ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"
Навчально-науковий інститут права та безпеки імені князя Володимира Великого

МАУП

Кафедра правоохоронної та антикорупційної діяльності

Затверджую:
Директор Навчально-наукового інституту права та безпеки ім. князя Володимира Великого
_____
Сергій ЛИСЕНКО
"08" _____ 2026 р.

Схвалено на засіданні кафедри правоохоронної та антикорупційної діяльності
Протокол № 1 від 28 серпня 2026 року
Завідувач кафедри
_____
Володимир ЗАРОСИЛО

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Інформаційно-аналітичне забезпечення та спеціальний зв'язок»

Спеціальності: **К9 Правоохоронна діяльність**

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

Освітньої програми: **Правоохоронна діяльність**

Спеціалізація: _____

Київ МАУП 2026

Розробник силабусу навчальної дисципліни:

Владислав Олександрович Веклич - доктор юридичних наук, доцент, професор кафедри правоохоронної та антикорупційної діяльності

(підпис)

Викладач:

Владислав Олександрович Веклич - доктор юридичних наук, доцент, професор кафедри правоохоронної та антикорупційної діяльності

(підпис)

Силабус розглянуто на засіданні кафедри правоохоронної та антикорупційної діяльності

Протокол №1від «28» 08. 2026 р.

Загальна інформація про навчальну дисципліну

Назва навчальної дисципліни	Інформаційно-аналітичне забезпечення та спеціальний зв'язок
Шифр та назва спеціальності	К9 «Правоохоронна діяльність»
Рівень вищої освіти	Другий магістерський рівень
Статус дисципліни	обов'язкова
Кількість кредитів і годин	3 кредита/90 год Лекції : 16 Семінарські заняття: 14 Самостійна робота студентів: 60
Терміни вивчення дисципліни	І семестр
Мова викладання	українська
Вид підсумкового контролю	**залік**
Сторінка дисципліни на сайті	https://maup.com.ua/ua/pro-akademiyu/instituti/institut-prava/nacionalna-bezpeka/silabusi.html

Загальна інформація про викладача. Контактна інформація.

Веклич Владислав Олександрович	
Науковий ступінь	Доктор юридичних наук
Вчене звання	доцент
Посада	Професор кафедри
Дисципліни, які викладає НПП	Розвідка на основі відкритих джерел (OSINT)
Напрями наукових досліджень	Державне будівництво, нотаріат, кібербезпека, розвідка на основі відкритих джерел, теорія та історія держави і права, цифровізація.
Посилання на реєстри ідентифікаторів для науковців	ORCID: https://orcid.org/0000-0003-2608-6781 Google Scholar: https://scholar.google.com.ua/citations?user=WBfH9f4AAAAJ&hl=ua
Контактна інформація викладача:	
E-mail:	tdp413@ukr.net
Контактний тел.	(044) 496-97-69
Телефон кафедри	(044) 496-97-69
Портфоліо викладача на сайті кафедри/Інституту/Академії	https://maup.com.ua/ua/pro-akademiyu/instituti/institut-prava/kafedra-istorii-ta-teorii-derzhavi-i-prava/veklich.html

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 інформації, аналітики та спеціального зв'язку у функціонуванні органів безпеки й правоохоронних органів. Дисципліна розкриває логіку перетворення даних на аналітичний продукт, що використовується для підготовки управлінських, профілактичних, оперативних і стратегічних рішень, а також охоплює питання організації інформаційних потоків, міжвідомчої взаємодії, роботи з базами даних, підготовки аналітичних документів, застосування інформаційно-аналітичних систем і дотримання режимів захисту інформації. Особлива увага приділяється сучасним підходам до аналітичної підтримки діяльності у сфері безпеки, зокрема risk-based, intelligence-led та evidence-based моделям, що забезпечують підвищення якості оцінювання загроз, ризиків і тенденцій розвитку безпекового середовища. Опрацювання змісту курсу дозволяє здобувачам зрозуміти місце аналітики в системі попередження правопорушень, виявлення зв'язків і закономірностей, підготовки ситуаційних звітів, профілів ризику та інших аналітичних продуктів, а також у забезпеченні захищеного обігу службової інформації.

