УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тип:	дисципліна професійної та практичної підготовки
Код:	ОК-22
Семестр:	5
Загальна кількість кредитів/годин:	4 кредити / 120 годин
Форма контролю:	іспит
Викладач:	к.т.н., Барибін О.І.
Необхідні обов'язкові попередні та супутні навчальні дисципліни:	«Нормативно-правове забезпечення інформаційної безпеки», «Стандартизація та сертифікація в інформацій безпеці»
Місце у структурно-логічній схемі:	ОК-22 Управління ризиками інформаційної безпеки викладається на третьому році навчання
Форми навчання:	лекції, лабораторні заняття, самостійна робота
Критерії оцінювання:	поточний контроль – 80 балів підсумковий контроль (іспит) – 20 балів
Мова викладання:	українська

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Місце управління ризиками в побудові СУІБ. Основні стандарти за темою. Зміст основних визначень. Оцінка ризиків ІБ. Обробка ризиків ІБ. Прийняття, комунікація, моніторинг і перегляд ризиків ІБ. Документальне забезпечення управління ризиками ІБ. Інструментальні засоби управління ризиками ІБ

Програмні результати навчання (ПРН) визначені в освітній програмі

Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки **ПРН-15**.

Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж **ПРН-19**.

Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ **ПРН-20**.

Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки **ПРН-24**.

Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу; здійснювати аналіз ризиків функціонування

ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками **ПРН-25**.

Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки **ПРН-28**.