ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"

Навчально-науковий інститут права імені князя Володимира Великого

МАУП

Кафедра правоохоронної та антикорупційної діяльності

Затверджую:
Директор Навчально-наукового інституту права ім. князя Володимира Великого
_____
Микола ЗУБРИЦЬКИЙ
"28" 08 2025 р.

Схвалено на засіданні
Кафедри правоохоронної та антикорупційної діяльності
Протокол № 1 від 28.08.2025 р.
Завідувач кафедри _____
Володимир ЗАРОСИЛО

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ТА СПЕЦІАЛЬНИЙ ЗВ'ЯЗОК»

Спеціальності: 262 Правоохоронна діяльність

Освітнього рівня: **другий (магістерський) рівень**

Освітньої програми: Правоохоронна діяльність

Спеціалізація: _____

Розробник силабусу навчальної дисципліни:

Сергій Олексійович Лисенко - доктор юридичних наук, професор, професор кафедри правоохоронної та антикорупційної діяльності

(підпис)

Викладач:

Сергій Олексійович Лисенко - доктор юридичних наук, професор, професор кафедри правоохоронної та антикорупційної діяльності

(підпис)

Силабус розглянуто на засіданні кафедри правоохоронної та антикорупційної діяльності
Протокол № 1 від 28 серпня 2025 р.

Загальна інформація про навчальну дисципліну

Назва навчальної дисципліни	**Інформаційно-аналітичне забезпечення та спеціальний зв'язок**
Шифр та назва спеціальності	262 Правоохоронна діяльність
Рівень вищої освіти	другий (магістерський) рівень
Статус дисципліни	обов'язкова
Кількість кредитів і годин	**3 кредита/90 год** Лекції : **20** Семінарські заняття: **14** Самостійна робота студентів:**56**
Терміни вивчення дисципліни	І семестр
Мова викладання	українська
Вид підсумкового контролю	**залік**
Сторінка дисципліни на сайті	https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-2025/b/osnovi-operativno-rozshukovoi-diyalnosti.pdf

Загальна інформація про викладача. Контактна інформація.

Лисенко Сергій Олексійович	
Науковий ступінь	Доктор наук з державного управління, Доктор юридичних наук
Вчене звання	професор
Посада	Професор кафедри
Дисципліни, які викладає НПП	Інформаційно-аналітичне забезпечення та спеціальний зв'язок
Напрями наукових досліджень	Освіта, безпека освіти
Посилання на реєстри ідентифікаторів для науковців	ORCID: https://orcid.org/0000-0002-7050-5536 Google Scholar: https://scholar.google.com.ua/citations?hl=uk&user=SKvoZKIAAAAJ
Контактна інформація викладача:	
E-mail:	crimeconsult@ukr.net
Контактний тел.	+380507417375
Телефон кафедри	
Портфоліо викладача на сайті кафедри/Інституту/Академії	https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-2025/b/teoriya-bezpeki-organizacij.pdf

1.1 Анотація курсу.

Курс «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» є навчальною дисципліною, спрямованою на формування у здобувачів вищої освіти цілісного уявлення про роль інформаційно-аналітичної діяльності та систем спеціального телекомунікаційного зв'язку у функціонуванні суб'єктів сектору безпеки і оборони. Дисципліна розкриває логіку перетворення масивів даних на структурований аналітичний продукт, що використовується для підготовки управлінських, оперативних і стратегічних рішень. Курс охоплює питання організації захищених інформаційних потоків, міжвідомчої взаємодії, роботи з державними базами даних, застосування сучасних інформаційно-аналітичних систем та дотримання суворих режимів захисту інформації.

1.2 Предмет вивчення курсу

Предметом вивчення навчальної дисципліни є теоретичні, організаційні та прикладні засади інформаційно-аналітичного забезпечення та функціонування систем спеціального зв'язку в секторі безпеки і оборони. До предмета належать принципи збирання, перевірки, обробки, аналізу, збереження, захисту та безпечного передавання інформації, що використовується для підтримки управлінських, стратегічних і оперативних рішень. До предмета курсу також входять моделі інформаційно-аналітичного циклу, види безпекового та оперативного аналізу, методи виявлення структурних закономірностей і прихованих зв'язків. Окрему увагу приділено архітектурі автоматизованих інформаційних систем, аналітичних платформ і телекомунікаційних мереж спеціального призначення, а також правовим, організаційним, інженерно-технічним і криптографічним механізмам захисту службової, таємної та іншої чутливої інформації під час її обробки й обміну закритими каналами зв'язку. Опрацювання дисципліни орієнтоване на розвиток умінь працювати з інформацією як стратегічним ресурсом, критично оцінювати джерела, формувати обґрунтовані аналітичні висновки, ідентифікувати ризики компрометації чи деструктивного впливу на дані. Здобувачі набувають компетенцій, необхідних для забезпечення безперебійної інформаційно-аналітичної підтримки та організації надійного спеціального зв'язку в системі національної безпеки.

1.3 Метою викладання навчальної дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» є формування у здобувачів вищої освіти комплексних знань щодо сутності, архітектури та функцій інформаційно-аналітичної діяльності і систем спеціального телекомунікаційного зв'язку в секторі безпеки і оборони держави. Мета передбачає набуття практичних умінь застосовувати сучасні аналітичні підходи для ідентифікації загроз, оцінювання безпекових ризиків, підготовки матеріалів стратегічного планування та підтримки управлінських і оперативних рішень. Вивчення дисципліни має забезпечити глибоке розуміння того, що ефективна діяльність органів державної влади ґрунтується на випереджальному використанні інформаційних масивів, науково обґрунтованих методів аналізу, захищеного міжвідомчого обміну даними та надійних засобів технічного і криптографічного захисту. Крім того, курс спрямований на формування у здобувачів здатності діяти відповідно до логіки інформаційно-аналітичного циклу, синтезувати відомості з розрізнених джерел, розробляти аналітичні довідки, зведення, профілі ризику та ситуаційні звіти. Невіддільною складовою мети є опанування механізмів гарантування конфіденційності, цілісності й доступності інформації під час її оброблення та передавання закритими каналами урядового і спеціального зв'язку в процесі здійснення професійної діяльності.

1.4 Завдання дисципліни є засвоєння базових понять, категорій і принципів інформаційно-аналітичного забезпечення та функціонування систем спеціального телекомунікаційного зв'язку в секторі безпеки і оборони; формування системного розуміння інформації як стратегічного ресурсу, що використовується для оцінювання оперативної обстановки, ідентифікації загроз і підтримки управлінських рішень; опанування логіки інформаційно-аналітичного циклу та основ безпекового, стратегічного й оперативного аналізу; розвиток умінь працювати з різноманітними джерелами даних, зокрема відкритими, відомчими та технічними, та здійснювати їх критичну верифікацію й комплексну аналітичну інтерпретацію; формування здатності розробляти основні види аналітичних документів у діяльності суб'єктів сектору безпеки із дотриманням суворих вимог щодо структури, логіки, обґрунтованості та режимів доступу; набуття знань щодо архітектури та функціонування автоматизованих інформаційно-аналітичних систем, інтегрованих баз даних, а також ролі передових цифрових технологій і систем штучного інтелекту в аналітичній діяльності; опанування організаційно-технічних засад спеціального і урядового зв'язку, технічного та криптографічного захисту інформації, дотримання режиму секретності та принципу службової необхідності як фундаментальних елементів безпечного обміну даними; формування умінь застосовувати аналітичний інструментарій для прогнозування безпекових загроз, забезпечення захищеної міжвідомчої взаємодії та безперебійного інформаційного супроводження діяльності органів державної влади та управління.