1.2 Предмет вивчення курсу

Предметом вивчення навчальної дисципліни є теоретичні, організаційні та прикладні засади інформаційно-аналітичного забезпечення систем безпеки та правоохоронної діяльності, включно з принципами збирання, перевірки, обробки, накопичення, аналізу, збереження, захисту та поширення інформації, що використовується для підтримки управлінських і оперативних рішень. До предмета курсу належать також моделі інформаційного та аналітичного циклу, види безпекового, кримінального й оперативного аналізу, методи виявлення зв'язків, структур і закономірностей, функціонування автоматизованих інформаційних систем та аналітичних платформ, підготовка аналітичних документів, а також правові, організаційні й технічні механізми захисту службової, конфіденційної та іншої чутливої інформації. Опрацювання дисципліни орієнтоване на розвиток умінь працювати з інформацією як зі стратегічним ресурсом безпекової діяльності, критично оцінювати джерела, формувати обґрунтовані аналітичні висновки, визначати ризики витоку чи спотворення даних та забезпечувати належну інформаційну підтримку процесів у системі безпеки і правоохоронної діяльності.

1.3 Метою викладання навчальної дисципліни «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.

1.4 Основні завдання

засвоєння базових понять, категорій і принципів інформаційно-аналітичного забезпечення систем безпеки 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.

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:

Навчальна дисципліна забезпечує формування здобувачами вищої освіти загальних і спеціальних компетентностей та набуття результатів навчання, визначених освітньо-професійною програмою «Правоохоронна діяльність» а саме:

Програмні компетентності

Загальні компетентності	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК8. Здатність приймати обґрунтовані рішення. ЗК10. Здатність оцінювати та забезпечувати якість виконуваних робіт.
Спеціальні компетентності	СК10. Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час рішення професійних завдань. СК12. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних, спеціальної техніки, оперативних та оперативнотехнічних засобів, здійснення оперативно-розшукової діяльності.
Результати навчання	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. РН9. Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення. РН10. Користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку. РН13. Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію. РН16. Використовувати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань. РН17. Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальних засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні); оперативні та

	оперативно-технічні засоби, здійснення оперативно-розшукової діяльності).

2. Зміст навчальної дисципліни

№	Назва теми	К-сть годин, з них:			
		Лекції	**Семінарські зан.**	**Самостійна робота**	**Методи навчання/методи оцінювання**
Сучасні аспекти кримінального процесу					**Методи навчання:** словесні (навчальна лекція; бесіда; навчальна дискусія); індуктивний метод; дедуктивний метод; аналітичний; практичний (робота з фабулами юридичних справ); пояснювально-ілюстративний; репродуктивний; метод проблемного викладу; частково-пошуковий; дослідницький; інтерактивні методи (аналіз ситуацій; дискусії, дебати, полеміки; діалог, синтез думок; мозковий штурм; відпрацювання навичок; ситуативне моделювання, опрацювання дискусійних питань); інноваційні методи навчання
Тема 1.	Сучасний кримінальний процес України: поняття, система, джерела та тенденції розвитку	2	2	6	
Тема 2.	Принципи кримінального провадження та гарантії прав людини			6	
Тема 3.	Учасники кримінального провадження та проблеми реалізації їхнього процесуального статусу			6	
Тема 4.	Докази та доказування: сучасні підходи до збирання, перевірки й оцінювання доказів	2	2	6	
Тема 5.	Заходи забезпечення кримінального провадження та судовий контроль	2	2	6	
Тема 6.	Сучасні проблеми досудового розслідування	2	2	6	

