ПРАТ «ВНЗ «МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА ІМЕНІ КНЯЗЯ ВОЛОДИМИРА ВЕЛИКОГО

Кафедра правоохоронної та антикорупційної діяльності

«ЗАТВЕРДЖУЮ»
Завідувач кафедри правоохоронної
та антикорупційної діяльності

_____ Володимир ЗАРОСИЛО
"08" _____08_____ 2025р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ТА СПЕЦІАЛЬНИЙ ЗВ'ЯЗОК»

Галузь знань: **26 Цивільна безпека**

Спеціальність: **262 Правоохоронна діяльність**

Освітній рівень: **другий (магістерський) рівень**

Освітня програма **«Правоохоронна діяльність»**

Київ 2025

Робоча програма з навчальної дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» для здобувачів вищої освіти освітньої програми «Правоохоронна діяльність» спеціальності 262 Правоохоронна діяльність:

Розробник:

Лисенко Сергій Олексійович - професор кафедри правоохоронної та антикорупційної діяльності, доктор наук з державного управління, доктор юридичних наук, професор.

Сергій ЛИСЕНКО

_____
(підпис)

Робочу програму погоджено

Гарант освітньої програми «Правоохоронна діяльність»

Олександр САВКА

_____
(підпис)

Робочу програму розглянуто та схвалено на засіданні кафедри правоохоронної та антикорупційної діяльності

Протокол № 1 від «23» 08 2025 року

Завідувач кафедри правоохоронної та антикорупційної діяльності

Володимир ЗАРОСИЛО

_____
(підпис)

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	очна (денна)	заочна
Вид дисципліни (обов'язкова чи вибіркова)	обов'язкова	
Мова викладання	українська	
Загальний обсяг у кредитах ЄКТС / годинах	3/90	3/90
Курс	1	1
Семестр	1	1
Кількість змістових модулів	2	2
Обсяг кредитів із розподілом за семестрами	4	4
Обсяг годин, у тому числі:		
- Аудиторні	34	4
- Лекційні	20	2
- Семінарські / Практичні	14	2
- Лабораторні	-	-
Самостійна робота, год	56	86
Форма семестрового контролю	залік	

Мета й завдання навчальної дисципліни

Метою навчальної дисципліни є «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» є формування у здобувачів комплексних знань щодо сутності, структури та функцій інформаційно-аналітичного забезпечення в системі безпеки й правоохоронної діяльності, а також набуття практичних умінь застосовувати інформаційно-аналітичні підходи для виявлення загроз, оцінювання ризиків, підготовки аналітичних матеріалів і підтримки управлінських та оперативних рішень. Вивчення дисципліни має забезпечити розуміння того, що сучасна безпекова діяльність ґрунтується не лише на реагуванні на події, а й на системному використанні даних, аналітичних методів, цифрових інструментів, міжвідомчого обміну інформацією та режимів її захисту. Метою курсу є також формування у здобувачів здатності працювати в логіці інформаційного циклу, поєднувати різні джерела даних, готувати аналітичні довідки, зведення, профілі ризику та ситуаційні звіти, а також

забезпечувати належний рівень конфіденційності, цілісності й доступності інформації у професійній діяльності.

Завдання навчальної дисципліни:

Засвоєння базових понять, категорій і принципів інформаційно-аналітичного забезпечення та спеціального зв'язку; формування системного розуміння інформації як стратегічного ресурсу, що використовується для оцінювання обстановки, виявлення загроз і підтримки рішень; опанування логіки інформаційного циклу та основ безпекового, кримінального й оперативного аналізу; розвиток умінь працювати з різними джерелами інформації, у тому числі відкритими, відомчими, процесуальними й технічними, та здійснювати їх критичну перевірку й аналітичну інтерпретацію; формування здатності готувати основні види аналітичних документів у діяльності органів безпеки та правоохоронних органів із дотриманням вимог до структури, логіки, доказовості й режиму доступу; набуття знань щодо функціонування інформаційно-аналітичних систем, інтегрованих інформаційних середовищ і ролі цифрових технологій та штучного інтелекту в аналітичній роботі; опанування основ спеціального зв'язку, технічного захисту інформації, режиму секретності та принципу need-to-know як ключових елементів безпечного обігу інформації; формування умінь застосовувати аналітику для прогнозування загроз, підтримки міжвідомчої взаємодії та інформаційного супроводження діяльності у сфері безпеки та правоохоронної практики.

Компетентності та результати навчання за освітньою програмою

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 4 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.

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, 6 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 інформаційноаналітичних 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.

Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ОСНОВИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ БЕЗПЕКИ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Тема 1. Теоретичні основи інформаційно-аналітичного забезпечення систем безпеки та правоохоронної діяльності

Тема формує базове розуміння сутності інформаційного забезпечення як організованої системи збору, перевірки, збереження, обробки, аналізу та доведення інформації до суб'єкта прийняття рішень. Розкривається роль аналітики як центрального елементу сучасних risk-based, intelligence-led та evidence-based підходів у діяльності органів безпеки і правоохоронних органів. Окрема увага приділяється інформації як стратегічному ресурсу безпекової системи та інформаційному циклу як логіці перетворення даних на аналітичний продукт для управлінських і оперативних рішень.

Тема 2. Джерела інформації у правоохоронній діяльності та забезпеченні безпеки

Тема присвячена характеристиці оперативних, процесуальних, відкритих і технічних джерел інформації, їх пізнавальним можливостям, правовим режимам, перевагам, обмеженням та ризикам використання. Розглядається OSINT як окремий інструмент сучасної аналітики у сфері безпеки, а також

значення відомчих баз даних і міжвідомчого інформаційного обміну для формування цілісної картини загроз і підтримки координації між органами.

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, їх 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 патернів.

Тема 4. Інформаційно-аналітичні системи органів безпеки та правоохоронних органів

Тема формує цілісне уявлення про автоматизовані інформаційні системи, аналітичні платформи та інтегровані інформаційні середовища, які забезпечують збір, узгодження, обмін і використання даних у правоохоронному та безпековому контурі. 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 моделей і витоку даних.

Тема 5. Аналітичні документи в діяльності органів безпеки та правоохоронних органів

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

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

Тема 6. Основи спеціального зв'язку в системах безпеки та правоохоронній діяльності

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 передачі 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, хешування, цифрового 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 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, передачі, архівування та знищення документів і носіїв, а також принцип need-to-know як центральна логіка мінімізації ризику витоку інформації у безпековому та правоохоронному середовищі.

Тема 9. Кіберзагрози та інсайдерські ризики в правоохоронних органах

Тема орієнтована на вивчення сучасних кіберзагроз для інформаційних систем, каналів зв'язку та службових комунікацій правоохоронних органів, 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, несанкціоновані передачі, порушення режиму доступу, використання незахищених каналів, а також базові організаційні й технічні контролі мінімізації таких ризиків. Назва і зміст цієї теми логічно випливають із контрольних питань курсу та внутрішньої структури попередніх лекцій, де тема 6 прямо пов'язує загрози спецзв'язку з темами 7–9.

Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій органів безпеки та 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 tasking і coordination, підготовки спільних аналітичних продуктів, узгодження режимів доступу, організації інформаційної підтримки операцій, а також використання аналітики для прогнозування загроз через індикатори, сценарії, risk-моделі та матриці ризику.

Структура навчальної дисципліни

Назви тем	Кількість годин							
	очна (денна) форма				заочна форма			
	Усього	у тому числі			Усього	у тому числі		
		Лекції	Семінари	Самостійна робота		Лекції	Семінари	Самостійна робота
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ОСНОВИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ БЕЗПЕКИ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ								
Тема 1. Теоретичні основи інформаційно-аналітичного забезпечення систем безпеки та правоохоронної діяльності.	8	2	2	4	12	2	2	8
Тема 2. Джерела інформації у правоохоронній діяльності та забезпеченні безпеки.	8	2		6	8			8
Тема 3. Основи безпекового, кримінального та оперативного аналізу.	10	2	2	6	8			8
Тема 4. Інформаційно-аналітичні системи органів безпеки та правоохоронних органів.	10	2	2	6	10			10
Тема 5. Аналітичні документи в діяльності органів безпеки та правоохоронних органів.	6	2		4	8			8

ЗМІСТОВИЙ МОДУЛЬ 2. СПЕЦІАЛЬНИЙ ЗВ'ЯЗОК, ЗАХИСТ ІНФОРМАЦІЇ ТА ІНТЕГРОВАНЕ АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАЦІЙ								
Тема 6. Основи спеціального зв'язку в системах безпеки та правоохоронній діяльності	10	2	2	6	8			8
Тема 7. Технічний та криптографічний захист інформації.	8	2		6	8			8
Тема 8. Режим секретності та захист службової інформації.	10	2	2	6	10			10
Тема 9. Кіберзагрози та інсайдерські ризики в правоохоронних органах.	10	2	2	6	10			10
Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій органів безпеки та оборони.	10	2	2	6	8			8
Модульна контрольна робота								
Всього:	**90**	**20**	**14**	**56**	**90**	**2**	**2**	**86**
Форма контролю: залік								

Теми семінарських занять

№ Семінар. заняття	Назва теми	Кількість годин	
		очна (денна) форма	заочна форма
Семінарське заняття №1	**Тема 1. Теоретичні основи інформаційно-аналітичного забезпечення систем безпеки та правоохоронної діяльності** Завдання: • Визначити сутність інформаційного забезпечення як системи збору, перевірки, збереження, обробки, аналізу та доведення інформації до суб'єкта прийняття рішень.	2	2