1.5 Пререквізити і постреквізити навчальної дисципліни:

Пререквізити:

Основи оперативно-розшукової діяльності. Навчальна дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» спирається на результати опанування курсу «Основи оперативно-розшукової діяльності», оскільки потребує сформованих умінь працювати з інформацією про загрози, оцінювати її достовірність, здійснювати первинну верифікацію та формувати аналітичні висновки для управлінських рішень. Логіка ОРД щодо документування обставин, процедурної дисципліни та недопущення недоброчесних практик підсилює здатність будувати систему безпеки організації на основі контрольованих процесів, де ризики і вразливості фіксуються, аналізуються і перетворюються на план заходів. Додатково засвоєння підходів до розмежування оперативної інформації та доказів сприяє коректному управлінню інцидентами в організації, коли якість матеріалів і підстави рішень можуть бути предметом перевірки, а відповідальність і законність дій мають ключове значення.

Постреквізити:

1.6 Програмні компетентності (загальні (ЗК); спеціальні (СК)):

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» формує здатність застосовувати знання у практичних ситуаціях через опанування методів збору, перевірки, оброблення, аналізу та узагальнення інформації, необхідної для прийняття управлінських і оперативних рішень. Засвоєння змісту

аналітичної діяльності, джерел інформації, механізмів її верифікації, способів побудови аналітичних продуктів і моделей оцінювання ризиків дає змогу здобувачам використовувати набуті знання у реальних професійних умовах, пов'язаних із забезпеченням безпеки, правопорядку та правоохоронної діяльності.

ЗК3. Здатність спілкуватися іноземною мовою.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» сприяє розвитку здатності спілкуватися іноземною мовою через опрацювання сучасної професійної термінології у сфері інформаційної безпеки, аналітики, кримінального аналізу, кіберзахисту, спеціального зв'язку та OSINT. Ознайомлення з англомовними поняттями, міжнародними підходами, стандартами та професійними моделями інформаційно-аналітичної діяльності розширює фаховий словник здобувачів і створює підґрунтя для використання іноземної мови у професійному та науковому середовищі.

СК4. Спроможність організовувати і керувати діяльністю підрозділів, створених для виконання завдань у сфері правоохоронної діяльності.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» формує спроможність організовувати і керувати діяльністю підрозділів правоохоронного спрямування завдяки засвоєнню принципів інформаційного забезпечення управління, побудови аналітичного циклу, оцінювання ризиків, формування аналітичних документів та координації роботи з різними джерелами інформації. Вивчення інформаційно-аналітичних систем, механізмів оброблення даних, звітності, моніторингу й контролю якості інформації дає змогу здобувачам усвідомити роль аналітичного супроводу в управлінні підрозділом у різних умовах службової діяльності.

СК10. Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час рішення професійних завдань.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» безпосередньо формує здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час вирішення професійних завдань. У межах курсу здобувачі опановують особливості функціонування інформаційно-аналітичних систем, баз даних, цифрових платформ, технологій автоматизованого аналізу інформації, сучасних засобів захисту інформації, а також інструментів, що використовуються для підготовки аналітичних продуктів і підтримки управлінських рішень у сфері безпеки та правоохоронної діяльності.

СК12. Здатність до використання спеціальних засобів, інформаційно-пошукових систем, баз даних для здійснення правоохоронної та оперативно-розшукової діяльності.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» забезпечує формування здатності до використання спеціальних засобів, інформаційно-пошукових систем і баз даних у правоохоронній та оперативно-розшуковій діяльності. Засвоєння змісту джерел інформації, відомчих інформаційних ресурсів, відкритих джерел, OSINT, аналітичних платформ, спеціального зв'язку та захищених інформаційних систем дозволяє здобувачам розуміти порядок, значення та межі застосування відповідних інструментів у професійній діяльності.

1.7 Очікувані результати навчання (ПРН)

РН6. Спілкуватися англійською мовою усно і письмово з професійних та наукових питань у сфері правоохоронної діяльності.

Опанування дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» сприяє досягненню результату навчання, пов'язаного зі спілкуванням англійською мовою з професійних та наукових питань, через засвоєння фахової англомовної термінології у сферах аналітики, безпеки, кіберзахисту, кримінального аналізу, інформаційних систем і спеціального зв'язку. Робота з поняттями intelligence-led policing, risk-based approach, evidence-based approach, OSINT, SOC, SIEM, DLP, Zero Trust та іншими категоріями створює основу для професійної комунікації англійською мовою.

РН7. Оцінювати та забезпечувати якість виконуваних робіт у процесі управління правоохоронним підрозділом в різних умовах обстановки, а також розробляти відповідні аналітичні та інформаційні матеріали, робити усні та письмові звіти та доповіді.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» формує результат навчання, пов'язаний з оцінюванням і забезпеченням якості виконуваних робіт у процесі управління правоохоронним підрозділом, а також із підготовкою аналітичних та інформаційних матеріалів. Опрацювання тем, присвячених аналітичним документам, методам верифікації інформації, розробленню профілів ризику, ситуаційних звітів, аналітичних довідок і прогнозів, забезпечує здобувачам уміння готувати усні та письмові звіти, доповіді й інформаційні матеріали в межах професійної діяльності.

РН9. Використовувати у професійній діяльності сучасні інформаційні технології, бази даних, стандартне і спеціалізоване програмне забезпечення.

Опанування дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» забезпечує здатність використовувати у професійній діяльності сучасні інформаційні технології, бази даних, стандартне і спеціалізоване програмне забезпечення. Вивчення інформаційно-аналітичних систем, автоматизованих баз даних, аналітичних платформ, цифрових інструментів оброблення інформації та захищених систем зв'язку дозволяє здобувачам засвоїти можливості сучасного технологічного середовища як основи підтримки правоохоронної та безпекової діяльності.

РН10. Користуватись відповідними системами зв'язку у питаннях формування та реалізації державної правоохоронної політики у напрямках кіберзахисту критичної інфраструктури, державних інформаційних ресурсів, захисту інформації та телекомунікаційних систем.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» формує здатність користуватися відповідними системами зв'язку у питаннях формування та реалізації державної правоохоронної політики в напрямах кіберзахисту критичної інфраструктури, державних інформаційних ресурсів, захисту інформації та телекомунікаційних систем. Вивчення основ спеціального зв'язку, технічного і криптографічного захисту інформації, режиму секретності,

кіберзагроз, інсайдерських ризиків та захисту службових комунікацій забезпечує розуміння місця систем зв'язку у сучасній безпековій політиці.

РН13. Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати отриману інформацію.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» прямо орієнтована на формування вміння відшуковувати необхідну інформацію у спеціальній літературі, базах даних та інших джерелах, а також аналізувати й об'єктивно оцінювати її. Опрацювання тем, пов'язаних із класифікацією джерел інформації, OSINT, верифікацією, аналітичним опрацюванням даних, визначенням достовірності, релевантності та актуальності інформації, створює основу для професійної інформаційно-пошукової та аналітичної діяльності.