Тема 7.	Негласні слідчі (розшукові) дії та допустимість отриманих результатів	2	2	6	(компетентнісний); кейс-метод.
Тема 8.	Закінчення досудового розслідування та альтернативні форми завершення провадження	2	2	6	**Методи оцінювання:** усний контроль (усне опитування, оцінювання участі у дискусіях, інших інтерактивних методах навчання); письмовий контроль (контрольні, самостійні роботи, реферати); тестовий контроль (тести закритої форми: тест-альтернатива, тест-відповідність); метод самоконтролю та самооцінки; оцінювання кейс-завдань.
Тема 9.	Судове провадження, перегляд судових рішень і забезпечення справедливого суду	2		6	
Тема 10.	Особливі порядки кримінального провадження, воєнний стан і міжнародне співробітництво	2	2	6	
Модульна контрольна робота					
Всього:		**16**	**14**	**60**	
Форма контролю: Залік					

Методи навчання та методи оцінювання

Методи навчання словесні (навчальна лекція; бесіда; навчальна дискусія); індуктивний метод; дедуктивний метод; аналітичний; практичний (робота з фабулами юридичних справ); пояснювально-ілюстративний; репродуктивний; метод проблемного викладу; частково-пошуковий; дослідницький; інтерактивні методи (аналіз ситуацій; дискусії, дебати, полеміки; діалог, синтез думок; мозковий штурм; відпрацювання навичок; ситуативне моделювання, опрацювання дискусійних питань); інноваційні методи навчання (компетентнісний); кейс-метод

Методи оцінювання: усний контроль (усне опитування, оцінювання участі у дискусіях, інших інтерактивних методах навчання); письмовий контроль (контрольні, самостійні роботи, реферати); тестовий контроль (тести закритої форми: тест-альтернатива, тест-відповідність); метод самоконтролю та самооцінки; оцінювання кейс-завдань.

Програма навчальної дисципліни та зміст практичних занять розміщені у відповідній робочій програмі навчальної дисципліни

Самостійна робота

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» полягає в самостійному опрацюванні нормативно-правових актів України та міжнародних договорів, навчальної й наукової літератури, актуальної судової практики Верховного Суду, Європейського суду з прав людини та Міжнародного кримінального суду з питань розвитку кримінального права.

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» полягає в самостійному опрацюванні нормативно-правових актів України, міжнародних стандартів і рекомендацій, навчальної та наукової літератури, методичних матеріалів, а також інших інформаційних джерел з питань організації інформаційно-аналітичної діяльності, використання інформаційних систем, спеціального зв'язку та захисту інформації у сфері безпеки й правоохоронної діяльності.

Самостійна робота передбачає поглиблене вивчення теоретичних і прикладних засад інформаційно-аналітичного забезпечення, джерел отримання та перевірки інформації, методів безпекового, кримінального й оперативного аналізу, функціональних можливостей інформаційно-аналітичних систем, вимог до підготовки аналітичних документів. Окрема увага приділяється принципам організації спеціального зв'язку, технічним і криптографічним засобам захисту інформації, дотриманню режиму секретності та порядку роботи зі службовою інформацією, виявленню кіберзагроз та оцінюванню інсайдерських ризиків. Важливим напрямом є вивчення можливостей інтегрованого інформаційно-аналітичного забезпечення операцій органів безпеки та оборони.

У процесі самостійної роботи здобувачі освіти здійснюють пошук, відбір, перевірку та систематизацію інформації, аналізують нормативно-правові вимоги й організаційно-технічні засади інформаційної діяльності, опрацьовують приклади

застосування інформаційно-аналітичних систем і засобів спеціального зв'язку, розв'язують ситуаційні та практичні завдання, готують аналітичні довідки, інформаційні огляди, доповіді й презентації, виконують індивідуальні дослідницькі завдання та готуються до семінарських занять, модульного контролю й підсумкового оцінювання.

Метою самостійної роботи є поглиблення теоретичних знань, формування навичок пошуку, критичного оцінювання та аналітичного опрацювання інформації, розуміння організаційних і технічних засад спеціального зв'язку та захисту інформації, розвиток здатності виявляти й оцінювати інформаційні та кібернетичні загрози, а також застосовувати набуті знання для інформаційно-аналітичного забезпечення професійної діяльності у сфері безпеки та правоохоронної діяльності.

