КОМП'ЮТЕРНИЙ ЗІР ТА ОБРОБКА СИГНАЛІВ

Тип:	дисципліна професійної підготовки за вибором студента
Код:	К-39
Семестр:	7; 8
Загальна кількість кредитів/годин:	8 кредитів / 240 годин
Форма контролю:	залік; іспит
Викладач:	к.т.н., Загоруйко Л.Г.
Необхідні обов'язкові попередні та супутні навчальні дисципліни:	Основи алгоритмізації та програмування, Інтелектуальний аналіз даних, Організація баз даних та знань, Вища математика, Обчислювальна математика
Місце у структурно-логічній схемі:	К-39 Комп'ютерний зір та обробка сигналів викладається на четвертому 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

Формування зображень. Формування зображень за допомогою гамма-випромінювання. Рентгенівські зображення. Зображення в ультрафіолетовому діапазоні. Зображення в інфрачервоному діапазоні. Зображення в діапазоні радіохвиль. Основи цифрового представлення зображень. Елементи зорового сприйняття. Будова людського ока. Формування зображення в людському оці. Зчитування і реєстрація зображення. Дискретизація і квантування зображення. Основні поняття, що використовуються при дискретизації та квантуванні. Фільтрація зображень. Просторова і частотна фільтрація. Обробка кольорових зображень. Основи теорії кольору. Моделі RGB, CMY і CMYK, HSI. Сегментація зображень. Знаходження точок, ліній. Порогова обробка. Розпізнавання зображень. Розпізнавання зображень методом теорії прийняття рішень (Нейронні мережі). Структурні методи розпізнавання (Співставлення номерів фігур та строк символів).

Програмні результати навчання (ПРН) визначені в освітній програмі

застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах ПРН-18

виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС; використовувати інструментарій для моніторингу даних в ІТС; виконувати аналіз зловмисного програмного коду ПРН-26

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