	• Охарактеризувати значення risk-based, intelligence-led та evidence-based підходів у діяльності органів безпеки і правоохоронних органів. • Скласти схему інформаційного циклу: дані → перевірка → обробка → 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 інформаційного циклу? **Тема 2. Джерела інформації у правоохоронній діяльності та забезпеченні безпеки** Завдання: • Визначити основні види джерел інформації: оперативні, процесуальні, відкриті, технічні та відомчі. • Порівняти їх пізнавальні можливості, правові режими, переваги, обмеження та ризики використання. • Проаналізувати значення OSINT, відомчих баз даних і міжвідомчого інформаційного обміну для формування цілісної картини загроз. Очікуваний результат: • Вміння класифікувати джерела		

	інформації та оцінювати їх придатність для виконання конкретних безпекових завдань. • Здатність визначати межі допустимого й ефективного використання різних джерел у правоохоронній діяльності. 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?		
Семінарське заняття №2	**Тема 3. Основи безпекового, кримінального та оперативного аналізу** Завдання: • Визначити поняття безпекового, кримінального та оперативного аналізу, розкрити їх 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 патернів. 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:	2	

	• Чи є стратегічний аналіз більш значущим для системи безпеки, ніж тактичний? • Наскільки аналітичний висновок залежить від якості вихідної інформації?		
Семінарське заняття №3	**Тема 4. Інформаційно-аналітичні системи органів безпеки та правоохоронних органів** 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 моделей і витоку даних. Очікуваний результат: • Вміння пояснювати місце інформаційно-аналітичних систем у діяльності органів безпеки та правоохоронних органів. • 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?	2	

	Тема 5. Аналітичні документи в діяльності органів безпеки та правоохоронних органів 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 їх 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?		
Семінарське заняття №4	**Тема 6. Основи спеціального зв'язку в системах безпеки та правоохоронній діяльності** Завдання: • Визначити сутність спеціального зв'язку як окремого класу службових і державних комунікацій. • Охарактеризувати види спеціального зв'язку та підходи до побудови захищених каналів передачі інформації.	2	

	• 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, хешування, цифрового 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?		
Семінарське заняття №5	**Тема 8. Режим секретності та захист службової інформації** Завдання: • Визначити правові режими інформації з обмеженим доступом: службова, конфіденційна, таємна інформація. • Розкрити правила маркування, обліку, зберігання, використання, копіювання, передачі, архівування та знищення документів і носіїв. • Пояснити значення принципу need-to-know 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?	2	
Семінарське	**Тема 9. Кіберзагрози та інсайдерські**	2	

заняття №6	**ризики в правоохоронних органах** Завдання: • Визначити сучасні кіберзагрози для інформаційних систем, каналів зв'язку та службових комунікацій правоохоронних органів. • Проаналізувати інсайдерські ризики як окрему категорію загроз, пов'язаних із діями або бездіяльністю персоналу. • Охарактеризувати типові моделі компрометації ключів і пристроїв, несанкціоновані передачі, порушення режиму доступу, використання незахищених каналів та базові контролі 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 правоохоронного органу: зовнішня кібератака чи внутрішнє порушення режиму? • Чи можливо повністю усунути інсайдерські ризики лише за допомогою технічних засобів?		
Семінарське заняття №7	**Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій органів безпеки та оборони** Завдання: • Розкрити, як джерела інформації, аналітичні процедури, управлінські механізми та міжвідомча взаємодія поєднуються в єдиний контур	2	

	підтримки оперативно-розшукових заходів і спеціальних операцій. • Охарактеризувати питання tasking, coordination, підготовки спільних аналітичних продуктів та узгодження режимів доступу. • Розглянути використання аналітики для прогнозування загроз через індикатори, сценарії, risk-моделі та матриці ризику. 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 годин:		14	2

Самостійна робота

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» передбачає підготовку до аудиторних занять шляхом опанування матеріалів лекції, вивчення базової і додаткової літератури, періодичних видань, інтернет-джерел та судової практики, виконання практичних завдань (написання рефератів, аналіз проблемних ситуацій, підготовка результатів власних досліджень до виступу на конференціях, участь в конкурсах наукових робіт, підготовці та публікації наукових статей, тез тощо) протягом семестру; самостійне опрацювання окремих тем навчальної дисципліни; підготовку доповідей та презентацій за тематикою практичних занять; переклад іноземних текстів

установлених обсягів; опрацювання матеріалів правозастосовної практики, підготовку аналітичних і порівняльних висновків та формування навичок науково-правового аналізу; виконання індивідуальних завдань; підготовку до усіх видів контролю, у тому числі модульних контрольних робіт і підсумкової атестації; підготовку юридичних документів, інші види діяльності, що використовуються в Академії, Інституті і кафедрі.

