



# Перевірка д/з:

---

Вправа: №6 стор. 12

**6\***. Знайдіть відомості про інформаційні технології, які ви не вивчали в курсі інформатики 5–9 класів, про сфери їх використання. Підготуйте на цю тему комп'ютерну презентацію.

# ВИКОНАЙ ТЕСТ




**Увага!** Під час роботи за комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.

<https://epkmoodle.znu.edu.ua>


□ Секція 1 □

Редагувати ▼


Інформаційні технології в суспільстві

□  Презентація "Основні поняття інформатики. Сучасні інформаційні технології та системи"\_2019 □

Редагувати ▼

□  Практичне завдання\_2019 □

Редагувати ▼

□  Основні поняття інформатики □

Редагувати ▼

# ЗРАЗОК ТЕСТОВОГО ЗАПИТАННЯ

Перехід по тесту

|    |    |    |    |    |
|----|----|----|----|----|
| 1  | 2  | 3  | 4  | 5  |
| 6  | 7  | 8  | 9  | 10 |
| 11 | 12 | 13 | 14 | 15 |
| 16 |    |    |    |    |

[Завершити спробу...](#)

Залишилося часу **0:09:44**

[Розпочати нову спробу](#)

Навігація □ □ ▾

- [На головну](#)
- [Інформаційна панель](#)
- [Сторінки сайту](#)


Ви можете переглянути цей тест, але якщо б це була реальна спроба проходження тесту, перегляд було б заблоковано, тому що:

Тест зараз недоступний

Питання **1**

Відповіді ще не було

Макс. оцінка до 1,00

 Відмітити питання

Редагувати питання

Основними інформаційними процесами є...

Виберіть одну відповідь:

- а. Використання, накопичення, розповсюдження, пошук, захист, кодування, сортування.
- б. Передача, обробка, збереження
- с. Передача, кодування, поширення

[← Практичне завдання\\_2019](#)

Перейти до...

Лекція 1 [▶](#)

[Наступна сторінка](#)



1. Які правила захисту даних у комп'ютерних системах ви знаєте?
2. Які загрози можуть виникнути під час роботи в мережі Інтернет?
3. Які особисті дані необхідно захищати? Які загрози із цим пов'язані?

# Проблеми інформаційної безпеки



# ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У зв'язку із зростанням ролі інформаційно-комунікативних технологій у сучасному суспільстві вимагають посиленої уваги **проблеми захисту даних** від:



# ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Інформаційна безпека** - це стан захищеності систем передачі, обробки та зберігання даних, при якому забезпечена конфіденційність, доступність і цілісність даних

## Конфіденційність

- Забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого доступу.

## Цілісність

- Захист даних від їх зловмисного або випадкового знищення чи спотворення.

## Доступність

- Забезпечення доступу до загальнодоступних даних усіма користувачами, захист цих даних від блокування зловмисниками.

# ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Інформаційна безпека** – це комплекс заходів, направлених на забезпечення захищеності даних від несанкціонованого доступу, використання, розголошення, внесення змін або знищення.

У лютому 2017 указом Президента України була затверджена Доктрина інформаційної безпеки України, яка визначає національні інтереси України в інформаційних сфері.

## **Життєво важливі інтереси суспільства і держави:**

- захист від агресивного впливу деструктивної пропаганди;
- захист від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;
- всебічне задоволення потреб громадян, підприємств, установ і організацій всіх форм власності в доступі до достовірних та об'єктивних даних і т.п.



# ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З технічної точки зору, в залежності від результату шкідливих впливів, можна виділити такі **види загроз інформаційної безпеки**:

- отримання несанкціонованого доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп'ютерної інформаційної системи;
- отримання несанкціонованого доступу до управління роботою комп'ютерної інформаційної системи;
- знищення і внесення змін до даних.

# ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## Загрози Інформаційної безпеки,

що виникають у результаті користування ресурсами Інтернету:



Проникнення до  
інформаційної  
системи  
шкідливого  
програмного  
забезпечення

?



Інтернет-  
шахрайство

?



Хакерські атаки

?



Ботнет-мережі

?



Крадіжка  
особистості

?

# ЗАГРОЗИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

**Смартфон** – це мобільний телефон, доповнений функціями персонального комп'ютера, зі своєю операційною системою і іншим програмним забезпеченням.



*Які загрози інформаційній безпеці виникають внаслідок користування мобільним телефоном?*

# ПРАЦЮЄМО ЗА КОМП'ЮТЕРОМ



**Увага!** Під час роботи за комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.

Групова робота над презентацією

## **«Загрози інформаційної безпеки»:**

- Шкідливого програмного забезпечення
  - Інтернет-шахрайство
  - Хакерські атаки
  - Ботнет -мережі
  - Крадіжка особистості
  - Загрози для мобільних пристроїв
- ст. 13-14

# СОЦІАЛЬНА ІНЖЕНЕРІЯ

**Соціальна інженерія** – це наука, яка вивчає людську поведінку і фактори, які на неї впливають.

Найбільш поширені прийоми, які використовуються зловмисниками (*засновані на методах соціальної інженерії - за даними антивірусної лабораторії **Zillya! Антивірус** (zillya.ua)*

- Відправка електронних листів, зміст яких спонукає користувача відкрити прикріплений до листа файл.
- Створення сайтів, які дуже схожі на справжні, для отримання логінів і паролів користувачів.
- Комбінація двох попередніх методів - відправка електронного листа з пропозицією перейти на фішинговий сайт.

# ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ

Рекомендації **CERTUA** (*англ. Computer Emergency Response Team of Ukraine - команда України по реагуванню на комп'ютерні надзвичайні ситуації*)


1. Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.
2. Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.
3. Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.
4. Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.
5. Приєднуйтеся тільки до перевірених **Wi-Fi**-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені **Wi-Fi**-мережі.
6. Установіть фільтр спливаючих вікон у браузері.


# ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ

Рекомендації **CERTUA** (*англ. Computer Emergency Response Team of Ukraine - команда України по реагуванню на комп'ютерні надзвичайні ситуації*)

7. Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера (мал. 1.4) та **URL**-адреси веб-сайтів, щоб визначити, чи не підроблений сайт ви відвідуєте.

Будьте обережні, якщо в адресному рядку браузера відображаються інші позначки:

 — інформація або не захищено. З'єднання із сайтом не конфіденційне;

 — не захищено або небезпечно. Уникайте перегляду таких сайтів.

8. Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.

9. Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет. Дуже легко розмістити дані в мережі Інтернет, але дуже складно їх видалити з неї.

10. Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.

# ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ

## Рекомендації для користувачів смартфонів:

- не дзвоніть на незнайомі номери;
- уважно контролюйте послуги, на які ви підписуєтеся;
- встановлюйте мобільні додатки тільки з офіційних магазинів:  
*PlayMarket (Android), AppStore (iOS), Marketplace (WindowsPhone);*
- уважно стежте за тим, до чого вимагає доступ програма при установці і оновленні програмного забезпечення на мобільних пристроях.



# ПРАЦЮЄМО ЗА КОМП'ЮТЕРОМ



**Увага!** Під час роботи за комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.

## Виконати:

- **вправа 1, 2** «Тема \_ Проблеми інформаційної безпеки»;
- **вправа (п.1-15) стр.16.**

# ДОМАШНЄ ЗАВДАННЯ

Вивчити: § 1.2;

Виконати:

- вправа (п.1-15) стор.16;
- № 3 стор.18.

