте? Поясніть чому саме їх.
* Назвіть можливості сучасних операційних систем щодо захисту даних.

**Домашнє завдання**

Пройти тестування <https://naurok.com.ua/test/join?gamecode=2535491>

**Джерела**

* [Дистосвіта](https://dystosvita.org.ua/course/view.php?id=9&section=1)
* [Всеосвіта](https://vseosvita.ua/lesson/pidsumkovyi-urok-prohramne-zabezpechennia-ta-informatsiina-bezpeka-285874.html)