ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"

Інститут безпеки

МАУП
Кафедра національної безпеки

Затверджую:
Завідувач кафедри національної безпеки
_____
Іван СЕРВЕЦЬКИЙ
"07" 08 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «АКТУАЛЬНІ ПИТАННЯ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Спеціальності: **262 правоохоронна діяльність**

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

Освітньої програми: **Правоохоронна діяльність**

Спеціалізація: _____

Київ МАУП 2025

Робоча програма з навчальної дисципліни «Актуальні питання стратегій кібербезпеки та інформаційної безпеки» для здобувачів вищої освіти освітньої програми «Правоохоронна діяльність» спеціальності 262 Правоохоронна діяльність:

Розробник:

Сергій Олексійович Лисенко - доктор наук з державного управління, доктор юридичних наук, професор, професор кафедри національної безпеки.

_____ Сергій ЛИСЕНКО
(підпис)

Робочу програму погоджено

Гарант освітньої програми «Правоохоронна діяльність»

_____ Олександр САВКА
(підпис)

Робочу програму розглянуто та схвалено на засіданні кафедри національної безпеки

Протокол №1 від «03» 08 2025 року

Завідувач кафедри національної безпеки

_____ Іван СЕРВЕЦЬКИЙ
(підпис)

Загальна інформація про навчальну дисципліну

Найменування показників	**Актуальні питання стратегій кібербезпеки та інформаційної безпеки**	
	очна (денна)	**заочна**
Вид дисципліни (обов'язкова чи вибіркова)	вибіркова	
Мова викладання	українська	
Загальний обсяг у кредитах ЄКТС/годинах	**3 кредита/90 год** Лекції : **20** Семінарські заняття: **14** Самостійна робота студентів: 56	
Курс	1	1
Семестр	1	1
Кількість змістових модулів	2	2
Обсяг кредитів із розподілом за семестрами	3	3
Обсяг годин, у тому числі:		
- Аудиторні	34	4
- Лекційні	20	2
- Семінарські	14	2
- Лабораторні	-	-
Самостійна робота, год	56	86
Форма семестрового контролю	залік	

Мета й завдання навчальної дисципліни

1.3 Мета навчальної дисципліни полягає у формуванні у здобувачів вищої освіти цілісного та системного розуміння актуальних питань стратегій кібербезпеки та інформаційної безпеки, засвоєнні сучасних теоретико-методологічних підходів до аналізу цифрових загроз, вивченні правових, організаційних, інституційних та управлінських механізмів забезпечення безпеки інформаційного простору й кіберпростору, а також у набутті здатності застосовувати отримані знання для оцінювання ризиків, підготовки аналітичних матеріалів, вироблення стратегічних рішень і обґрунтування напрямів удосконалення державної політики у сфері кібербезпеки та інформаційної безпеки в умовах цифрової трансформації, гібридних

загроз, інформаційного протиборства та зростання вразливостей критичної інфраструктури.

Завдання навчальної дисципліни полягають у вивченні сутності кібербезпеки та інформаційної безпеки як складових національної безпеки держави, дослідженні сучасних стратегій, концепцій і моделей захисту інформаційних ресурсів та цифрових систем, аналізі нормативно-правових засад державного регулювання у відповідній сфері, з'ясуванні повноважень і функцій основних суб'єктів забезпечення кібербезпеки та інформаційної безпеки, опануванні підходів до виявлення, оцінювання, моніторингу та прогнозування кіберзагроз і інформаційних загроз, вивченні механізмів протидії дезінформації, інформаційно-психологічним операціям, кібератакам і гібридним впливам, набутті навичок стратегічного мислення у сфері безпеки, а також формуванні вмінь застосовувати теоретичні положення і практичні інструменти для підготовки управлінських рішень, аналітичних висновків і пропозицій щодо підвищення ефективності системи кібербезпеки та інформаційної безпеки на державному, інституційному й прикладному рівнях.

Перелік компетентностей та результатів навчання, що формує дана дисципліна:

Перелік компетентностей, що формує дана дисципліна: ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Усвідомлення рівних можливостей та гендерних проблем. СК5. Здатність давати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності. СК7. Здатність ефективно здійснювати правове виховання молодших колег у процесі набуття і вдосконалення ними професійних навичок. СК11. Здатність взаємодіяти з представниками інших органів виконавчої влади та місцевого самоврядування, громадськістю з питань правоохоронної діяльності.

Перелік результатів навчання, що формує дана дисципліна. Здобувачі повинні досягти таких програмних результатів навчання: РН1. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців; зокрема, під час публічних виступів, дискусій, проведення занять. РН4. Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів. РН8. Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків. РН15. Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Програма навчальної дисципліни

Тема 1. Актуальні питання стратегій кібербезпеки та інформаційної безпеки як наукова і практична категорія

Розглядаються поняття безпеки, оборони, національної стійкості та стратегічного управління. Аналізується еволюція підходів від секторного реагування до інтегрованого безпекового управління, система суб'єктів безпеки й оборони держави, а також взаємозв'язок національної, воєнної, громадської, інформаційної та кібернетичної безпеки.