Матриця самостійної роботи здобувачів вищої освіти міститься у робочій програмі навчальної дисципліни та відповідних методичних рекомендаціях.

Контрольні питання з дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок»

Тема 1

Теоретичні основи інформаційно-аналітичного забезпечення систем безпеки та правоохоронної діяльності

1. Які поняття, сутність і основне призначення інформаційно-аналітичного забезпечення у сфері безпеки та правоохоронної діяльності?
2. Які основні цілі, завдання та функції інформаційно-аналітичного забезпечення?
3. Які принципи організації інформаційно-аналітичної діяльності в системах безпеки та правоохоронних органах?
4. Які основні етапи інформаційно-аналітичного циклу та їхній зміст?
5. Яке значення має інформація для підготовки, обґрунтування та прийняття управлінських рішень?
6. Як співвідносяться інформаційне забезпечення, інформаційно-аналітична діяльність та інформаційна підтримка управління?
7. Які особливості інформаційно-аналітичного забезпечення діяльності органів безпеки та правоохоронних органів?
8. Які нормативно-правові засади регулюють інформаційну діяльність у сфері безпеки та правоохоронної діяльності?
9. Які основні вимоги висуваються до якості, достовірності, повноти та своєчасності інформації?
10. Які сучасні тенденції розвитку інформаційно-аналітичного забезпечення в умовах цифровізації та трансформації систем безпеки?

Тема 2

Джерела інформації у правоохоронній діяльності та забезпеченні безпеки

1. Які поняття, види та класифікаційні ознаки джерел інформації у сфері безпеки та правоохоронної діяльності?

2. Які основні категорії інформації використовуються в діяльності правоохоронних органів та органів безпеки?

3. Які особливості використання відкритих джерел інформації (OSINT) у правоохоронній діяльності?

4. Які можливості надають державні реєстри, офіційні бази даних та інформаційні ресурси для забезпечення безпеки?

5. Які особливості отримання та використання інформації з відомчих інформаційних систем?

6. Які основні методи пошуку, збирання та первинного опрацювання інформації?

7. Які критерії використовуються для оцінювання достовірності, актуальності та релевантності інформаційних джерел?

8. Які методи застосовуються для перевірки інформації та виявлення недостовірних відомостей і дезінформації?

9. Які правові обмеження встановлено щодо збирання, обробки, зберігання та використання інформації?

10. Які ризики виникають під час використання відкритих і відомчих джерел інформації та як забезпечується захист отриманих даних?

Тема 3

Основи безпекового, кримінального та оперативного аналізу

1. Які поняття, мета та основні завдання безпекового, кримінального й оперативного аналізу?

2. Які спільні та відмінні ознаки безпекового, кримінального й оперативного аналізу?

3. Які основні напрями та рівні здійснення аналітичної діяльності у сфері безпеки та правоохоронної діяльності?

4. Які методи збору, систематизації та аналітичного опрацювання інформації застосовуються в правоохоронній діяльності?

5. У чому полягає сутність структурного, порівняльного, ситуаційного та причинно-наслідкового аналізу?

6. Які можливості надають методи аналізу зв'язків і мереж для виявлення взаємозалежностей між особами, подіями та об'єктами?

7. Як здійснюється аналіз криміногенної обстановки та визначення основних тенденцій кримінальних загроз?

8. Які методи використовуються для виявлення закономірностей, індикаторів ризику та потенційних загроз безпеці?

9. Яке значення мають прогнозування, оцінювання ризиків та сценарний аналіз у діяльності органів безпеки й правоохоронних органів?

10. Які вимоги висуваються до обґрунтованості, об'єктивності та практичної значущості результатів аналітичної роботи?

Тема 4

Інформаційно-аналітичні системи органів безпеки та правоохоронних органів

1. Які поняття, призначення та основні функції інформаційно-аналітичних систем?

