СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційна та кібернетична безпека	
1. Кафедра:	Кафедра кримінального аналізу та інформаційних технологій
2. Ступінь вищої освіти/освітня програма	«магістр»/ «Системний аналіз»
3. Статус навчальної дисципліни	Вибіркова
4. Місце в структурно-логічній схемі	Викладається: заочна форма навчання - у третьому семестрі другого року навчання.
5. Кількість кредитів ЄКТС: **- загальна кількість годин:** ***- з них аудиторних годин:*** ***- лекції:*** ***- семінарські заняття:*** ***- самостійна робота:***	4 120 8 12 100
6. Короткий зміст навчальної дисципліни	Навчальна дисципліна **«Інформаційна та кібернетична безпека»** спрямована на формування у здобувачів вищої освіти системи знань та практичних навичок щодо забезпечення захисту інформаційних ресурсів і цифрового середовища в умовах сучасних кіберзагроз. Її вивчення дозволяє осягнути принципи безпеки інформаційних систем, зрозуміти методи технічного, програмного й організаційного захисту, а також виробити комплексний підхід до управління ризиками. Важливим є й те, що дисципліна формує вміння застосовувати сучасні стандарти та моделі безпеки, аналізувати вразливості, оцінювати рівень захищеності систем та обґрунтовувати рішення щодо їх удосконалення. Вона сприяє розвитку критичного мислення, відповідального ставлення до інформації та підготовці фахівців, здатних ефективно працювати у сфері інформаційної та кібернетичної безпеки. **Метою** дисципліни є надання теоретичних знань та практичних навичок здобувачам вищої освіти щодо організаційно-правових засад актуальних і важливих питань протидії кіберзагрозам та визначення шляхів удосконалення цього напрямку діяльності.
7. Міждисциплінарні зв'язки	Інформаційна та кібернетична безпека ґрунтується на застосуванні здобувачами вищої освіти знань із дисциплін: «Сучасні інформаційні технології», «Захист інтелектуальної власності», «Кримінальний аналіз». Ці знання забезпечують всебічний розвиток аналітичних навичок

	здобувачів вищої освіти, сприяють формуванню здатності до критичного мислення та інтеграції даних із різних джерел. Вони дозволяють застосовувати комплексний підхід до вивчення та використання кримінального аналізу в професійній діяльності, що включає ефективне прогнозування злочинів, оптимізацію роботи правоохоронних органів та створення стратегій запобігання кіберзлочинності.
8. Форми і методи навчання:	Заняття проводяться у формі лекцій, семінарських 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. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК10. Здатність оцінювати та забезпечувати якість виконуваних робіт. **Спеціальні компетентності**: СК4. Здатність оцінювати ризики, розробляти алгоритми управління ризиками в складних системах різної природи. СК9. Здатність здійснювати захист прав інтелектуальної власності, комерціалізацію результатів досліджень та інновацій. СК10. Здатність до самоосвіти та професійного розвитку **Результати навчання**: 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 14. Здатність застосовувати сучасні інформаційні технології при вирішення завдань кримінального аналізу в умовах військового стану.

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