РН16. Використовувати сучасні механізми, методи і засоби системного аналізу, імітаційного моделювання, збирання, зберігання та оброблення інформації для аналізу варіантів управлінських рішень при реалізації професійних завдань.

Опанування дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» забезпечує здатність використовувати сучасні механізми, методи і засоби системного аналізу, моделювання, збирання, зберігання та оброблення інформації для аналізу варіантів управлінських рішень. Засвоєння змісту інформаційного циклу, безпекового, кримінального та оперативного аналізу, профілювання ризиків, побудови аналітичних моделей, використання інформаційно-аналітичних систем і цифрових платформ формує у здобувачів уміння працювати з інформацією як із ресурсом прийняття рішень.

РН17. Розуміти принципи забезпечення суспільної безпеки та правопорядку, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальних засобів, засобів фізичної сили), технологій захисту даних, методів обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, здійснення правоохоронної діяльності.

Дисципліна «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» формує розуміння принципів забезпечення суспільної безпеки та правопорядку через вивчення інформаційно-аналітичної складової правоохоронної діяльності, технологій захисту даних, методів збирання, оброблення, накопичення й оцінювання інформації, а також ролі аналітичної роботи у прийнятті рішень. Опанування змісту спеціального зв'язку, технічного та криптографічного захисту інформації, режиму секретності, роботи з базами даних, аналітичними системами та джерелами інформації дозволяє усвідомити місце інформаційного компонента у сучасному забезпеченні безпеки і правопорядку.

2. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ОСНОВИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ У СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ

Тема 1. Теоретичні основи інформаційно-аналітичного забезпечення систем сектору безпеки і оборони

Тема формує базове розуміння сутності інформаційного забезпечення як організованої системи збирання, перевірки, збереження, оброблення, аналізу та доведення інформації до суб'єкта прийняття рішень. Розкривається роль аналітики як центрального елемента сучасних ризик-орієнтованих, розвідувально-керованих та науково обґрунтованих підходів у діяльності органів державної влади. Окрема увага приділяється інформації як стратегічному ресурсу безпекової системи та інформаційно-аналітичному циклу як логіці перетворення даних на аналітичний продукт для управлінських і оперативних рішень.

Тема 2. Джерела інформації у діяльності суб'єктів сектору безпеки і оборони

Тема присвячена характеристиці оперативних, процесуальних, відкритих і технічних джерел інформації, їхнім пізнавальним можливостям, правовим режимам, перевагам, обмеженням та ризикам використання. Розглядається розвідка на основі відкритих джерел як окремий інструмент сучасної аналітики у сфері безпеки, а також значення державних баз даних і міжвідомчого інформаційного обміну для формування цілісної картини загроз та підтримки координації між відомствами.

Тема 3. Основи безпекового, кримінального та оперативного аналізу

Тема розкриває аналіз як ключовий процес перетворення інформації на знання, необхідні для підтримки управлінських та оперативних рішень. Вивчаються поняття безпекового та кримінального аналізу, їхнє співвідношення і функціональне призначення, а також особливості тактичного, оперативного і стратегічного аналізу залежно від часового горизонту, змісту запиту та виду аналітичного продукту. Окремо розглядаються методи виявлення зв'язків, структур і закономірностей, включно з аналізом злочинних мереж, серійності та просторово-часових моделей.

Тема 4. Інформаційно-аналітичні системи суб'єктів сектору безпеки і оборони

Тема формує цілісне уявлення про автоматизовані інформаційні системи, аналітичні платформи та інтегровані інформаційні середовища, які забезпечують збирання, узгодження, обмін і використання даних у контурі національної безпеки. Розкривається архітектура інформаційно-аналітичних систем, життєвий цикл даних, роль стандартизації та взаємосумісності, а також значення штучного інтелекту в аналітиці, його прикладний потенціал і пов'язані з ним ризики упередженості, непрозорості, деградації алгоритмічних моделей та витоку даних.

Тема 5. Аналітичні документи в діяльності суб'єктів сектору безпеки і оборони

Тема присвячена видам аналітичних документів, які використовуються у діяльності органів сектору безпеки, зокрема аналітичній довідці, зведенню, профілю особи, профілю ризику та ситуаційному звіту. Розглядаються вимоги до їхньої структури, логіки, доказовості, рівнів впевненості, порядку подання ключових суджень та рекомендацій, а також питання безпечного поширення аналітичних продуктів з урахуванням категорії доступу та кола адресатів.

ЗМІСТОВИЙ МОДУЛЬ 2. СПЕЦІАЛЬНИЙ ЗВ'ЯЗОК, ЗАХИСТ ІНФОРМАЦІЇ ТА ІНТЕГРОВАНЕ АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАЦІЙ

Тема 6. Основи спеціального зв'язку в секторі безпеки і оборони

Тема розкриває спеціальний зв'язок як окремий клас службових і державних комунікацій, що забезпечують виконання управлінських, оперативних та

координаційних завдань у безпековій сфері. Вивчаються види спеціального зв’язку, підходи до побудови захищених каналів передавання інформації, поєднання технічних і організаційних заходів захисту, а також роль Державної служби спеціального зв’язку та захисту інформації України у функціонуванні національної системи захищених комунікацій.

Тема 7. Технічний та криптографічний захист інформації

Тема формує розуміння основних загроз перехоплення та компрометації інформації, сутності криптографічного захисту, його можливостей і меж, а також системи технічного захисту інформації як комплексу інженерних, технічних та організаційних заходів. Розглядаються основи симетричного та асиметричного шифрування, криптографічного гешування, електронного підпису, керування ключами, а також особливості захисту мовної, текстової та цифрової інформації в каналах зв’язку.

Тема 8. Режим секретності та захист службової інформації

Тема присвячена правовим режимам обігу інформації з обмеженим доступом, зокрема службовій, конфіденційній та таємній інформації, а також практиці організації режиму секретності в діяльності підрозділів. Розглядаються правила маркування, обліку, зберігання, використання, копіювання, передавання, архівування та знищення документів і носіїв, а також принцип службової необхідності як центральна логіка мінімізації ризику витоку інформації у секторі безпеки і оборони.

Тема 9. Кіберзагрози та інсайдерські ризики в органах сектору безпеки і оборони

Тема орієнтована на вивчення сучасних кіберзагроз для інформаційних систем, каналів зв’язку та службових комунікацій, а також інсайдерських ризиків як окремої категорії загроз, пов’язаних із діями або бездіяльністю персоналу. У центрі уваги перебувають типові моделі компрометації ключів і пристроїв, несанкціоноване передавання даних, порушення режиму доступу, використання незахищених каналів, а також базові організаційні й технічні заходи контролю для мінімізації таких ризиків. Назва і зміст цієї теми логічно випливають із загальної структури курсу, де загрози спеціальному зв’язку безпосередньо пов’язані з питаннями захисту інформації.

Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій суб’єктів сектору безпеки і оборони

Тема узагальнює курс і формує прикладне розуміння того, як джерела інформації, аналітичні процедури, управлінські механізми та міжвідомча взаємодія поєднуються в єдиний контур підтримки оперативно-розшукових заходів і спеціальних операцій. Розглядаються питання постановки завдань і координації, підготовки спільних аналітичних продуктів, узгодження режимів доступу, організації інформаційної підтримки операцій, а також використання аналітики для прогнозування загроз через індикатори, сценарії, моделювання небезпек та матриці ризиків.

