

ПРАКТИЧНА РОБОТА №7

Тема: Інформаційна безпека

Мета роботи: формування знань про основи інформаційної безпеки, основні загрози в інформаційному середовищі та набуття практичних навичок захисту персональних даних і безпечної поведінки в цифровому просторі.

Короткі теоретичні відомості

Інформаційна безпека – це стан захищеності інформації, при якому забезпечуються її конфіденційність, цілісність та доступність. Основними загрозами є: шкідливе програмне забезпечення, фішинг, соціальна інженерія, витік даних, кібербулінг тощо.

Практичні завдання

Завдання 1. Охарактеризуйте основні складові інформаційної безпеки:

Таблиця 1.

Основні складові інформаційної безпеки

Складова	Визначення	Приклад порушення
Конфіденційність		
Цілісність		
Доступність		

Завдання 2. Проаналізуйте 3 найбільш поширені загрози інформаційній безпеці (наприклад: фішинг, віруси, витік даних):

Таблиця 2.

Аналіз кіберзагроз

Вид загрози	Опис	Механізм дії	Наслідки

Завдання 3. Оцініть власний рівень інформаційної безпеки.

Таблиця 3

Самооцінка рівня інформаційної безпеки

Показник	Так / Ні	Коментар
Використання складних паролів		
Наявність двофакторної аутентифікації		
Регулярне оновлення ПЗ		
Захист персональних даних		
Використання антивірусу		

Завдання 4. Розгляньте ситуацію:

Ви отримали електронний лист із проханням терміново підтвердити банківські дані за посиланням.

Необхідно:

визначити тип загрози
описати ознаки небезпеки
запропонувати алгоритм дій.

Завдання 5. Аналіз інформаційної безпеки в гірничодобувній галузі

Розгляньте ситуацію:

На гірничому підприємстві використовується автоматизована система управління виробничими процесами (SCADA), а також геоінформаційні системи (ГІС) для моніторингу родовищ. Унаслідок кібератаки було втрачено доступ до частини даних та порушено роботу обладнання.

Потрібно:

Визначити основні кіберзагрози для кожного елемента.

Оцінити можливі наслідки для виробництва та безпеки працівників.

Запропонувати заходи захисту (технічні та організаційні).

Зробити висновок про важливість інформаційної безпеки у гірничій галузі.

Таблиця 4.

Вплив антропогенних факторів на ліси

Елемент системи	Потенційна загроза	Можливі наслідки	Заходи захисту
SCADA-система			
ГІС-система			
База даних підприємства			
Мережеве обладнання			

Завдання 6. Розробіть пам'ятку (інфографіку або короткий список правил)

«10 правил безпечної поведінки в Інтернеті» для студентів.

Контрольні запитання.

1. Що таке інформаційна безпека?
2. Назвіть основні принципи інформаційної безпеки.
3. Які існують основні види кіберзагроз?
4. Що таке фішинг і як його розпізнати?
5. Які заходи захисту персональних даних є найбільш ефективними?
6. Що таке соціальна інженерія?
7. Яку роль відіграють паролі в забезпеченні безпеки?
8. Що таке двофакторна аутентифікація?
9. Які наслідки може мати витік інформації?
10. Як забезпечити безпечну роботу в мережі Інтернет?