2. Які основні види та класифікаційні ознаки інформаційно-аналітичних систем?

3. Які основні компоненти інформаційно-аналітичних систем та особливості їхньої взаємодії?

4. Які інформаційні системи використовуються в діяльності органів безпеки та правоохоронних органів України?

5. Які можливості надають відомчі бази даних та інтегровані інформаційні ресурси для виконання правоохоронних завдань?

6. Які принципи організації інформаційної взаємодії та обміну даними між державними органами?

7. Які можливості застосування геоінформаційних систем (GIS) у правоохоронній діяльності та забезпеченні безпеки?

8. Які напрями використання технологій штучного інтелекту та автоматизованого аналізу даних в інформаційно-аналітичних системах?

9. Які вимоги висуваються до розмежування доступу, захисту та контролю використання інформаційних ресурсів?

10. Які основні проблеми інтеграції, сумісності та модернізації інформаційно-аналітичних систем органів безпеки й правоохоронних органів?

Тема 5

Аналітичні документи в діяльності органів безпеки та правоохоронних органів

1. Які поняття, призначення та основні функції аналітичних документів у діяльності органів безпеки та правоохоронних органів?

2. Які основні види аналітичних документів та особливості їх використання?

3. Які вимоги висуваються до структури, змісту та оформлення аналітичних документів?

4. Які особливості підготовки аналітичної довідки, інформаційного огляду та аналітичного звіту?

5. Які етапи підготовки аналітичного документа — від визначення завдання до формулювання висновків і рекомендацій?

6. Які методи систематизації, узагальнення та візуалізації інформації застосовуються під час підготовки аналітичних матеріалів?

7. Яке значення мають аргументованість, об'єктивність і перевірюваність висновків в аналітичних документах?

8. Які особливості використання статистичних даних, таблиць, графіків і схем у підготовці аналітичних матеріалів?

9. Які вимоги щодо захисту інформації та обмеження доступу враховуються під час підготовки й поширення аналітичних документів?

10. Яке значення мають аналітичні документи для інформаційного супроводу управлінських рішень та оцінювання результатів діяльності правоохоронних органів?

Тема 6

Основи спеціального зв'язку в системах безпеки та правоохоронній діяльності

1. Які поняття, призначення та основні завдання спеціального зв'язку в системах безпеки та правоохоронній діяльності?

2. Які основні принципи організації спеціального зв'язку та вимоги до його функціонування?

3. Які основні види та засоби спеціального зв'язку використовуються в системах державного управління, безпеки й оборони?

4. У чому полягають особливості урядового зв'язку та його місце в системі спеціального зв'язку?

5. Які основні завдання та функції виконує Державна служба спеціального зв'язку та захисту інформації України?

6. Яке призначення та особливості функціонування Національної системи конфіденційного зв'язку?

7. Які відмінності між відкритими, захищеними та спеціальними каналами зв'язку?

8. Які особливості застосування цифрових радіомереж стандартів DMR і TETRA у правоохоронній діяльності та забезпеченні безпеки?

9. Які вимоги висуваються до надійності, безперервності, оперативності та захищеності спеціального зв'язку?

10. Які основні проблеми розвитку й модернізації систем спеціального зв'язку в умовах сучасних безпекових загроз?

Тема 7

Технічний та криптографічний захист інформації

1. Які поняття, мета та основні завдання технічного й криптографічного захисту інформації?

2. Які основні принципи та нормативно-правові засади захисту інформації в інформаційно-комунікаційних системах?

3. Які основні загрози порушення конфіденційності, цілісності та доступності інформації?

4. Які методи та засоби технічного захисту інформації застосовуються в системах безпеки та правоохоронних органах?

5. У чому полягає сутність криптографічного захисту інформації та які завдання він вирішує?

6. Які основні види криптографічних алгоритмів і механізмів використовуються для захисту інформації?

