СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Аналіз інформації з відкритих джерел	
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 6 6 8 100
6. Короткий зміст навчальної дисципліни	Навчальна дисципліна «Аналіз інформації з відкритих джерел» є комплексом теоретичних положень та практичних завдань щодо нормативно-правового забезпечення, юридичних підстав застосування та пошуку інформації з відкритих джерел (OSINT) оперативними підрозділами поліції України під час виконання доручень слідчих органів, попередження, припинення, запобігання кримінальним правопорушенням та з метою їх своєчасного, ефективного виявлення, документування та забезпечення розслідування кримінальних проваджень. **Метою** дисципліни є вивчення навчальної дисципліни «Аналіз інформації з відкритих джерел» – навчання здобувачів вищої освіти діям зі збору інформації в мережі інтернет, формування професійних навичок, пов'язаних з професійною діяльністю в сфері аналізу інформації, виробленого в різних галузях наукових досліджень;

	загальних і приватних принципів здійснення аналітичної діяльності та вирішенні управлінських завдань; створення уявлення про цілі управління, формулюванні завдання інформаційно- аналітичної роботи.
7. Міждисциплінарні зв'язки	Аналіз інформації з відкритих джерел ґрунтується на застосуванні здобувачами вищої освіти знань із дисциплін: Логіка, Криміналістика, Кримінальний процес, Поліцейська діяльність, Інформаційні технології, Інформаційне забезпечення професійної діяльності, Оперативно-розшукова діяльність, Основи кримінального аналізу. Ці знання забезпечують всебічний розвиток аналітичних навичок здобувачів вищої освіти, сприяють формуванню здатності до критичного мислення, системного аналізу 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 злочинності.
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; -
	Загальні компетентності: **Загальні компетентності**: ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК4. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).. **Спеціальні компетентності:** СК1. Здатність інтегрувати знання та здійснювати системні дослідження, застосовувати методи математичного та інформаційного моделювання

11.Перелік програмних компетентностей та результатів навчання, визначених відповідною освітньою програмою	складних систем та процесів різної природи. СК2. Здатність проєктувати 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 проєктувати складні системи і процеси на основі методів та інструментальних засобів системного аналізу. СК6Здатність застосовувати теорію і методи Data Science для здійснення інтелектуального аналізу даних з метою виявлення нових властивостей та генерації нових знань про складні системи. 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 СК11. Здатність доносити до фахівців і нефахівців інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією щодо кримінального аналізу. СК12. Здатність аналізувати та інтерпретувати результати наукових досліджень, враховуючи використання міждисциплінарних та порівняльно- правових підходів. СК13. Здатність застосовувати методи кримінального аналізу при вирішенні задач оперативно-розшукової діяльності *Результати навчання:* Загальні компетентності: ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння. професійної діяльності. ЗК4. Здатність використовувати інформаційні та комунікаційні технології. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК7. Здатність до адаптації та дії в новій ситуації. ЗК8. Здатність приймати обґрунтовані рішення. ЗК9. Здатність працювати в команді. ЗК12. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. Спеціальні компетентності: СК1. Усвідомлення функцій держави у сфері правоохоронної діяльності, способів та механізмів реалізації цих функцій. СК3. Здатність до критичного мислення та системного аналізу правових явищ. СК4. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел. СК5. Здатність визначати придатні для юридичного аналізу факти, систематизувати одержані результати, встановлювати причинно-

наслідкові зв’язки, формулювати аргументовані висновки та рекомендації. СК8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних посягань. СК10. Здатність до аналізу та оцінки причин, умов та факторів, що впливають на вчинення кримінальних та адміністративних правопорушень. СК11. Здатність визначати особу правопорушника, аналізувати кількісні та якісні показники злочинності. СК16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури. СК17. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом. СК18. Здатність вживати заходів з метою запобігання, виявлення та припинення кримінальних та адміністративних правопорушень, усунення загроз життю та здоров’ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення правопорушення. СК19. Здатність здійснювати взаємодію з іншими суб’єктами сектору безпеки і оборони, у тому числі при усуненні потенційних та реальних загроз державному суверенітету та територіальній цілісності держави.

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 5. Використовувати міри оцінювання ризиків та застосовувати їх при аналізі багатофакторних ризиків в складних системах. 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. секретності та захисту інформації. РН 10. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців, зокрема до осіб, які навчаються РН 11. Вільно презентувати та обговорювати усно і письмово результати досліджень та інновацій, інші питання професійної діяльності державною та англійською мовами. РН12. Застосовувати методи розкриття невизначеностей в задачах кримінального аналізу, розкривати ситуаційні невизначеності та невизначеності в задачах взаємодії, протидії та конфлікту стратегій в умовах військового стану. РН 13. Розробляти та застосовувати методи,

	алгоритми та інструменти прогнозування кримінального аналізу при оцінки процесів різної природи в умовах військового стану. РН 14. Здатність застосовувати сучасні інформаційні технології при вирішення завдань кримінального аналізу в умовах військового стану

12. Рекомендована література:

Основна:

1. Жмур Н. В., Землянікін М. П. Історія становлення та сучасний стан технології пошуку інформації OSINT. Юридичний вісник № 3 (64) 2022. С. 95- 101. DOI: 10.18372/2307-9061.64.16895.
2. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. Південноукраїнський правничий часопис. 2016. № 2. С. 110-113.
3. Мовчан А.В. Поняття та сутність аналітичної розвідки як особливої форми інформаційно-аналітичної роботи в ОРД. Науковий вісник ЛьвДУВС. 2012. № 3. С. 443-450.
4. Щурат Т. Г. Напрями використання OSINT в оперативно-розшуковій діяльності. Роль та місце правоохоронних органів у розбудові демократичної правової держави: матеріали XIV міжнар. наук.-практ. інтернетконф., м. Одеса, 31 жовтня 2022 р. С.144-146.
5. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. Системи управління, навігації та зв'язку. 2016. Вип. 4. С. 81-84. URL: http://nbuv.gov.ua/UJRN/suntz_2016_4_22 (дата звернення 01.07.2025).
6. Кожушко О. О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. URL: http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/3217 (дата звернення 01.07.2025).
7. Розвідка на основі відкритих джерел. URL: https://www.wikidata.uk-ua.nina.az/OSINT.html (дата звернення 01.07.2025).
8. NATO Open Source Intelligence Handbook. URL: https://archive.org/details/NATOOSINTHandbookV1.2/mode/2u (дата звернення 01.07.2025).
9. Ржевська Н.Ф., Кожушко О.О. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE)URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/a964dfbb-a16d-4e8a-b621-9aa6cb277197/content (дата звернення 01.07.2025).