Опис освітнього компонента вільного вибору

Освітній компонент	Вибірковий освітній компонент 3 «Соціальна інженерія»
Рівень ВО	перший (бакалаврський) рівень
Назва спеціальності/освітньо-професійної програми	125 Кібербезпека та захист інформації/ Кібербезпека та захист інформації
Форма навчання	Денна
Курс, семестр, протяжність	2 (4 семестр), 5 кредитів ЄКТС
Семестровий контроль	залік
Обсяг годин (усього: з них лекції/практичні)	150 год, з них: лекц. – 10 год, лаб. – 20 год
Мова викладання	українська
Кафедра, яка забезпечує викладання	Комп'ютерних наук та кібербезпеки
Автор ОК	Доктор педагогічних наук, професор кафедри комп'ютерних наук та кібербезпеки **Чернящук Наталія Леонідівна**
Короткий опис	
Вимоги до початку вивчення	Вивчення та оволодіння основними концепціями соціальної інженерії, етапами і процедурами соціоінженерної діяльності, методами соціальної інженерії, основними напрямами соціоінженерної діяльності.
Що буде вивчатися	Предмет вивчення присвячений вивченню та засвоєнню сучасних технологій, які використовуються для соціальної інженерії.
Чому це цікаво/треба вивчати	Формування комплексу знань, що включає основні теоретичні поняття соціальної інженерії, методи аналізу поведінки та психологічні техніки, які використовуються для виявлення та запобігання соціально-інженерним загрозам, зокрема їх застосування в сучасному інформаційному середовищі для забезпечення кібербезпеки та захисту даних.
Чому можна навчитися (результати навчання)	- Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційних технологій; - здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій; - здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.
Як можна користуватися набутими знаннями й уміннями (компетентності)	Використання набутих знань на практиці, наприклад, технічних прийомів маніпулювання користувачами, які використовуються під час атак.