3. Технічне й програмне забезпечення/обладнання

В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення аудиторних занять з

елементам презентацій Microsoft PowerPoint. Вивчення окремих тем і виконання практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

4. Форми і методи навчання

Основними формами занять із навчальної дисципліни «Вступ до спеціальності «Національна безпека» є практичні заняття та самостійна робота здобувачів вищої освіти.

При проведенні практичних занять передбачено поєднання таких форм і методів навчання, як-то: робота у малих групах, рольові ігри, дискусія, публічні виступи, групові проєкти та кейс-завдання.

Здобувачі освіти опрацьовують інформацію з наукових, навчальних та лекційних джерел, в тому числі за допомогою всесвітньої мережі Інтернет і бібліотек, під час занять виконують усні та письмові завдання, виступають із доповідями та презентаціями, що можуть бути підготовленими як у групі, так і індивідуально.

Програмою курсу також передбачено **індивідуальні завдання.**

5. Система оцінювання та вимоги (критерії оцінювання результатів навчання здобувачів освіти та розподіл балів, які вони отримують)

Оцінювання знань здійснюється відповідно до:

1. Положення про організацію освітнього процесу в ПрАТ «ВНЗ «МАУП» https://surl.li/bpxlbj
2. Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП» http://surl.li/fkfyye

1-й семестр.

№ тем	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Заг.сума балів**
Робота на сем.занятті	2	2	2	2	1	1	1	1	1	1	14
Сам.робота	3	3	3	3	3	3	3	3	2	2	20
Всього	**5**	**5**	**5**	**5**	**4**	**4**	**4**	**4**	**3**	**3**	**34**

Підсумкове оцінювання	Сума балів за семінари	Сума балів за самостійні роботи	Модульна контрольна робота	Сума балів за екзамен	Загальна сума
	35	10	15	40	100

5.1 Відвідування та робота на семінарських (практичних) заняттях та критерії їх оцінювання

Під час вивчення курсу виконується *робота на семінарських (практичних) заняттях по кожній з тем***.**

Критерії оцінювання:

правильність відповідей та розрахунків – від 0 до 3 балів;
відповідність оформлення практичних робіт вимогам – 1 бал.
(враховуються лише за умови нарахування балів за правильність відповідей).

Робота на семінарському занятті оцінюється у **4 бали**.

Максимальна кількість балів за семінарські (практичні) заняття по курсу – **36 балів.**

Зміст практичних занять

№ з/п	Назва теми
1	**Тема 1. Теоретичні основи інформаційно-аналітичного забезпечення суб'єктів сектору безпеки і оборони** Завдання: Визначити сутність інформаційного забезпечення як системи збирання, перевірки, збереження, оброблення, аналізу та доведення інформації до суб'єкта прийняття рішень. Охарактеризувати значення ризик-орієнтованих, розвідувально-керованих та науково обґрунтованих підходів у діяльності органів сектору безпеки і оборони. Скласти схему інформаційного циклу: дані → перевірка → оброблення → аналіз → аналітичний продукт → управлінське або оперативне рішення. Очікуваний результат: Вміння пояснювати сутність інформаційно-аналітичного забезпечення як базової функції сучасної безпекової діяльності. Здатність розкривати роль аналітики у трансформації даних в управлінське знання. Дискусія: Чому в сучасних умовах інформація розглядається як стратегічний ресурс безпекової системи? Чи може управлінське рішення бути якісним без належно побудованого інформаційно-аналітичного циклу? **Тема 2. Джерела інформації у діяльності суб'єктів сектору безпеки і оборони** Завдання: Визначити основні види джерел інформації: оперативні, процесуальні, відкриті, технічні та відомчі. Порівняти їхні пізнавальні можливості, правові режими, переваги, обмеження та ризики використання. Проаналізувати значення розвідки на основі відкритих джерел, державних баз даних і міжвідомчого інформаційного обміну для формування цілісної картини загроз. Очікуваний результат: Вміння класифікувати джерела інформації та оцінювати їхню придатність для виконання конкретних безпекових завдань.

	Здатність визначати межі допустимого й ефективного використання різних джерел у діяльності сектору безпеки і оборони. Дискусія: Чи можна вважати відкриті джерела повноцінною основою для аналітичних висновків у сфері безпеки? Що є важливішим для органу безпеки: обсяг зібраної інформації чи її якість і перевіреність? **Тема 3. Основи безпекового, кримінального та оперативного аналізу** Завдання: Визначити поняття безпекового, кримінального та оперативного аналізу, розкрити їхнє співвідношення і функціональне призначення. Охарактеризувати тактичний, оперативний і стратегічний аналіз залежно від горизонту планування та виду аналітичного продукту. Розглянути методи виявлення зв'язків, структур і закономірностей, включно з аналізом злочинних мереж, серійності та просторово-часових моделей. Очікуваний результат: Вміння розрізняти види аналізу та обирати їх залежно від характеру безпекового запиту. Здатність пояснювати, як аналітичні методи допомагають виявляти приховані зв'язки та загрози. Дискусія: Чи є стратегічний аналіз більш значущим для системи безпеки, ніж тактичний? Наскільки аналітичний висновок залежить від якості вихідної інформації? **Тема 4. Інформаційно-аналітичні системи суб'єктів сектору безпеки і оборони** Завдання: Охарактеризувати автоматизовані інформаційні системи, аналітичні платформи та інтегровані інформаційні середовища у безпековому контурі. Розкрити архітектуру інформаційно-аналітичних систем, життєвий цикл даних, значення стандартизації та взаємосумісності. Проаналізувати потенціал штучного інтелекту в аналітиці та пов'язані з ним ризики упередженості, непрозорості, деградації алгоритмічних моделей і витоку даних. Очікуваний результат: Вміння пояснювати місце інформаційно-аналітичних систем у діяльності суб'єктів сектору безпеки і оборони. Здатність оцінювати сильні сторони та ризики цифровізації аналітичних процесів. Дискусія: Чи підвищує автоматизація якість аналітики, чи створює нові вразливості? Де проходить межа між технологічною ефективністю та потребою людського контролю в аналітичних системах? **Тема 5. Аналітичні документи в діяльності суб'єктів сектору безпеки і оборони** Завдання: Визначити основні види аналітичних документів: аналітична довідка, зведення, профіль особи, профіль ризику, ситуаційний звіт. Розкрити вимоги до структури, логіки, доказовості, рівнів впевненості та