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 систем безпеки та правоохоронної діяльності** Підготувати короткий аналітичний опис сутності інформаційно-аналітичного забезпечення як функції систем безпеки та правоохоронної діяльності, визначивши його місце у процесі прийняття управлінських і оперативних рішень. Скласти глосарій із 20 ключових термінів теми з короткими визначеннями: інформація, дані, аналітика, інформаційне забезпечення, аналітичний продукт, управлінське рішення, безпекова інформація, ризик, загроза, індикатор, intelligence-led policing, risk-based approach, evidence-based approach, інформаційний цикл, обробка даних, верифікація, джерело інформації, достовірність, релевантність, інформаційна цінність.	Презентація результатів
2	**Тема 2. Джерела інформації у правоохоронній діяльності та забезпеченні безпеки** Підготувати порівняльну характеристику основних джерел інформації у сфері безпеки та правоохоронної діяльності, визначивши їх переваги, обмеження та особливості практичного використання. Скласти перелік і коротко охарактеризувати 20 понять теми: джерело інформації, відкрите джерело, OSINT, HUMINT, SIGINT, відомча база даних, міжвідомчий обмін, оперативна інформація,	Презентація результатів

	процесуальна інформація, первинні дані, вторинні дані, достовірність, повнота, актуальність, верифікація, аналітична вибірка, інформаційний масив, реєстр, облік, інформаційний слід.	
3	**Тема 3. Основи безпекового, кримінального та оперативного аналізу** Підготувати короткий текстовий матеріал про співвідношення безпекового, кримінального та оперативного аналізу із визначенням їх функціонального призначення у практичній діяльності органів безпеки та правоохоронних органів. Скласти глосарій із 20 термінів: безпековий аналіз, кримінальний аналіз, оперативний аналіз, стратегічний аналіз, тактичний аналіз, аналітична модель, часовий аналіз, просторовий аналіз, зв'язковий аналіз, профілювання, шаблон поведінки, серійність, аналітична гіпотеза, аналітичний висновок, патерн, прогнозування, сценарій, ймовірність, аналітичний критерій, оцінювання загроз.	Презентація результатів
4	**Тема 4. Інформаційно-аналітичні системи органів безпеки та правоохоронних органів** Підготувати короткий опис ролі інформаційно-аналітичних систем у діяльності органів безпеки та правоохоронних органів, звернувши увагу на автоматизацію обробки даних, підтримку рішень та ризики цифровізації. Скласти глосарій із 20 термінів: інформаційна система, аналітична система, база даних, дата-центр, інтероперабельність, цифровізація, алгоритм, штучний інтелект, машинне навчання, автоматизація, модуль аналітики, кіберзахист, захищений доступ, життєвий цикл даних, резервування, інтегрована платформа, журнал подій, метадані, модель даних, вразливість системи.	Презентація результатів
5	**Тема 5. Аналітичні документи в діяльності органів безпеки та правоохоронних органів** Підготувати зразкову структуру аналітичного	Презентація результатів

	документа для практичних потреб органу безпеки або правоохоронного органу з виділенням вступної, описової, оціночної та рекомендаційної частин. Скласти глосарій із 20 термінів: аналітична довідка, службова записка, інформаційне зведення, ситуаційний звіт, профіль ризику, профіль особи, аналітична записка, рекомендація, доказовість, рівень впевненості, аналітичне судження, висновок, джерельна база, виконавська дисципліна, формат документа, цільова аудиторія, конфіденційність, службове користування, узагальнення, візуалізація даних.	
6	**Тема 6. Основи спеціального зв'язку в системах безпеки та правоохоронній діяльності** Підготувати короткий огляд значення спеціального зв'язку для функціонування систем безпеки та правоохоронної діяльності, визначивши його місце в координації, управлінні та захисті службових комунікацій. Скласти глосарій із 20 термінів: спеціальний зв'язок, захищений канал, урядовий зв'язок, службова комунікація, передавання даних, криптографічний захист, технічний захист, вузол зв'язку, телекомунікаційна мережа, комутація, радіозв'язок, резервний канал, стійкість каналу, пропускна здатність, конфіденційність, цілісність, доступність, автентифікація, мережевий протокол, режим захисту.	Презентація результатів
7	**Тема 7. Технічний та криптографічний захист інформації** Підготувати стислий матеріал про базові механізми технічного і криптографічного захисту інформації та пояснити, як вони застосовуються в безпековій і правоохоронній практиці. Скласти глосарій із 20 термінів: криптографія, шифрування, дешифрування, ключ шифрування, симетричне шифрування, асиметричне шифрування, хешування, цифровий підпис, сертифікат, компрометація ключа, технічний канал витоку,	Презентація результатів

