СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Організація баз даних та знань	
1. Кафедра:	Кафедра кримінального аналізу та інформаційних технологій
2. Ступінь вищої освіти/освітня програма	«магістр» \ОПП «Кримінальний аналіз»
3. Статус навчальної дисципліни	Вибіркова
4. Місце в структурно-логічній схемі	Викладається: у третьому семестрі на другому році навчання
5. Кількість кредитів ЄКТС: **- загальна кількість годин:** ***- з них аудиторних годин:*** ***- лекції:*** ***- семінарські заняття:*** ***- практичні заняття:*** ***- самостійна робота:***	4 120 8 12 100
6. Короткий зміст навчальної дисципліни	Навчальна дисципліна **«Організація баз даних та знань»** спрямована на формування у здобувачів вищої освіти системи знань та практичних навичок щодо формування теоретичної бази знань для кваліфікованого та ефективного використання теорії організації реляційних баз даних, а також знань в процесі побудови та застосування інформаційних систем з метою організації надійної та ефективної роботи з інформацією. Засвоївши програму навчальної дисципліни «Організація баз даних та знань», здобувачі вищої освіти мають бути здатнимина кваліфікованому рівні застосовувати отриманні знання під час роботи із сучасними пошуковими, аналітичними та іншими інформаційними системами. **Метою дисципліни є** підготовка висококваліфікованих фахівців, які зможуть не тільки кваліфіковано вирішувати питання роботи з існуючою

	інформаційною системою, але й забезпечувати раціональну побудову нових спеціалізованих систем, від якісної роботи яких залежить ефективність роботи організації в цілому.
7. Міждисциплінарні зв'язки	«Організація баз даних та знань» ґрунтується на застосуванні здобувачами вищої освіти знань із дисциплін: «Сучасні інформаційні технології», «Програмні методи та засоби алгоритмізації процесів». З іншого боку зазначений курс «Організація баз даних та знань» є підґрунтям для наступних дисциплін: «Системний аналіз та прогнозування ризиків», «Системи підтримки прийняття рішень», «Теорія та проектування інформаційних систем», «Аналіз даних та знань», «Кримінальний аналіз», «Інформаційна та кібернетична безпека», «Технологія моделювання», «Безпека технічних систем».
8. Форми і методи навчання:	Заняття проводяться у формі лекцій, семінарських, практичних занять. Лекції здійснюються з ключових проблем курсу. Методами навчання є: пояснювально-ілюстративний, репродуктивний, проблемно-пошуковий та дослідницький методи.
9. Форма контролю:	Залік
10. Методи та критерії оцінювання:	Підсумкова оцінка з навчальної дисципліни визначається за рейтинговою шкалою, що передбачає накопичення 100 балів, які перераховуються в національну шкалу та шкалу оцінювання ЄКТС. Види робіть, які складають суму підсумкових балів здобувача вищої освіти: - робота на семінарських заняттях – 80 б; - самостійна робота – 20 б;
11.Перелік програмних компетентностей та результатів навчання, визначених відповідною освітньою програмою	**Загальні компетентності:** ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК5. Здатність розробляти проекти та управляти ними.. **Спеціальні компетентності**: СК1. Здатність інтегрувати знання та здійснювати системні дослідження, застосовувати методи математичного та інформаційного моделювання складних систем та процесів різної природи. СК2. Здатність проектувати архітектуру інформаційних систем. СК3. Здатність розробляти системи підтримки прийняття рішень та рекомендаційні системи. СК4. Здатність оцінювати ризики, розробляти алгоритми управління ризиками в складних системах різної природи. СК5. Здатність моделювати, прогнозувати та проектувати складні системи і процеси на основі методів та інструментальних засобів системного аналізу. СК7. Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів. СК10. Здатність до самоосвіти та професійного розвитку.

Результати навчання:

РН 1 Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень.

РН 2 Будувати та досліджувати моделі складних систем і процесів застосовуючи методи системного аналізу, математичного, комп'ютерного та інформаційного моделювання.

РН 3 Застосовувати методи розкриття невизначеностей в задачах системного аналізу, розкривати ситуаційні невизначеності та невизначеності в задачах взаємодії, протидії та конфлікту стратегій, знаходити компроміс при розкритті концептуальної невизначеності.

РН 4 Розробляти та застосовувати методи, алгоритми та інструменти прогнозування розвитку складних систем і процесів різної природи.

РН 6 Застосовувати методи машинного навчання та інтелектуального аналізу даних, математичний апарат нечіткої логіки, теорії ігор та розподіленого штучного інтелекту для розв'язання складних задач системного аналізу.

РН 7 Розробляти інтелектуальні системи в умовах слабо структурованих даних різної природи.

РН 8 Здійснювати ідентифікацію та оцінювання параметрів математичних моделей об'єктів керування.

РН 9 Розробляти та застосовувати моделі, методи та алгоритми прийняття рішень в умовах конфлікту, нечіткої інформації, невизначеності та ризиків.

РН 13. Розробляти та застосовувати методи, алгоритми та інструменти прогнозування

12. ***Рекомендована література:***

1. Актуальні питання інформаційного права: навч. посіб. /В. Г. Хахановський, О. В. Корнейко. Київ: Нац. акад. внутр. справ, 2024. 258 с.
2. Анонімність в інтернеті. Цифрові цінності: наук.-прак.посібник /авт.кол.: М.Г. Вербенський, В.О. Криволапчук, Д.В. Смерницький та ін. Київ: «Видавництво Людмила, 2022. 48 с.
3. Базова безпека вашого мобільного пристрою. URL: https://deepstateua.com/bazova-biezpieka-vashogho-mobilnogho-pristroiu
4. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : 2020. 112 с.
5. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д. ю. н., проф. В. Л. Грохольського. Одеса. ОДУВС, 2020. 142 с.
6. Куцаєв В.В., Живило Є.О., Срібний С.П., Черниш Ю.О. Розширення термінології сучасного кіберпростору. URL: mino.esrae.ru/pdf/2014/3Sm/1387.doc
7. Форос Г.В. Правові основи захисту інформації в кіберпросторі. *Правова держава*. Одеса. № 30. 2018. С. 181-187.
8. Гуцалюк, М. В. (2025). Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності. *Інформаційне право / Інститут прикладних правових досліджень*, № 1(52). DOI: https://doi.org/10.37750/2616-6798.2025.1(52).324708
9. Honcharuk, V. (2025, September). Legal mechanisms for combating cybercrime: global practice and the Ukrainian context. *Issues of Crime Prevention*, 49(49), 178–184. DOI: https://doi.org/10.31359/2079-6242-2025-49-178