

| | |
|---|--|
| Освітній компонент | ВОК Моніторинг, аудит та управління системами кібербезпеки |
| Рівень ВО | перший бакалаврський |
| Назва спеціальності/освітньо-професійної (освітньо-наукової) програми | 125 Кібербезпека та захист інформації/ Кібербезпека та захист інформації |
| Форма навчання | денна |
| Курс, семестр, протяжність | 8 семестр, 4-ий рік навчання, протяжність — один семестр |
| Семестровий контроль | залік |
| Обсяг годин (усього: з них лекції/практичні) | 150 год: лекції 10 год, лабораторні 20 год |
| Мова викладання | українська |
| Кафедра, яка забезпечує викладання | комп'ютерних наук та кібербезпеки |
| Автор курсу | Онищук Оксана Олександрівна |
| Короткий опис | |
| Вимоги до початку вивчення | Володіти базовими знаннями з основ та концепції налаштування, проектування системи кібербезпеки. |
| Що буде вивчатися | Програма спрямована на вивчення основи комутації, маршрутизації та бездротових мереж версії 7.0 (SRWE). Це другий курс освітньої програми CCNA. Він присвячений технологіям комутації та роботі маршрутизаторів, які підтримують мережі малого та середнього бізнесу, і включає бездротові локальні мережі (WLAN) та принципи безпеки. Крім вивчення ключових принципів комутації і маршрутизації, студенти зможуть виконувати базову конфігурацію мережі та усувати несправності, виявляти та нейтралізувати загрози безпеки LAN, а також налаштовувати та забезпечувати базову WLAN. |
| Чому це цікаво/треба вивчати | У цьому курсі вивчають ключових принципів комутації і маршрутизації, студенти зможуть виконувати базову конфігурацію мережі та усувати несправності, виявляти та нейтралізувати загрози безпеки LAN, а також налаштовувати та забезпечувати базову WLAN. |
| Чому можна навчитися (результати навчання) | Студенти зможуть вести моніторинг, аудит та управляти системою кібербезпеки, налаштувати пристрої з використанням практичних рекомендацій |

| | |
|---|--|
| | <p>щодо забезпечення безпеки, пояснювати процес переадресації даних комутаторами Рівня 2, реалізовувати VLAN та транкінгу в комутованій мережі, виявляти і усувати проблем із маршрутизацією між віртуальними локальними мережами на пристроях Рівня 3, пояснювати як протокол STP забезпечує резервування у комутованих мережах, шукати та усувати несправностей EtherChannel у комутованих мережах, впроваджувати DHCPv4 для роботи у кількох локальних мережах. Налаштування динамічного розподілу адрес у мережах IPv6, пояснювати того, як FHRP забезпечують послуги шлюзу за замовчуванням у мережі з резервуванням, як уразливості загрожують безпеці локальної мережі, налаштовувати безпеку на комутаторі для нейтралізації атак на локальну мережу, пояснювати як WLAN забезпечують мережне з'єднання, реалізовувати WLAN за допомогою бездротового маршрутизатора і контролера бездротової локальної мережі (WLC)., ояснювати як маршрутизатори використовують інформацію у пакетах для прийняття рішень щодо переадресації, налаштовувати статичних маршрутів IPv4 та IPv6 та усувати неполадок з маршрутами статичними та за замовчуванням.</p> |
| <p>Як можна користуватися набутими знаннями й уміннями (компетентності)</p> | <p>Потреба в добре підготовлених спеціалістах з кібербезпеки продовжує зростати в геометричній прогресії. Навчання фахівця з кібербезпеки вимагає глибокого розуміння та ознайомлення з тим, як відбуваються моніторинг, аналіз та управління системамою кібербезпеки. Ці навички, природно, також включатимуть вивчення методів, які використовують для конфіденційності та безпеки комп'ютера та мережі.</p> |