	екранування, автентичність, цілісність, конфіденційність, захищений носій, контроль доступу, токен, сертифікація засобу захисту, криптографічний протокол.	
8	**Тема 8. Режим секретності та захист службової інформації** Підготувати короткий опис організаційних і правових засад режиму секретності, зосередившись на порядку доступу до інформації з обмеженим доступом та вимогах до її захисту. Скласти глосарій із 20 термінів: державна таємниця, службова інформація, конфіденційна інформація, гриф обмеження доступу, режим секретності, допуск, доступ, носій інформації, облік документів, зберігання, копіювання, знищення, архівування, витік інформації, розголошення, режимне приміщення, need-to-know, контроль доступу, інструктаж, відповідальність за порушення режиму.	Презентація результатів
9	**Тема 9. Кіберзагрози та інсайдерські ризики в правоохоронних органах** Підготувати короткий аналітичний опис основних кіберзагроз та інсайдерських ризиків у діяльності правоохоронних органів із визначенням їх джерел та можливих наслідків. Скласти глосарій із 20 термінів: кіберзагроза, кібератака, фішинг, шкідливе програмне забезпечення, компрометація облікового запису, витік даних, інсайдер, інсайдерський ризик, несанкціонований доступ, інцидент інформаційної безпеки, цифровий слід, журналювання, моніторинг, сегментація мережі, багатофакторна автентифікація, парольна політика, людський фактор, привілейований доступ, реагування на інцидент, політика безпеки.	Презентація результатів
10	**Тема 10. Інтегроване інформаційно-аналітичне забезпечення операцій органів безпеки та оборони** Підготувати короткий матеріал про сутність інтегрованого інформаційно-аналітичного	Презентація результатів

	забезпечення операцій, показавши взаємозв'язок збору інформації, її аналізу, міжвідомчої координації та підтримки рішень. Скласти глосарій із 20 термінів: інтегроване забезпечення, міжвідомча взаємодія, координація, tasking, ситуаційна обізнаність, спільний аналітичний продукт, оперативна обстановка, ризик-модель, матриця ризику, прогнозування, індикатор загрози, сценарне планування, оперативний штаб, аналітична підтримка, інформаційний контур, сумісність систем, обмін даними, пріоритезація, управління ризиками, оцінка ефективності.	

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Інформаційно-аналітичне забезпечення систем безпеки та правоохоронної діяльності».

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. Теоретичні основи інформаційно-аналітичного забезпечення у сфері безпеки та правоохоронної діяльності.

2. Інформація як стратегічний ресурс у системі забезпечення національної безпеки.

3. Місце інформаційно-аналітичної діяльності в системі управління безпекою.

4. Сутність та структура інформаційного циклу в діяльності органів безпеки.

5. Джерела інформації у правоохоронній діяльності: класифікація та характеристика.

6. Використання відкритих джерел інформації в аналітичній роботі органів безпеки.

7. Значення OSINT у сучасному інформаційно-аналітичному забезпеченні.

8. Відомчі інформаційні ресурси як основа аналітичної діяльності правоохоронних органів.

9. Міжвідомчий інформаційний обмін у системі безпеки: проблеми та перспективи.

10. Основні принципи перевірки та верифікації інформації в аналітичній діяльності.

11. Безпековий аналіз як складова управлінської діяльності у сфері національної безпеки.

12. Кримінальний аналіз: поняття, завдання та значення для правоохоронної практики.

13. Оперативний аналіз у діяльності правоохоронних органів: теоретичний і прикладний аспект.

14. Стратегічний аналіз загроз у системі безпеки держави.

15. Тактичний аналіз у процесі прийняття рішень у правоохоронній діяльності.

16. Методи аналітичного виявлення зв'язків між подіями, особами та об'єктами.

17. Просторово-часовий аналіз у сфері безпеки та правоохоронної діяльності.

18. Профілювання ризиків як інструмент аналітичної підтримки безпекових рішень.

19. Прогнозування загроз у діяльності органів безпеки та оборони.

20. Аналітичні моделі оцінювання ризиків у системі безпеки.

21. Інформаційно-аналітичні системи в діяльності правоохоронних органів України.

22. Автоматизовані бази даних у сфері безпеки: можливості та ризики використання.

23. Цифровізація аналітичних процесів у правоохоронній діяльності.

24. Використання штучного інтелекту в інформаційно-аналітичному забезпеченні систем безпеки.

25. Ризики автоматизації аналітичної діяльності в безпековому секторі.

26. Інтероперабельність інформаційних систем як умова ефективної міжвідомчої взаємодії.

27. Аналітичні документи у правоохоронній діяльності: види та вимоги до змісту.

28. Аналітична довідка як форма узагальнення безпекової інформації.