Тема 2. Теоретичні засади формування стратегій кібербезпеки та інформаційної безпеки

Розглядаються основні наукові підходи до розуміння стратегій кібербезпеки та інформаційної безпеки, їх структура, функції та місце в системі державного управління. Досліджуються принципи стратегічного планування, механізми визначення пріоритетів, цілей і завдань безпекової політики, а також роль прогнозування й оцінювання ризиків у процесі формування стратегічних рішень.

Тема 3. Нормативно-правове забезпечення кібербезпеки та інформаційної безпеки

Аналізуються правові засади регулювання відносин у сфері кібербезпеки та інформаційної безпеки, система національного законодавства, стратегічних документів і підзаконних актів. Розглядаються питання правового статусу суб'єктів забезпечення безпеки, розмежування їх компетенції, а також напрями вдосконалення нормативної бази з урахуванням сучасних викликів і міжнародних стандартів.

Тема 4. Інституційна система забезпечення кібербезпеки та інформаційної безпеки

Розглядається система державних органів, спеціальних служб, правоохоронних структур, військових формувань, органів місцевого самоврядування, підприємств, установ і організацій, залучених до забезпечення кібербезпеки та інформаційної безпеки. Аналізуються їх повноваження, форми взаємодії, координаційні механізми та проблеми інституційної узгодженості в умовах кризових і воєнних загроз.

Тема 5. Загрози у сфері кібербезпеки та інформаційної безпеки: сутність, класифікація, тенденції розвитку

Досліджуються сучасні кіберзагрози та інформаційні загрози, джерела їх виникнення, форми прояву та наслідки для держави, суспільства й особи. Аналізуються кібератаки, витоки даних, дезінформація, інформаційно-психологічні операції, втручання у функціонування критичної інфраструктури, а також гібридні впливи як складова сучасного безпекового середовища.

Тема 6. Стратегічне управління ризиками у сфері кібербезпеки та інформаційної безпеки

Розглядаються підходи до ідентифікації, оцінювання, моніторингу та мінімізації ризиків у сфері кібербезпеки та інформаційної безпеки. Висвітлюються методи аналізу вразливостей, побудови систем реагування на інциденти, забезпечення безперервності функціонування інформаційних систем, а також використання аналітичних інструментів у процесі прийняття стратегічних управлінських рішень.

Тема 7. Критична інформаційна інфраструктура як об'єкт стратегічного захисту

Аналізується поняття критичної інформаційної інфраструктури, її місце у функціонуванні держави, економіки та суспільства, а також специфіка захисту критично важливих інформаційних ресурсів і цифрових платформ. Розглядаються питання стійкості, резервування, кіберзахисту, кризового реагування та міжвідомчої координації у процесі забезпечення безпеки критичних об'єктів.

Тема 8. Протидія дезінформації та інформаційно-психологічним операціям

Розглядаються механізми реалізації інформаційно-психологічного впливу, технології маніпулювання суспільною свідомістю та засоби поширення дезінформації в цифровому середовищі. Аналізуються інструменти державної та суспільної протидії деструктивним інформаційним кампаніям, підходи до розвитку медіаграмотності, стратегічних комунікацій, інформаційної стійкості населення та захисту національного інформаційного простору.

Тема 9. Міжнародний досвід і стандарти у сфері кібербезпеки та інформаційної безпеки

Досліджуються основні міжнародні підходи до формування стратегій кібербезпеки та інформаційної безпеки, практика діяльності міжнародних організацій, міждержавного співробітництва та обміну інформацією. Аналізуються міжнародні стандарти, моделі реагування на кіберінциденти, підходи до захисту даних, цифрового суверенітету та перспективи адаптації зарубіжного досвіду до національної системи безпеки.

Тема 10. Перспективи розвитку стратегій кібербезпеки та інформаційної безпеки в умовах цифрової трансформації

Розглядаються сучасні тенденції трансформації безпекового середовища під впливом цифровізації, штучного інтелекту, автоматизації управління, розвитку хмарних технологій і розширення кіберпростору. Аналізуються перспективи вдосконалення державної політики, стратегічного планування, міжсекторальної взаємодії, кадрового забезпечення та інституційної модернізації системи кібербезпеки та інформаційної безпеки в умовах нових глобальних і національних викликів.