7. Яке призначення мають електронний цифровий підпис, електронні довірчі послуги та інфраструктура відкритих ключів?

8. Які особливості захисту інформації під час її передавання каналами зв'язку та зберігання в інформаційних системах?

9. Які основні методи контролю, оцінювання та перевірки ефективності технічного й криптографічного захисту інформації?

10. Які сучасні технологічні тенденції та проблеми розвитку систем технічного й криптографічного захисту інформації?

Тема 8

Режим секретності та захист службової інформації

1. Які поняття, правові засади та основні принципи забезпечення режиму секретності в Україні?

2. Які відомості належать до державної таємниці та за якими критеріями визначається ступінь їх секретності?

3. Які основні категорії інформації з обмеженим доступом та в чому полягають відмінності між ними?

4. Які особливості правового режиму службової інформації та її відмінності від інформації, що становить державну таємницю?

5. Який порядок надання допуску та доступу до державної таємниці?

6. Які основні вимоги встановлено до обліку, зберігання, використання та пересилання матеріальних носіїв секретної інформації?

7. Які організаційні та технічні заходи забезпечують дотримання режиму секретності й захист службової інформації?

8. Які вимоги висуваються до роботи з документами та інформаційними ресурсами, що містять інформацію з обмеженим доступом?

9. Які види відповідальності передбачені за порушення законодавства про державну таємницю та захист службової інформації?

10. Які основні проблеми забезпечення режиму секретності та захисту службової інформації в умовах цифровізації й воєнного стану?

Тема 9

Кіберзагрози та інсайдерські ризики в правоохоронних органах

1. Які поняття, види та основні характеристики кіберзагроз у діяльності правоохоронних органів?

2. Які основні види кібератак та способи їх здійснення становлять загрозу інформаційним ресурсам правоохоронних органів?

3. Які особливості фішингу, соціальної інженерії, шкідливого програмного забезпечення та атак на інформаційні системи?

4. Які поняття, причини виникнення та основні різновиди інсайдерських загроз?

5. Які чинники можуть зумовлювати виникнення внутрішніх загроз інформаційній безпеці правоохоронних органів?

6. Які методи виявлення, оцінювання та попередження інсайдерських ризиків застосовуються в організаціях?

7. Яке значення мають розмежування прав доступу, автентифікація користувачів і журналювання подій для запобігання внутрішнім загрозам?

8. Які організаційні та технічні заходи застосовуються для протидії кіберзагрозам і захисту від несанкціонованого доступу?

9. Які основні етапи реагування на кіберінциденти та відновлення функціонування інформаційних систем?

10. Які особливості забезпечення кіберстійкості та протидії інсайдерським загрозам у правоохоронних органах в умовах воєнного стану?

Тема 10

Інтегроване інформаційно-аналітичне забезпечення операцій органів безпеки та оборони

1. Які поняття, призначення та основні завдання інтегрованого інформаційно-аналітичного забезпечення операцій органів безпеки та оборони?

2. Які основні принципи організації інформаційної взаємодії між органами безпеки, правоохоронними органами та складовими сектору оборони?

3. Які інформаційні потреби виникають на різних етапах підготовки, планування та проведення операцій?

4. Які джерела інформації та інформаційно-аналітичні системи використовуються для забезпечення міжвідомчої взаємодії?

5. Які методи інтеграції, узагальнення та комплексного аналізу інформації застосовуються під час підготовки операцій?

6. Яке значення мають ситуаційна обізнаність, оцінювання ризиків і прогнозування розвитку обстановки для прийняття управлінських рішень?

7. Які можливості надають геоінформаційні системи, цифрові платформи та засоби візуалізації для інформаційно-аналітичного супроводу операцій?

8. Які вимоги висуваються до захищеності інформаційного обміну, спеціального зв'язку та розмежування доступу під час проведення міжвідомчих операцій?

9. Які основні проблеми сумісності інформаційних систем, координації та обміну інформацією між органами безпеки й оборони?

