КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ПРОЕКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД

Тип:	дисципліна професійної підготовки
Код:	ОК-20
Семестр:	5, 6
Загальна кількість кредитів/годин:	7 кредитів / 210 годин
Форма контролю:	іспит, іспит
Викладач:	доцент, Дудатьєв А.В.
Необхідні обов'язкові попередні та супутні навчальні дисципліни:	«Комп'ютерні системи та мережі», «Управління ризиками інформаційної безпеки», «Нормативно-правове забезпечення інформаційної безпеки»
Місце у структурно-логічній схемі:	ОК-20 Комплексні системи захисту інформації: проектування, впровадження, супровід викладається на третьому році навчання
Форми навчання:	лекції, лабораторні заняття, самостійна робота, підготовка курсової роботи
Критерії оцінювання:	поточний контроль – 50 балів підсумковий контроль (іспит) – 50 балів
Мова викладання:	українська

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи та технології захисту інформації в системах передачі даних та системах зв'язку. Типи шахрайств. Захист GSM. Алгоритми захисту. Алгоритми захисту GSM та їх взламування. Технологія перехоплення сигналу GSM. Безпека CDMA. Оцінка захищеності інформації в системах передачі даних та системах зв'язку. Засоби забезпечення безпеки в обчислювальних мережах. Обмеження доступу до облікового запису Адміністратор. Обмеження доступу по мережі. Контроль за обліковими записами Адміністратор. Класифікація вразливостей. Захист серверів та робочих станцій. Засоби захисту локальних мереж при приєднанні до Інтернету. Технологія міжмережевих екранів. Побудова правил міжмережевих екранів. Класифікація міжмережевих екранів. Захист програмного забезпечення. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Захист баз даних. Типи загроз. Ідентифікація, аутентифікація та авторизація користувачів. Дискреаційний, мандатний та рольовий принцип керування доступом. Схеми даних. Керування контекстом виконання процедур та функцій користувачів. Захист файлів баз даних. Шифрування даних на диску. Аудит. Керування ролями.

Програмні результати навчання (ПРН) визначені в освітній програмі

Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних,стандартів та практик щодо здійснення професійної діяльності **ПРН-15**. Здатність здійснювати проектування (розробку) систем, технологій і засобів кібербезпеки **ПРН-17**. Здатність здійснювати протидію

несанкціонованому проникненню в ІТ системи і мережі **ПРН-18**. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем **ПРН-19.** Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС **ПРН-21**.Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки **ПРН-22**. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою **ПРН-23.** Здатність проводити дослідження у практичній професійній діяльності на відповідному рівні **ПРН-28**.