	формулювання рекомендацій. Проаналізувати порядок безпечного поширення аналітичних продуктів з урахуванням категорій доступу і кола адресатів. Очікуваний результат: Вміння правильно розрізняти аналітичні документи за їхнім функціональним призначенням. Здатність формувати вимоги до змісту та якості аналітичного продукту. Дискусія: Чи повинен аналітичний документ лише описувати ситуацію, чи також пропонувати рішення? Як співвідноситься стислий формат аналітичного документа з вимогою повноти й доказовості? **Тема 6. Основи спеціального зв'язку в секторі безпеки і оборони** Завдання: Визначити сутність спеціального зв'язку як окремого класу службових і державних комунікацій. Охарактеризувати види спеціального зв'язку та підходи до побудови захищених каналів передавання інформації. Розкрити роль Державної служби спеціального зв'язку та захисту інформації України у функціонуванні національної системи захищених комунікацій. Очікуваний результат: Вміння пояснювати значення спеціального зв'язку для управлінських, оперативних і координаційних завдань у безпековій сфері. Здатність розуміти взаємозв'язок технічних і організаційних заходів захисту комунікацій. Дискусія: Чи може сучасна система безпеки ефективно діяти без спеціального зв'язку? Наскільки організаційна дисципліна впливає на ефективність навіть технічно захищених каналів зв'язку? **Тема 7. Технічний та криптографічний захист інформації** Завдання: Охарактеризувати основні загрози перехоплення та компрометації інформації. Визначити сутність криптографічного захисту, його можливості й межі у забезпеченні інформаційної безпеки. Розкрити основи симетричного та асиметричного шифрування, криптографічного гешування, електронного підпису, керування ключами та особливості захисту різних видів інформації в каналах зв'язку. Очікуваний результат: Вміння пояснювати базові механізми криптографічного й технічного захисту інформації. Здатність оцінювати роль інженерних, технічних та організаційних заходів у комплексному захисті інформації. Дискусія: Чи може криптографія сама по собі гарантувати повну безпеку інформації? Який елемент є вразливішим у системі захисту: технологія чи людина, яка її використовує? **Тема 8. Режим секретності та захист службової інформації** Завдання:

	Визначити правові режими обігу інформації з обмеженим доступом: службова, конфіденційна, таємна інформація. Розкрити правила маркування, обліку, зберігання, використання, копіювання, передавання, архівування та знищення документів і носіїв. Пояснити значення принципу службової необхідності як базової логіки мінімізації ризику витоку інформації. Очікуваний результат: Вміння орієнтуватися у правових і організаційних засадах режиму секретності. Здатність пояснювати практичне значення процедурного контролю доступу до службової інформації. Дискусія: Чи завжди обмеження доступу до інформації підвищує рівень безпеки? Де межа між захистом інформації та надмірною закритістю діяльності органу? **Тема 9. Кіберзагрози та інсайдерські ризики в органах сектору безпеки і оборони** Завдання: Визначити сучасні кіберзагрози для інформаційних систем, каналів зв'язку та службових комунікацій органів сектору безпеки і оборони. Проаналізувати інсайдерські ризики як окрему категорію загроз, пов'язаних із діями або бездіяльністю персоналу. Охарактеризувати типові моделі компрометації ключів і пристроїв, несанкціоноване передавання даних, порушення режиму доступу, використання незахищених каналів та базові заходи контролю для мінімізації таких ризиків. Очікуваний результат: Вміння розрізняти зовнішні кіберзагрози та внутрішні інсайдерські ризики. Здатність пояснювати значення організаційних і технічних заходів протидії компрометації інформаційного середовища. Дискусія: Що є небезпечнішим для суб'єкта сектору безпеки і оборони: зовнішня кібератака чи внутрішнє порушення режиму? Чи можливо повністю усунути інсайдерські ризики лише за допомогою технічних засобів? **Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій суб'єктів сектору безпеки і оборони** Завдання: Розкрити, як джерела інформації, аналітичні процедури, управлінські механізми та міжвідомча взаємодія поєднуються в єдиний контур підтримки оперативно-розшукових заходів і спеціальних операцій. Охарактеризувати питання постановки завдань, координації, підготовки спільних аналітичних продуктів та узгодження режимів доступу. Розглянути використання аналітики для прогнозування загроз через індикатори, сценарії, моделі ризиків та матриці ризиків. Очікуваний результат: Вміння пояснювати логіку інтегрованого інформаційно-аналітичного забезпечення операцій. Здатність показувати значення міжвідомчої взаємодії та прогнозної аналітики у підтримці безпекових рішень. Дискусія:

	Чи можлива ефективна операція без єдиного інформаційно-аналітичного контуру? Що є критичнішим для успіху операції: швидкість отримання інформації чи якість її аналітичного опрацювання?
Усього за навчальною дисципліною	

5.2 Завдання для самостійної роботи та критерії її оцінювання.

Під час вивчення курсу виконуються завдання для самостійних робіт до 19 тем.

Критерії оцінювання:

Змістовність, відповідність темі та вимогам оформлення – 1 бал.
Максимальна кількість балів за одиницю самостійної роботи – 1 бал.
Максимальна кількість балів за самостійну роботу по курсу – 19 балів.

Зміст завдань для самостійної роботи здобувача (СРЗ)

№ п/п	Зміст самостійної роботи здобувача вищої освіти	Форми контролю СРЗ
1	**Тема 1. Теоретичні основи інформаційно-аналітичного забезпечення суб'єктів сектору безпеки і оборони** Завдання для самостійної роботи: Проаналізувати еволюцію інформаційно-аналітичного забезпечення у секторі безпеки і оборони України. Підготувати огляд сучасних науково обґрунтованих та розвідувально-керованих підходів до прийняття управлінських рішень. Скласти структурну схему інформаційно-аналітичного циклу із зазначенням ролі кожного етапу.	Презентація результатів
2	**Тема 2. Джерела інформації у діяльності суб'єктів сектору безпеки і оборони** Завдання для самостійної роботи: Здійснити порівняльний аналіз відкритих, відомчих та технічних джерел інформації. Підготувати короткий аналітичний звіт на основі методів розвідки за відкритими джерелами щодо обраної безпекової проблеми, аргументовано оцінивши достовірність та надійність використаних джерел.	Презентація результатів
3	**Тема 3. Основи безпекового, кримінального та оперативного аналізу** Завдання для самостійної роботи: Проаналізувати відмінності між стратегічним, оперативним та тактичним аналізом. На основі навчального сценарію	Презентація результатів

	побудувати схему зв'язків (просторово-часову або структурну) для виявлення закономірностей у діяльності умовного злочинного угруповання або джерела загрози.	
4	**Тема 4. Інформаційно-аналітичні системи суб'єктів сектору безпеки і оборони** Завдання для самостійної роботи: Дослідити архітектуру та функціональні можливості однієї з сучасних державних інформаційно-аналітичних систем. Підготувати есе щодо перспектив та ризиків впровадження алгоритмів штучного інтелекту в аналітичну діяльність органів державної влади.	Презентація результатів
5	**Тема 5. Аналітичні документи в діяльності суб'єктів сектору безпеки і оборони** Завдання для самостійної роботи: Розробити проєкт аналітичного документа (профіль ризику або ситуаційний звіт) за заданою викладачем фабулою. Забезпечити суворе дотримання вимог щодо структури, логіки викладу, аргументованості висновків та формулювання рекомендацій для прийняття управлінського рішення.	Презентація результатів
6	**Тема 6. Основи спеціального зв'язку в секторі безпеки і оборони** Завдання для самостійної роботи: Проаналізувати нормативно-правову базу функціонування державної системи урядового та спеціального зв'язку в Україні. Підготувати доповідь про архітектуру захищених комунікацій та роль організаційно-технічних заходів у забезпеченні їхньої безперебійності під час кризових ситуацій.	Презентація результатів
7	**Тема 7. Технічний та криптографічний захист інформації** Завдання для самостійної роботи: Дослідити базові принципи криптографічного захисту інформації (симетричне та асиметричне шифрування, електронний підпис). Скласти порівняльну таблицю загроз перехоплення даних у відкритих та захищених каналах зв'язку із зазначенням конкретних методів їх нейтралізації.	Презентація результатів
8	**Тема 8. Режим секретності та захист службової інформації** Завдання для самостійної роботи: Розробити алгоритм дій посадової особи щодо оброблення, зберігання та передавання документа, що містить службову інформацію. Пояснити на конкретному прикладі практичне застосування принципу службової необхідності для запобігання витоку даних.	Презентація результатів
9	**Тема 9. Кіберзагрози та інсайдерські ризики в органах**	Презентація

	сектору безпеки і оборони Завдання для самостійної роботи: Проаналізувати відомі інциденти (на основі відкритих джерел) витоку чутливої інформації через інсайдерську діяльність або кібератаки на державні ресурси. Сформувати перелік першочергових організаційних та технічних заходів контролю для мінімізації подібних ризиків у підрозділі.	результатів
10	**Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій суб'єктів сектору безпеки і оборони** Завдання для самостійної роботи: Розробити концептуальну схему інтегрованого інформаційно-аналітичного супроводження умовної спеціальної операції. Описати механізми постановки завдань, міжвідомчої координації обміну даними та використання прогностичного моделювання для мінімізації ризиків під час операції.	Презентація результатів

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок».

