**КОМП’ЮТЕРНІ МЕРЕЖІ ТА КІБЕРБЕЗПЕКА**

**Кафедра комп’ютерних систем і мереж**

**Факультет Інформаційних технологій**

|  |  |
| --- | --- |
| ***Лектор*** | **Доцент Блозва А.І.** |
| ***Семестр*** | **7** |
| ***Освітній ступінь*** | **Бакалавр** |
| ***Кількість кредитів ЄКТС*** | **4** |
| ***Форма контролю*** | **Залік** |
| ***Аудиторні години*** | **30 (15год лекцій, 15 год практичних/лабораторних)**  |

**Загальний опис дисципліни**

Сучасний інформаційний світ постійно працює у високому темпі і розвитку. Великі об’єми даних передаються кожної секунди на великі відстані. Тому необхідно забезпечити безвідмовну роботу комп’ютерної мережі У даній дисципліні розглядається структурна моделі OSI комп’ютерної мережі, які є протоколи, що забезпечують стабільну роботу. Вивчається що таке маршрутизатори і комутатори, як вони працюють. Створення віртуальних машин. Структура мережевого захисту. Які є види атак і як захищатися. Розглянуто основні вимоги до побудови комп’ютерної мережі офісу.

Даний курс розроблено і схвалено компанією CISCO, яка є світовим лідером у напрямі побудови комп’ютерних мереж та кіберзахисту.

Також при позитивному складанні екзамену по дисципліні студент отримає два сертифікати від компанії CISCO про проходження даного курсу.

**Теми лекцій:**

1. Комп’ютерні мережі у нашому повсякденному житті.

2. Передача даних у локальній мережі.

3. Мережева адресація.

4. Надання мережевих сервісів.

5. Створення домашньої мережі.

6. Елементи кібербезпеки.

7. Налаштування промислового мережевого обладнання.

8. Тестування і пошук несправностей у локальній мережі.

9. Кібербезпека – світ експертів і злочинців.

10. Куб кібербезпеки.

11. Кібербезпека – загрози, вразливості та атаки.

12. Мистецтво захисту таємниць.

13. Забезпечення цілісності даних.

14. Концепція п’яти дев’яток кіберзахисту.

15. Захист домену кібербезпеки.

**Теми занять:**

***(практичних, лабораторних)***

1. Створення простої мережі та трасування підключення до Інтернету.

2. Визначення конфігурації ІР-адреса комп’ютера. Виготовлення Ethernet кабеля.

3. Мережеві підключення та службові команди. Підключення до WI-FI роутера.

4. Захоплення пакетів за допомогою WireShark.

5. Вивчення дозволів DNS-імен.

6. Базові налаштування безпеки WI-FI мереж.

7. Створення мережі невеликого офісу. Пошук несправностей у мережі.

8. Встановлення віртуальної машини. Вивчення автентифікації, авторизації та обліку.

9. Виявлення загроз та вразливостей.

10. Використання стенографії для приховування паролей.

11. Злам паролів користувачів на окремому ПК.

12. Використання цифрових підписів.

13. Створення віддаленого доступу.

14. Захист Linux систем.

15. Захист Windows систем.