10. Які перспективи розвитку інтегрованого інформаційно-аналітичного забезпечення операцій в умовах цифрової трансформації та сучасних безпекових загроз?

Технічне обладнання та/або програмне забезпечення. В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проєктор, комп'ютерна техніка та доступ до мережі Інтернет через Wi-Fi. Практичне опрацювання тем дисципліни забезпечується наявними в закладі освіти технічними засобами спеціального зв'язку та телекомунікаційним обладнанням, зокрема радіостанціями, автоматизованою телефонною станцією, засобами комутації, зразком обладнання захищеного каналу зв'язку, генераторами електроживлення, джерелами безперебійного та резервного живлення тощо. Також використовуються комп'ютерні й програмні засоби пошуку, опрацювання, аналізу та візуалізації інформації.

Форми та методи контролю. Іспит проводиться в письмовій та усній формі: до завдання входять 3 теоретичних питання. Поточний контроль, модульний контроль, контроль самостійної роботи, підсумковий контроль у формі іспиту.

Загальна підсумкова оцінка (в балах) результати поточної роботи + результати іспиту.

Таблиця розподілу балів, які отримують здобувачі вищої освіти*

	Поточний контроль знань										**Модульна контрольна робота**	**Залік****	**Загальна кількість балів**
Теми	Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 7	Тема 8	Тема 9	Тема 10	20	Відповідно до Положення про систему оцінювання результатів навчання здобувачів вищої освіти	100
Робота на семінарському занятті	5	5	5	5	5	5	5	5	5	5			
Самостійна робота	3	3	3	3	3	3	3	3	3	3			

Підсумкове	Сума балів за	Сума балів за	Модульна	Сума балів за	Загальна сума

оцінювання	семінари	самостійну роботу	контрольна робота	залік	балів
	50	30	20	**	100

*Таблиця містити інформацію про максимальні бали за кожен вид навчальної роботи здобувача вищої освіти.

*Робота на семінарському занятті оцінюється у 5 балів.

Види робіт передбачених на семінарському занятті:

- експрес-опитування;
- опитування за темою заняття;
- тест;
- виконання практичного завдання;
- розв'язання задач;
- презентації студентів.

** Самостійна робота студента передбачає підготовка до аудиторних занять шляхом опанування матеріалів лекції, вивчення базової і додаткової літератури, періодичних видань, Інтернет - джерел та судової практики, підготовка юридичних документів. Оцінюється в 3 бали.

***Модульний контроль здійснюється у вигляді *тестування*.

Студентами пропонуються тестові завдання у кількості 20 питань.

Види тестових завдань:

- З вибором однієї правильної відповіді з наведених варіантів;
- З вибором кількох правильних відповідей;

Критерії оцінювання: виконання тестових завдань – максимум 20 балів.

Оцінювання знань здійснюється відповідно до «Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП» (https://drive.google.com/file/d/1ENRncPY-dU2qLke7awVKn1OdfG88Hg8D/view).

Сума балів за всі види навчальної діяльності	Оцінка ECTS	**Оцінка за національною шкалою**	
		для екзамену	**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

Політика курсу. Вивчення навчальної дисципліни «Інформаційно-аналітичне забезпечення та спеціальний зв'язок» ґрунтується на принципах академічної доброчесності, взаємоповаги, відповідальності, систематичності навчання та активної участі здобувачів вищої освіти в освітньому процесі.

Здобувачі вищої освіти зобов'язані дотримуватися вимог освітньої програми, робочої програми навчальної дисципліни та внутрішніх нормативних документів закладу вищої освіти; своєчасно виконувати навчальні завдання, готуватися до лекційних і семінарських занять, брати участь у дискусіях, виконувати індивідуальні завдання та самостійну роботу.

Академічна доброчесність. Під час виконання письмових робіт, підготовки доповідей, презентацій, аналітичних довідок здобувачі освіти повинні самостійно формулювати висновки, належним чином зазначати використані джерела, дотримуватися правил цитування та не допускати академічного плагіату, фабрикації чи фальсифікації результатів досліджень. Використання технологій штучного інтелекту допускається відповідно до встановлених у закладі освіти правил із дотриманням вимог академічної доброчесності та належного зазначення такого використання, якщо це передбачено відповідними правилами.