Тему реферату здобувач визначає за першою буквою за списком групи.

В окремих випадках здобувач може самостійно запропонувати та розробити тему реферату, попередньо обговоривши її з викладачем.

Структура, зміст і тема рефератів визначаються програмою курсу, що зумовлює таку послідовність роботи:

вибір теми;

розробка плану;

ознайомлення з рекомендованою літературою;

написання та оформлення роботи.

При написанні реферату та його оформленні варто керуватися такими критеріями:

обґрунтування вибраної теми;

опрацювання відповідної літератури;

наявність авторського розділу;

наявність списку використаних джерел.

Цитати та статистичні матеріали слід обов'язково супроводжувати посиланнями на джерела інформації, які мають бути відображені у списку використаних джерел. Посилання на інформаційні джерела необхідно подавати по тексту у квадратних дужках, наприклад [15, с. 74], 15 – це порядковий номер джерела у списку літератури, а 74 – сторінка із вказаного джерела.

Реферат має складатися із вступу (актуальність теми, предмет, об'єкт, мета, завдання), основної частини (визначення проблеми та послідовне її розкриття), висновків та списку використаних літературних джерел.

Загальний обсяг реферату – до 20 машинописних сторінки формату А4 з 14 шрифтом та інтервалом 1,5, із полями (верхнє/нижнє – 2 см, ліве – 3 см, праве –

1 см.).

Слід мати на увазі, що головною вимогою до реферату є розкриття суті питань, а не кількість сторінок.

Теми рефератів

1 Еволюція інформаційно-аналітичного забезпечення в секторі безпеки і оборони України.

2 Інформація як стратегічний ресурс у процесі прийняття управлінських рішень.

3 Теоретичні засади функціонування інформаційно-аналітичного циклу в безпековій діяльності.

4 Ризик-орієнтований підхід в організації діяльності органів державної влади.

5 Науково обґрунтовані моделі управління та аналізу у сфері національної безпеки.

6 Розвідка за відкритими джерелами: можливості, обмеження та правові засади використання.

7 Роль державних реєстрів і відомчих баз даних у формуванні єдиного інформаційного простору.

8 Міжвідомчий інформаційний обмін: організаційно-правові проблеми та шляхи їх вирішення.

9 Специфіка використання технічних джерел інформації у діяльності суб’єктів сектору безпеки.

10 Оцінювання достовірності та надійності джерел інформації в аналітичній роботі.

11 Безпековий аналіз як інструмент прогнозування загроз національній безпеці.

12 Оперативний аналіз у системі протидії транснаціональній злочинності та тероризму.

13 Стратегічний аналіз: методологія підготовки довгострокових безпекових прогнозів.

14 Процес виявлення прихованих закономірностей та мережевих структур в аналітичній діяльності.

15 Просторово-часовий аналіз у системі оцінювання оперативної обстановки.

16 Архітектура автоматизованих інформаційно-аналітичних систем сектору безпеки і оборони.

17 Проблема взаємосумісності інформаційних систем різних державних відомств та шляхи її подолання.

18 Штучний інтелект в інформаційно-аналітичній діяльності: прикладний потенціал і безпекові ризики.

19 Життєвий цикл цифрових даних у захищених інформаційних середовищах.

20 Алгоритмічна упередженість і ризики непрозорості аналітичних платформ.

21 Аналітичний документ як формалізація результатів інформаційно-аналітичної роботи.

22 Вимоги до структури, логіки та доказової бази аналітичної довідки.

23 Профіль ризику як інструмент превентивної безпекової діяльності.

24 Ситуаційний звіт: методика підготовки в умовах кризового реагування.

25 Стандарти та методи візуалізації даних в інформаційно-аналітичних документах.

26 Спеціальний зв’язок у системі управління сектором безпеки і оборони України.

27 Організаційно-технічні засади побудови захищених мереж урядового зв’язку.

28 Роль Державної служби спеціального зв’язку та захисту інформації України у забезпеченні національної безпеки.

29 Забезпечення стійкості та безперебійності систем спеціального зв’язку в умовах надзвичайних ситуацій.

30 Інтеграція сучасних телекомунікаційних технологій у контур спеціального та урядового зв’язку.

31 Криптографічний захист інформації: сучасні алгоритми та перспективи розвитку.

32 Системи управління ключовою інформацією в мережах спеціального зв’язку.

33 Електронний підпис як інструмент забезпечення цілісності та автентичності електронних документів.

34 Інженерно-технічні заходи захисту інформації на об’єктах інформаційної діяльності.

35 Технічні канали витоку інформації та методи їх надійної нейтралізації.

36 Організація режиму секретності в підрозділах сектору безпеки і оборони.

37 Правові режими обігу інформації з обмеженим доступом в Україні.

38 Принцип службової необхідності як основа мінімізації ризиків витоку таємної інформації.

39 Порядок поводження з носіями службової та таємної інформації: організаційний та правовий аспекти.

40 Архівування та знищення документів з обмеженим доступом: суворі вимоги безпеки.

41 Внутрішні загрози інформаційній безпеці: психологічні та організаційні чинники інсайдерської діяльності.

42 Методи виявлення та нейтралізації інсайдерських ризиків в органах державної влади.

43 Кіберзагрози для закритих телекомунікаційних мереж спеціального призначення.

44 Моделі компрометації інформаційних ресурсів та алгоритми реагування на кіберінциденти.

45 Соціальна інженерія як інструмент несанкціонованого доступу до відомчих систем зв’язку.

46 Інтегроване інформаційно-аналітичне забезпечення спеціальних операцій.

47 Прогностичне моделювання ризиків у діяльності правоохоронних органів та спеціальних служб.

48 Координація міжвідомчої взаємодії під час планування та реалізації спільних безпекових заходів.

49 Використання матриць ризиків та індикаторів загроз в оперативній діяльності.

50 Інформаційне супроводження процесу прийняття управлінських рішень в умовах дефіциту часу та неповноти даних.

5.3 Форми проведення модульного контролю та критерії оцінювання

Проведення модульного контролю з дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв’язок».

здійснюється у формі тестового завдання.

Тестові завдання стосуються термінології, функцій, принципів та особливостей адміністративного судочинства.

Запитання формулюються з урахуванням принципів:

Лаконічність: чіткі та стислі формулювання.

Завершеність: відповіді охоплюють всі аспекти запитання.

