СІЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ	
1. Кафедра:	Кафедра кримінального аналізу та інформаційних технологій
2. Ступінь вищої освіти:	Магістр / «Кримінальний аналіз»
3. Статус навчальної дисципліни:	Обов'язкова
4. Місце в структурно-логічній схемі:	Викладається у другому семестрі на першому році навчання.
5. Кількість кредитів ЄКТС: **- загальна кількість годин:** **- з них аудиторних годин:** **- лекції:** **- семінарські заняття** **- практичні заняття:** **- самостійна робота:**	3 90 6 10 74
6. Короткий зміст навчальної дисципліни	**Метою** викладання дисципліни є формування теоретичних знань та практичних навичок, необхідних для створення умов, що запобігають розголошенню, витоку і неправомірному оволодінню конфіденційною інформацією у технічних системах (ТС), а також запобігають протиправним діям щодо знищення, модифікації, копіювання і блокування інформації. **Завданням вивчення** дисципліни полягають у тому, щоб ознайомити слухачів із законодавчим, адміністративним, організаційним і інженерно- технічним рівнями забезпечення захисту ТС, особливостями криптографічного і стенографічного захисту, навчити їх реалізовувати практично правила політики безпеки підприємства.
7. Міждисциплінарні зв'язки:	Математичне модулювання, Програмні методи та засоби алгоритмізації процесів, Теорія та проектування технічних систем, Виробнича практика.

8. Форми і методи навчання:	Заняття проводяться у формі лекцій, семінарських занять. Лекції здійснюються з ключових проблем курсу. Методами навчання є: пояснювально-ілюстративний, репродуктивний, 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 робіт, які складають суму підсумкових балів здобувача вищої освіти: - робота на семінарських, практичних заняттях – 80 балів; - самостійна робота – 20 балів.
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. 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. СК8. Здатність розробляти і реалізовувати наукові та прикладні проєкти в галузі інформаційних технологій та дотичні до неї міждисциплінарні проєкти. СК9. Здатність здійснювати захист прав інтелектуальної власності, комерціалізацію результатів досліджень та інновацій 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 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 10. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців, зокрема до осіб, які навчаються
12. Рекомендована література:	1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. - Київ : Держ. торг.-екон. ун-т, 2023. 376 с. 2. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний - Львів : Видавець Марченко Т. В., 2023. 370 с. 3. Костюк Ю., Шестак Я. Транспортний рівень моделі ISO/OSI в комп'ютерних мережах. Міжнародний науково-практичний журнал "Товари і ринки". 2021. № 4. С. 49-58. 4. Костюк Ю.В. Стратегії захисту крайових пристроїв з використанням нейронних мереж Коско // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 26 квітня 2024 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. - К.: ВПЦ "Київський університет", 2024. с. 17-18. 5. Костюк Ю.В. Математичне моделювання захищених інформаційних систем // Інноваційний потенціал сучасної науки: зб. наук. праць IV Всеукраїнської наук.-практ. інтернет-конф., (18 травня 2023 року. Кам'янець-Подільський). - Кам'янець-

Подільський Заклад вищої освіти «Подільський державний університет», 2023. с. 171-174.
6. Технології захисту інформації: підручник / М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. - К.: ЦП «Компринт», 2021. 296 с.
7. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. - Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236с.
8. Костюк Ю.В., Кравченко Д.В. Методи захисту даних на підприємствах соціальної сфери. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1033-1047.
9. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. - Львів: «Новий Світ- 2000», 2020 . 678 с.
10. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. - Кропивницький: ЦНТУ, 2022. 967 с.