29. Інформаційне зведення як інструмент оперативного управління в системі безпеки.

30. Доказовість та обґрунтованість аналітичних висновків у професійній діяльності.

31. Спеціальний зв'язок як елемент забезпечення функціонування систем безпеки.

32. Роль захищених комунікацій у діяльності органів безпеки та правоохоронних органів.

33. Основи організації спеціального зв'язку в Україні.

34. Технічний захист інформації в діяльності суб'єктів сектору безпеки і оборони.

35. Криптографічний захист інформації як інструмент забезпечення конфіденційності даних.

36. Значення електронного цифрового підпису та криптографічних засобів у безпековій сфері.

37. Захист інформації в телекомунікаційних системах органів безпеки.

38. Режим секретності як складова захисту інформації з обмеженим доступом.

39. Правові засади захисту службової інформації в Україні.

40. Організація доступу до інформації з обмеженим доступом у правоохоронних органах.

41. Кіберзагрози в діяльності органів безпеки: сутність і сучасні прояви.

42. Інсайдерські ризики у правоохоронних органах та шляхи їх мінімізації.

43. Людський фактор у системі інформаційної безпеки правоохоронних органів.

44. Політика інформаційної безпеки як інструмент протидії кіберінцидентам.

45. Реагування на інциденти інформаційної безпеки в органах державної влади.

46. Інтегроване інформаційно-аналітичне забезпечення спеціальних операцій.

47. Міжвідомча координація в процесі інформаційно-аналітичного забезпечення безпекових заходів.

48. Ситуаційна обізнаність як результат аналітичної діяльності у сфері безпеки.

49. Управління ризиками в системі інформаційно-аналітичного забезпечення.

50. Перспективи розвитку інформаційно-аналітичного забезпечення систем безпеки та правоохоронної діяльності в умовах цифрової трансформації.

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.

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.

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.

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://drive.google.com/file/d/1b19SAAb9_C7rwcO5LCg1uDAgISflyArq/view?pli=1

2. «Положенням про систему оцінювання результатів навчання 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

Таблиця розподілу балів, які отримують здобувачі вищої освіти

№ тем	1	2	3	4	5	6	7	8	9	10	Заг.сума балів
Робота на сем.занят.	5		5	5		5		5	5	5	35
Сам.робота	3	3	3	3	3	3	3	3	3	3	30
Всього											**65**

Підсумкове оцінювання	Сума балів за семінари	Сума балів за самостійні роботи	Модульна контрольна робота	Сума балів за екзамен	Загальна сума
	35	30	15	20	100

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 5 балів;

відповідність оформлення практичних робіт вимогам – 1 бал.

(враховуються лише за умови нарахування балів за правильність відповідей).

Робота на семінарському занятті оцінюється **у 5 балів.**

Максимальна кількість балів за семінарські (практичні) заняття по курсу – 35 балів.

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 – 3 бал.

Максимальна кількість балів за самостійну роботу по курсу – 30 балів.

Форми проведення модульного контролю та критерії оцінювання

Проведення модульного контролю з дисципліни «Інформаційно-аналітичне забезпечення систем безпеки та правоохоронної діяльності».

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).

Шкала підсумкового оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	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 складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Форми проведення семестрового контролю та критерії оцінювання

Залік. Відбувається згідно з «Положенням про систему оцінювання результатів навчання 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 контрольних питань з дисципліни "Інформаційно-аналітичне забезпечення та спеціальний зв'язок"

1. Розкрийте сутність інформаційно-аналітичного забезпечення у сфері безпеки та правоохоронної діяльності.
2. Визначте місце інформаційно-аналітичного забезпечення в системі управління безпекою.
3. Охарактеризуйте інформацію як стратегічний ресурс у діяльності органів безпеки.
4. Розкрийте зміст понять дані, інформація, знання в аналітичній діяльності.
5. У чому полягає відмінність між інформаційним забезпеченням і аналітичним забезпеченням.
6. Назвіть основні функції інформаційно-аналітичного забезпечення.
7. Охарактеризуйте основні принципи інформаційно-аналітичної діяльності.
8. Розкрийте сутність intelligence-led підходу у правоохоронній діяльності.
9. Поясніть значення risk-based підходу в системі безпеки.
10. Охарактеризуйте evidence-based підхід у процесі підготовки управлінських рішень.
11. Назвіть і розкрийте основні етапи інформаційного циклу.
12. Охарактеризуйте процес збору інформації в системі безпеки.
13. У чому полягає значення перевірки та верифікації інформації.
14. Розкрийте зміст етапу обробки інформації.
15. Охарактеризуйте сутність аналітичного опрацювання інформації.
16. Поясніть роль аналітичного продукту у прийнятті рішень.
17. Які вимоги ставляться до якості інформації в аналітичній діяльності.
18. Що таке релевантність інформації та як вона оцінюється.
19. У чому полягає актуальність інформації в безпековій діяльності.
20. Розкрийте поняття достовірності інформації.
21. Охарактеризуйте основні джерела інформації у правоохоронній діяльності.
22. Наведіть класифікацію джерел інформації у сфері безпеки.
23. У чому полягають особливості використання відкритих джерел інформації.
24. Розкрийте сутність OSINT та його значення для безпекової діяльності.
25. Охарактеризуйте значення HUMINT у системі збору інформації.
26. Розкрийте особливості використання SIGINT у безпековому середовищі.
27. Яке значення мають відомчі бази даних у правоохоронній діяльності.
28. Розкрийте сутність міжвідомчого інформаційного обміну.
29. Назвіть переваги та обмеження відкритих джерел інформації.
30. У чому полягає різниця між первинними та вторинними даними.
31. Розкрийте сутність безпекового аналізу.
32. Охарактеризуйте кримінальний аналіз як вид аналітичної діяльності.
33. У чому полягає специфіка оперативного аналізу.
34. Поясніть співвідношення безпекового, кримінального та оперативного аналізу.
35. Що таке стратегічний аналіз та яке його значення.