Гомогенність: правильні та неправильні варіанти відповіді логічно та граматично подібні.

Вибірковість: питання стосуються суттєвих аспектів вивченого матеріалу.

Завдання передбачають вибір одного правильного варіанта з трьох запропонованих.

Кожне тестове завдання оцінюється в **1 бал**. (**1 бал** – відповідь правильна; **0** балів – відповідь неправильна).

Загальна максимальна можлива кількість балів за модульну контрольну роботу - 15 балів.

Час на виконання.

На виконання всього контрольного завдання відводиться **30 хвилин.**

Мінімальний поріг.

Для успішного складання модульного контролю здобувач повинен набрати не менше 10 балів (60% від максимальної кількості).

Загальні критерії оцінювання тестових завдань:

Бали	**Процент виконання**	**Результат**
14-15	-100%	Зараховано
13	83-90%	
12	76-82%	
11	60-75%	
10	60-67%	
0-9	< 60%	Не зараховано

5.4 Індивідуальні завдання та критерії їх оцінювання

До додаткових (індивідуальних) видів навчальної діяльності відносять участь здобувачів у роботі наукових конференцій, наукових гуртків здобувачів і проблемних груп, підготовці публікацій, участь у Всеукраїнських олімпіадах і конкурсах та Міжнародних конкурсах тощо понад обсяги завдань, які встановлені відповідною робочою програмою навчальної дисципліни.

За рішенням кафедри здобувачам освіти, які брали участь у науково-дослідній роботі та виконували певні види додаткових (індивідуальних) видів навчальної діяльності, можуть присуджуватися заохочувальні (бонусні) бали за визначену освітню компоненту.

Також, заохочувальні бали можуть нараховуватися, якщо здобувач освіти, наприклад, виконав і захистив певні види робіт, відвідував всі лекції, семінарські й

практичні заняття, має власний рукописний конспект лекцій та опрацьований додатковий навчальний матеріал, немає пропусків занять без поважних причин, відвідував додаткові консультації за участі лектора тощо.

Сума заохочувальних балів враховується при виставленні підсумкових балів в заліково-екзаменаційну відомість (але не більше **89 балів** в загальному підсумку) і може бути автоматично зарахована при виставленні підсумкової семестрової оцінки з відповідної освітньої компоненти.

Заохочувальні бали не є нормативними і не входять до таблиці розподілу балів, які отримують здобувачі вищої освіти та основної шкали системи оцінювання.

Один захід може бути підставою для виставлення заохочувальних балів лише за однією найбільш релевантною освітньою компонентою.

5.5 Форми проведення семестрового контролю та критерії оцінювання

Екзамен. Відбувається згідно з «Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ ВНЗ МАУП» https://maup.com.ua/assets/files/yakist/studcentr/polozhennya-pro-sistemu-ocinyuvannya-rezultativ-navchannya-zdobuvachiv-vishhoi-osviti.pdf

Орієнтовний перелік питань для комплексного контролю:

1 Сутність та завдання інформаційно-аналітичного забезпечення в діяльності суб’єктів сектору безпеки і оборони.
2 Еволюція підходів до оброблення інформації в органах державної влади.
3 Інформація як стратегічний ресурс: критерії якості, повноти та своєчасності.
4 Структура та логіка функціонування інформаційно-аналітичного циклу.
5 Сутність та переваги ризик-орієнтованого підходу у безпековій діяльності.
6 Характеристика розвідувально-керованої моделі прийняття управлінських рішень.
7 Науково обґрунтований підхід до оцінювання оперативної обстановки.
8 Роль аналітика у трансформації необроблених даних в управлінське знання.
9 Основні перешкоди та когнітивні викривлення на етапі інтерпретації безпекової інформації.
10 Сутність та завдання інформаційно-аналітичного забезпечення в діяльності суб’єктів сектору безпеки і оборони.
11 Еволюція підходів до оброблення інформації в органах державної влади.
12 Інформація як стратегічний ресурс: критерії якості, повноти та своєчасності.
13 Структура та логіка функціонування інформаційно-аналітичного циклу.
14 Сутність та переваги ризик-орієнтованого підходу у безпековій діяльності.
15 Характеристика розвідувально-керованої моделі прийняття управлінських рішень.
16 Науково обґрунтований підхід до оцінювання оперативної обстановки.
17 Роль аналітика у трансформації необроблених даних в управлінське знання.
18 Основні перешкоди та когнітивні викривлення на етапі інтерпретації безпекової інформації.

19 Класифікація джерел інформації в системі національної безпеки.
20 Оперативні джерела інформації: специфіка здобуття та критерії перевірки.
21 Правові та етичні межі використання відкритих джерел інформації.
22 Методологія розвідки за відкритими джерелами в аналітичній діяльності.
23 Технічні канали отримання даних: можливості та обмеження.
24 Роль державних реєстрів і відомчих баз даних у формуванні єдиної картини загроз.
25 Проблема взаємосумісності та міжвідомчого обміну базами даних.
26 Критерії оцінювання достовірності інформації та надійності її джерела.
27 Процесуальні джерела інформації та їхнє значення для кримінального аналізу.
28 Поняття та функціональне призначення безпекового аналізу.
29 Співвідношення безпекового, кримінального та оперативного аналізу.
30 Стратегічний аналіз: завдання, горизонт планування та методологія.
31 Оперативний аналіз як інструмент супроводження поточних безпекових заходів.
32 Тактичний аналіз: специфіка швидкого реагування на локальні загрози.
33 Методи виявлення прихованих зв’язків та мережевих структур.
34 Аналіз злочинних мереж: побудова графових моделей та ідентифікація ключових вузлів.
35 Просторово-часове моделювання в оцінюванні безпекових ризиків.
36 Виявлення серійності та патернів у діях об’єктів оперативної зацікавленості.
37 Архітектура автоматизованих інформаційно-аналітичних систем в органах державної влади.
38 Інтегровані інформаційні середовища: принципи побудови та функціонування.
39 Життєвий цикл цифрових даних у закритих інформаційних системах.
40 Стандартизація форматів даних як передумова ефективного міжвідомчого обміну.
41 Прикладний потенціал систем штучного інтелекту в аналітичній роботі.
42 Алгоритмічна упередженість та ризики непрозорості моделей машинного навчання.
43 Загрози деградації алгоритмічних моделей у процесі оброблення великих масивів даних.
44 Роль людського контролю в автоматизованих системах підтримки прийняття рішень.
45 Хмарні технології у секторі безпеки: переваги та ризики компрометації даних.
46 Класифікація та функціональне призначення аналітичних документів.
47 Аналітична довідка: вимоги до структури, стилю та доказової бази.
48 Інформаційне зведення як форма оперативного інформування керівництва.
49 Профіль ризику: методика розроблення та сфера застосування.
50 Ситуаційний звіт: алгоритм підготовки в умовах кризового управління.
51 Профіль особи (об’єкта): ключові елементи та джерела формування.
52 Рівні впевненості та ймовірності у формулюванні аналітичних висновків.
53 Стандарти візуалізації даних у звітах для керівного складу.
54 Порядок безпечного поширення аналітичних продуктів серед визначених адресатів.
55 Сутність, завдання та види спеціального зв’язку.

