Освітній компонент	ВОК Тестування на проникнення, етичний хакінг та цифрова криміналістика
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	7 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 кібербезпеки.
Що буде вивчатися	Програма спрямована на створення глобальних засобів вирішення проблем, необхідних для побудови, масштабування, безпеки та захисту мереж, які використовуються в нашому бізнесі та повсякденному житті. Навчання фахівця з кібербезпеки вимагає глибокого розуміння та ознайомлення з тим, як відбуваються кібератаки, а також як їх виявляють і запобігають. Ці навички, природно, також включатимуть вивчення методів, які використовують зловмисники для обходу даних, конфіденційності та безпеки комп'ютера та мережі.
Чому це цікаво/треба вивчати	У цьому курсі учні використовуватимуть інструменти та методи в «пісочниці», середовищі віртуальної машини, що дозволяє їм створювати, впроваджувати, контролювати та виявляти різні типи кібератак. Практичні заняття проводяться в цьому середовищі, щоб студенти могли отримати необхідні навички та знання, необхідні для запобігання цим і майбутнім кібератакам. Дірки в безпеці та вразливі місця, створені в цьому курсі, слід використовувати лише з дотриманням етичних норм і лише в цьому віртуальному середовищі «пісочниці». Експериментування з цими інструментами, техніками та ресурсами за межами

	наданого віртуального середовища ізольованого програмного середовища залишається на розсуд викладача та місцевої установи. Якщо студент має будь-які сумніви щодо того, які комп'ютерні системи та мережі є частиною віртуального середовища ізольованого програмного середовища, він повинен зв'язатися зі своїм інструктором перед будь-яким експериментом. Несанкціонований доступ до даних, комп'ютерних і мережевих систем є злочином у багатьох юрисдикціях і часто супроводжується тяжкими наслідками, незалежно від мотивації злочинця.
Чому можна навчитися (результати навчання)	Студенти зможуть створювати, впроваджувати, контролювати та виявляти різні типи кібератак. Практичні заняття дають можливість студентам отримати необхідні навички та знання, необхідні для запобігання цим і майбутнім кібератакам.
Як можна користуватися набутими знаннями й уміннями (компетентності)	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 кібератаки, а також як їх виявляють і запобігають. Ці навички, природно, також включатимуть вивчення методів, які використовують зловмисники для обходу даних, конфіденційності та безпеки комп'ютера та мережі.