Навчальна активність і відповідальність. Здобувачі освіти повинні брати активну участь у навчальних заняттях, аргументовано висловлювати власну правову позицію, аналізувати положення кримінального законодавства України, міжнародно-правові акти та судову практику, дотримуватися професійної етики й поважати думки інших учасників освітнього процесу.

Виконання навчальних завдань. Усі передбачені робочою програмою завдання, зокрема практичні кейси, контрольні роботи, завдання для самостійного опрацювання та курсова робота, виконуються у встановлені строки. У разі виникнення обставин, що перешкоджають своєчасному виконанню завдань або участі в заняттях, здобувач освіти повинен завчасно повідомити викладача та діяти відповідно до правил закладу вищої освіти.

Оцінювання навчальних досягнень. Оцінювання здійснюється на основі визначених критеріїв, з урахуванням повноти й системності знань, уміння застосовувати норми кримінального права до конкретних ситуацій, аргументувати правові висновки, аналізувати судову практику та самостійно розв'язувати професійні завдання. Здобувачі освіти мають право отримувати роз'яснення щодо критеріїв оцінювання та результатів виконаних робіт.

Комунікація та професійна етика. У взаємодії з викладачем та іншими здобувачами освіти необхідно дотримуватися норм академічної культури, коректності, толерантності й професійної етики. Обговорення проблем кримінального права має відбуватися на основі законодавства, наукових аргументів і належних джерел.

Дотримання політики курсу сприяє формуванню професійних компетентностей, розвитку критичного мислення, навичок правового аналізу та відповідального застосування кримінально-правових норм у майбутній професійній діяльності у сфері правоохоронної діяльності.

Методичне забезпечення навчальної дисципліни

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. Гриценко 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
6. Кудінов В. А., Накриш О. Є. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навчально-практичний посібник. Київ : Національна академія внутрішніх справ, 2025. 116 с. URL: https://elar.navs.edu.ua/handle/123456789/39413
7. Ланде Д. В. OSINT у кібербезпеці : навчальний посібник. Київ : Інжиніринг, 2024. 522 с.

8. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін. ; за заг. ред. Ю. Я. Бобала та І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с. URL: https://ena.lpnu.ua/handle/ntb/45626

9. Keay S., Kirby S. *Improving Intelligence Analysis in Policing*. 2nd ed. Abingdon : Routledge, 2026. 204 p.

10. Ross R., Pillitteri V. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53, Revision 5. Gaithersburg : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5

Рекомендовані джерела інформації :

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

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

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

4. 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

5. 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. Електронна бібліотека юриста, WEB кафедра права. URL: http://www.kafedr.at.ua/board/rimske_pravo.
2. Національна парламентська бібліотека України. URL: http://www.catalogue.nplu.org.
3. Офіційний веб. Сайт Міністетства юстиції України. URL: http://www.minjust.gov.ua.
4. Інформаційно – пошукова система «Нормативні акти України (НАУ)». URL: http://www. nau.ua.
5. Офіційний сайт Офісу Президента. URL: http://www.president.gov.ua/ru/content/secretariat.
6. Національна бібліотека України ім.В.І.Вернадського. URL: http://www.nbuv.gov.ua.
7. Офіційний веб-сайт Верховної Ради України. URL: http://www.rada.gov.ua
8.. Національна парламентська бібліотека України. URL: http://www.catalogue.nplu.org
9. Офіційний сайт Кабінету Міністрів України – http://www.kmu.gov.ua
10. Офіційний веб портал судової влади в Україні URL: https://court.gov.ua/
11. Єдиний реєстр судових рішень в Україні. URL: https://reyestr.court.gov.ua/
12. Prozorro: система публічних закупівель. URL: https://prozorro.gov.ua