56 Архітектура державної системи урядового зв’язку України.
57 Роль Державної служби спеціального зв’язку та захисту інформації України.
58 Вимоги до стійкості, безперебійності та прихованості каналів спеціального зв’язку.
59 Організаційно-технічні заходи забезпечення безпеки телекомунікаційних мереж.
60 Взаємодія підрозділів спеціального зв’язку з іншими суб’єктами сектору оборони.
61 Функціонування систем захищених комунікацій в умовах надзвичайних ситуацій.
62 Інтеграція сучасних цифрових технологій у класичні системи спеціального зв’язку.
63 Дисципліна зв’язку як ключовий фактор запобігання перехопленню інформації.
64 Характеристика основних загроз перехоплення інформації у каналах зв’язку.
65 Сутність та завдання криптографічного захисту інформації.
66 Симетричні алгоритми шифрування: принципи дії, переваги та недоліки.
67 Асиметрична криптографія та її роль у захисті службових комунікацій.
68 Криптографічне гешування як засіб забезпечення цілісності даних.
69 Електронний підпис: правовий статус та технічні механізми реалізації.
70 Інфраструктура відкритих ключів (PKI) у державному секторі.
71 Системи технічного захисту інформації на об’єктах інформаційної діяльності.
72 Виявлення та блокування технічних каналів витоку інформації.
73 Правові режими обігу інформації з обмеженим доступом в Україні.
74 Державна таємниця: критерії віднесення, ступені секретності та строки дії.
75 Службова та конфіденційна інформація: порядок визначення та захисту.
76 Принцип службової необхідності як базова логіка мінімізації ризиків витоку даних.
77 Порядок надання та скасування допуску до державної таємниці.
78 Організація обліку, маркування та зберігання матеріальних носіїв секретної інформації.
79 Правила копіювання, передавання та транспортування документів з обмеженим доступом.
80 Процедура архівування та комісійного знищення секретних документів.
81 Відповідальність посадових осіб за порушення законодавства про державну таємницю.
82 Класифікація сучасних кіберзагроз для відомчих інформаційних систем.
83 Внутрішні (інсайдерські) ризики: психологічний портрет та мотивація порушника.
84 Моделі несанкціонованого доступу та компрометації пристроїв у захищених мережах.
85 Соціальна інженерія як метод подолання організаційного захисту інформації.
86 Несанкціоноване передавання даних через використання відкритих каналів зв'язку.
87 Апаратні та програмні закладки: методи виявлення та нейтралізації.
88 Організаційні заходи контролю для мінімізації інсайдерських ризиків.
89 Технічні засоби моніторингу та запобігання витоку даних (DLP-системи).
90 Алгоритм дій посадових осіб у разі виявлення факту компрометації інформації.

Шкала відповідності оцінок

Сума балів за всі види навчальної діяльності	Оцінка ECT8	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи),	для заліку
90 – 100	A	відмінно	Зараховано
82-89	B	добре	
75-81	C		
68-74	D	задовільно	
60-67	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

6. Політика курсу:

Курс Інформаційно-аналітичне забезпечення та спеціальний зв'язок передбачає засвоєння та дотримання принципів етики та академічної доброчесності згідно Кодексу академічної доброчесності МАУП та Положення про запобігання та виявлення плагіату в наукових та академічних текстах у ПрАТ ВНЗ МАУП, зокрема орієнтації на запобігання плагіату у будь-яких його проявах: всі роботи, доповіді, есе, реферати та презентації мають бути оригінальними та авторськими, не переобтяженими цитатами, що мають супроводжуватися посиланнями на першоджерела. Порушеннями академічної доброчесності вважаються: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання.

Оцінювання здобувача освіти орієнтовано на отримання балів за активність на семінарських (практичних) заняттях, а також виконання завдань для самостійної роботи.

Відпрацювання семінарського заняття може здійснюватися у формі опитування, тестування, виконання практичного завдання, розв'язання задачі з відповідної теми.

В кінці вивчення курсу проводиться модульна контрольна робота 1. Результат модульної контрольної роботи для здобувача, який не з'явився на контрольні заходи, є нульовим. У такому разі, здобувач має можливість повторно виконати модульну контрольну роботи.

Не допустимо: пропуск занять без поважних причин; запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття (за винятком дозволу викладача при зверненні до текстів нормативно-правових актів); списування та плагіат.

Рекомендовані джерела (література):

Основні джерела:

1. Франчук В. І. Теорія безпеки соціальних систем: підручник. 2-ге вид., перероб. і допов. Львів; Одеса: Фенікс, 2020. 224 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3462/1/%D1%84%D1%80%D0%B0%D0%BD%D1%87%D1%83%D0%BA%20%D1%82%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.pdf
2. Отенко І. П., Москаленко Н. О., Азаренков Г. Ф. Теорія управління безпекою соціальних систем: навчальний посібник. Харків: ХНЕУ ім. С. Кузнеця, 2014. 220 с.
3. Живко З. Б., Баворовська О. Б., Занора В. О. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник. Черкаси: видавець Чабаненко Ю. А., 2019. 120 с.
4. Монастирський Г. Л. Теорія організації: підручник. Тернопіль: ТНЕУ, 2014. 288 с. URL: https://elcat.pnpu.edu.ua/docs/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9.pdf
5. Гриненко В. В. Основи безпеки бізнесу: навчальний посібник. Харків: ХНУМГ ім. О. М. Бекетова, 2020. URL: https://eprints.kname.edu.ua/59074/1/2020%20%D0%BF%D0%B5%D1%87%20100%D0%9B%20%D0%9A%D0%9B%20%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81%D1%83%20%D0%93%D1%80%D0%B8%D0%BD%D0%B5%D0%BD%D0%BA%D0%BE.pdf

Додаткові:

Коломієць Б. С. Еволюція поняття безпеки: від класичних теорій до сучасних підходів. Economics: Time Realities. 2024. № 6(76). С. 47–55.

Олійник П. П. Організаційно-правові аспекти забезпечення безпеки підприємства: монографія. Тернопіль: ТНЕУ, 2016.

Резнікова О. С. Національна стійкість: монографія. Гарміш-Партенкірхен: Центр Джорджа К. Маршалла, 2021.

Корж І. Методологічні підходи до визначення поняття «безпека». Юридичний науковий електронний журнал. 2019. № 4. URL: https://www.jurnaluljuridic.in.ua/archive/2019/4/part_1/14.pdf

Стиценко Т. Є., Пронюк Г. В., Сердюк Н. М., Хондак І. І. Безпека життєдіяльності: навчальний посібник. Харків: ХНУРЕ, 2018. 336 с. URL: https://os.nure.ua/wp-content/uploads/2021/04/posibnik-bgd_2018.pdf

Інформаційні ресурси:

1.Бібліотека ім. В. І. Вернадського – http://www.nbuv.gov.ua
2. Верховна Рада України – http://zakon.rada.gov.ua
3. Президент України – http://www.president.gov.ua
4. Кабінет Міністрів України – http://www.kmu.gov.ua
5. Міністерство юстиції України – http://www.minjust.gov.ua
6. Офіційний веб портал судової влади в Україні URL: https://court.gov.ua/
7. Єдиний реєстр судових рішень в Україні. URL: https://reyestr.court.gov.ua/
8. Prozorro: система публічних закупівель. URL: https://prozorro.gov.ua
9. Сайт Національної бібліотеки України ім. В. І. Вернадського. Ресурси. URL: http://www.nbuv.gov.ua/