36. Розкрийте сутність тактичного аналізу.
37. У чому полягає значення оперативного рівня аналітичної діяльності.
38. Охарактеризуйте просторовий аналіз у сфері безпеки.
39. Розкрийте зміст часового аналізу у правоохоронній практиці.
40. Що таке зв'язковий аналіз і для чого він використовується.
41. Розкрийте поняття профілювання у безпековому аналізі.
42. Охарактеризуйте виявлення закономірностей і патернів у масивах даних.
43. У чому полягає значення прогнозування загроз.
44. Розкрийте поняття сценарного аналізу в системі безпеки.
45. Що таке аналітична гіпотеза та як вона формується.
46. Охарактеризуйте структуру аналітичного висновку.
47. Які критерії використовуються для оцінювання загроз.
48. У чому полягає значення ризик-моделей в аналітичній діяльності.
49. Розкрийте сутність матриці ризику та її практичне значення.
50. Яке місце займає аналітика у попередженні правопорушень і загроз.
51. Охарактеризуйте інформаційно-аналітичні системи органів безпеки та правоохоронних органів.
52. Розкрийте сутність автоматизованих інформаційних систем у безпековій сфері.
53. У чому полягає значення баз даних для аналітичної роботи.
54. Охарактеризуйте поняття інтероперабельності інформаційних систем.
55. Поясніть значення цифровізації інформаційно-аналітичних процесів.
56. Розкрийте переваги автоматизації аналітичної діяльності.
57. Назвіть ризики цифровізації у сфері безпеки.
58. Охарактеризуйте можливості використання штучного інтелекту в аналітичній діяльності.
59. У чому полягають ризики застосування штучного інтелекту в системі безпеки.
60. Поясніть значення журналів подій і метаданих у сучасних інформаційних системах.
61. Назвіть основні види аналітичних документів у діяльності органів безпеки.
62. Охарактеризуйте аналітичну довідку як форму аналітичного документа.
63. Розкрийте особливості інформаційного зведення.
64. Що таке ситуаційний звіт і яке його практичне значення.
65. Охарактеризуйте структуру аналітичного документа.
66. Які вимоги ставляться до доказовості аналітичних висновків.
67. У чому полягає значення рівня впевненості в аналітичному документі.
68. Розкрийте вимоги до рекомендаційної частини аналітичного документа.
69. Поясніть значення конфіденційності під час підготовки аналітичних матеріалів.
70. Яка роль візуалізації даних у сучасному аналітичному документі.
71. Розкрийте сутність спеціального зв'язку в системах безпеки.
72. Яке значення має спеціальний зв'язок у діяльності органів безпеки та правоохоронних органів.

73. Охарактеризуйте основні види захищених каналів зв'язку.

74. Поясніть значення конфіденційності, цілісності та доступності в системах зв'язку.

75. Розкрийте роль технічного захисту інформації у функціонуванні спеціального зв'язку.

76. Охарактеризуйте криптографічний захист інформації та його основні завдання.

77. У чому полягає різниця між симетричним і асиметричним шифруванням.

78. Розкрийте значення хешування та цифрового підпису в системах захисту інформації.

79. Що таке компрометація ключа і які її наслідки.

80. Охарактеризуйте технічні канали витоку інформації.

81. Розкрийте сутність режиму секретності у сфері захисту інформації.

82. Назвіть основні види інформації з обмеженим доступом.

83. Охарактеризуйте порядок надання допуску до інформації з обмеженим доступом.

84. У чому полягає принцип need-to-know і яке його значення.

85. Розкрийте вимоги до обліку, зберігання та використання службової інформації.

86. Охарактеризуйте сучасні кіберзагрози в діяльності правоохоронних органів.

87. Розкрийте сутність інсайдерських ризиків у системі безпеки.

88. Яку роль відіграє людський фактор у виникненні інформаційних інцидентів.

89. Охарактеризуйте основні заходи протидії кіберзагрозам та інсайдерським ризикам.

90. Розкрийте сутність інтегрованого інформаційно-аналітичного забезпечення операцій органів безпеки та оборони.

Політика курсу:

Курс Інформаційно-аналітичне забезпечення систем безпеки та правоохоронної діяльності 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:

1. Рижков Е. В., Синиціна Ю. П., Прокопов С. О., Гребенюк А. М., Рибальченко Л. В. Інформаційно-аналітичне забезпечення правоохоронної

діяльності : навч. посіб. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 180 с. URL: https://er.dduvs.edu.ua/handle/123456789/15045

2. Мовчан А. В., Крутік Ю. Ю., Горбенко Г. В. Інформаційне забезпечення кримінального аналізу. В: Інформаційно-аналітична діяльність у міжнародних відносинах : колект. монографія. Київ, 2024. Розд. 14. URL: https://vaite.kiev.ua/doi/ilp/ILP_Ch_14.pdf

3. Биков І. О. Інформаційно-аналітичне забезпечення діяльності оперативних підрозділів Бюро економічної безпеки України. Право і суспільство. 2024. № 1, ч. 2. С. 382–387. URL: https://pravoisuspilstvo.org.ua/archive/2024/1_2024/part_2/61.pdf

4. Корнієнко М. В. Кримінальний аналіз у діяльності Національної поліції України як інструмент протидії злочинності. Право і суспільство. 2024. № 1, ч. 2. С. 388–394. URL: https://pravoisuspilstvo.org.ua/archive/2024/1_2024/part_2/62.pdf

5. Калугін В. Ю. Джерела інформаційно-аналітичної діяльності в оперативно-розшуковій протидії кримінальним правопорушенням. Адміністративне право і процес. 2022. № 2. С. 168–173. URL: https://app-journal.in.ua/wp-content/uploads/2022/05/33.pdf

6. Ільченко О. В., Короценко К. Р. Правоохоронні органи як суб'єкти забезпечення кібербезпеки в інформаційному просторі України. Адміністративне право і процес. 2022. № 2. С. 163–167. URL: https://app-journal.in.ua/wp-content/uploads/2022/05/32.pdf

7. Власюк О. В. Використання кримінального аналізу у протидії злочинності. Університетські наукові записки. 2012. № 4. С. 296–302. URL: https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2FUnzap_2012_4_51.pdf&P21DBN=UJRN

8. Шинкаренко І. Р. Кримінальний аналіз як напрям інформаційно-аналітичної роботи у правоохоронній діяльності. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 1. С. 233–239. URL: https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2FNvdduvs_2017_1_34.pdf&P21DBN=UJRN

9. Калиновський О. В., Школьніков В. І. Використання методу кримінального аналізу в діяльності правоохоронних органів України. Часопис Київського університету права. 2017. № 1. С. 267–271. URL: https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2FChkup_2017_1_67.pdf&P21DBN=UJRN

10. Цигикал П. О., Катеринчук І. П., Коваленко В. В. Кримінальний аналіз як елемент інформаційно-аналітичного забезпечення оперативно-розшукової діяльності Державної прикордонної служби України. Збірник наукових праць Національної академії Державної прикордонної служби України. Серія:

військові та технічні науки. 2017. № 2. С. 247–258. URL: https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fznpnapv_vtn_2017_2_22.pdf&P21DBN=UJRN

11. Довгань О. Д. Формування культури кібербезпеки в Україні: правовий аспект. Інформація і право. 2018. № 3(26). С. 95–104. URL: https://ippi.org.ua/sites/default/files/11_9.pdf

12. Кузнєцов О. М. Правове забезпечення кібербезпеки як складова інформаційної безпеки держави. Інформація і право. 2021. № 1(36). С. 107–115. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2021_1_14.pdf

13. Федієнко О. П. Планування кіберстійкості об'єктів критичної інфраструктури: міжнародні стандарти та підходи. Інформація і право. 2024. № 2(49). С. 182–191. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2024_2_16.pdf

14. Мануїлов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури: організаційно-правовий аспект. Інформація і право. 2023. № 1(48). С. 146–156. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2023_1_15.pdf

15. Лепіхов А. В. Ключові інституції стратегічного аналізу у сфері національної безпеки: досвід США для України. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. 2020. № 2(69). С. 70–76. URL: https://znp-cvsd.nuou.org.ua/article/download/213102/213630

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/