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
Змістовний модуль 1. Теоретико-методологічні засади стратегій кібербезпеки та інформаційної безпеки								
Тема 1. Актуальні питання стратегій кібербезпеки та інформаційної безпеки як наукова і практична категорія	8	2	1	5	9	2	2	9

Тема 2. Теоретичні засади формування стратегій кібербезпеки та інформаційної безпеки	8	2	1	5	9			9
Тема 3. Нормативно-правове забезпечення кібербезпеки та інформаційної безпеки	9	2	2	5	9			9
Тема 4. Інституційна система забезпечення кібербезпеки та інформаційної безпеки	9	2	1	6	9			9
Тема 5. Загрози у сфері кібербезпеки та інформаційної безпеки: сутність, класифікація, тенденції розвитку	10	2	2	6	9			9
Змістовий модуль 2. Прикладні та функціональні аспекти стратегій кібербезпеки та інформаційної безпеки								
Тема 6. Стратегічне управління ризиками у сфері кібербезпеки та інформаційної безпеки	9	2	1	6	9			9
Тема 7. Критична інформаційна інфраструктура як об’єкт стратегічного захисту	9	2	2	5	9			8
Тема 8. Протидія дезінформації та інформаційно-психологічним операціям	9	2	1	6	9			8
Тема 9. Міжнародний досвід і стандарти у сфері кібербезпеки та інформаційної безпеки	9	2	2	5	9			8
Тема 10. Перспективи розвитку стратегій кібербезпеки та інформаційної безпеки в умовах цифрової трансформації	10	2	1	7	9			8
Модульна контрольна робота								
Всього:	**90**	**20**	**14**	**56**	**90**	**2**	**2**	**86**
Форма контролю: залік								

Теми семінарських / практичних занять

№ сем. зан.	Назва теми	Кількість годин
1.	**Тема 1. Актуальні питання стратегій кібербезпеки та інформаційної безпеки як наукова і практична категорія.** 1. Поняття безпеки, інформаційної безпеки та кібербезпеки. 2. Місце стратегій кібербезпеки та інформаційної безпеки в системі національної безпеки держави. 3. Співвідношення понять національна безпека, інформаційна безпека, кібербезпека, цифрова стійкість. 4. Еволюція підходів до забезпечення безпеки в умовах цифровізації. 5. Кіберпростір та інформаційний простір як об'єкти державного управління. 6. Національна стійкість як основа сучасної безпекової політики. 7. Актуальні виклики у сфері інформаційної та кібернетичної безпеки. **Завдання:** Осмислити сутність стратегій кібербезпеки та інформаційної безпеки як складових державної безпекової політики, визначити їх місце в системі національної безпеки та з'ясувати їх значення в умовах цифрової трансформації й гібридних загроз. **Результат:** Розуміння здобувачами сутності стратегій кібербезпеки та інформаційної безпеки, їх ролі в системі державного управління, а також вміння визначати місце цих категорій у сучасному безпековому середовищі.	1
2.	**Тема 2. Теоретичні засади формування стратегій кібербезпеки та інформаційної безпеки.** 1. Поняття стратегії, політики, доктрини, концепції та плану. 2. Теоретичні основи стратегічного мислення у сфері безпеки. 3. Стратегічна культура та її значення для безпекової політики держави. 4. Принципи формування стратегій кібербезпеки та інформаційної безпеки. 5. Роль прогнозування та сценарного аналізу у стратегічному управлінні. 6. Стратегічна мета, пріоритети та індикатори ефективності. 7. Значення адаптивності та гнучкості в реалізації безпекових стратегій. **Завдання:** Опанувати теоретичні підходи до формування стратегій кібербезпеки та інформаційної безпеки, з'ясувати значення стратегічного мислення, культури та прогнозування в процесі вироблення управлінських рішень. **Результат:** Розуміння здобувачами змісту основних стратегічних категорій, принципів формування безпекових стратегій та вміння розмежовувати стратегічні, політичні й концептуальні рівні безпекового управління.	1
3.	**Тема 3. Нормативно-правове забезпечення кібербезпеки та інформаційної безпеки.** 1. Нормативно-правове регулювання у сфері кібербезпеки та інформаційної безпеки. 2. Законодавчі	2

	основи державної політики у сфері цифрової безпеки. 3. Стратегічні документи як інструменти правового забезпечення. 4. Повноваження суб'єктів публічного управління у цій сфері. 5. Правові режими реагування на кіберінциденти та інформаційні загрози. 6. Захист інформаційного простору та цифрових ресурсів у правовому вимірі. 7. Перспективи вдосконалення законодавства у сфері кібербезпеки. **Завдання:** Проаналізувати систему нормативно-правового забезпечення кібербезпеки та інформаційної безпеки, визначити роль законів, стратегій і підзаконних актів у формуванні механізму державного реагування на загрози. **Результат:** Розуміння здобувачами правових засад забезпечення кібербезпеки та інформаційної безпеки, а також вміння характеризувати основні напрями вдосконалення правового регулювання у цій сфері.	
4.	**Тема 4. Інституційна система забезпечення кібербезпеки та інформаційної безпеки.** 1. Поняття інституційної системи у сфері безпеки. 2. Основні суб'єкти забезпечення кібербезпеки та інформаційної безпеки. 3. Повноваження органів державної влади у сфері цифрової безпеки. 4. Механізми міжвідомчої взаємодії та координації. 5. Інституційна узгодженість як умова ефективного реагування на загрози. 6. Місце спеціалізованих центрів реагування в системі безпеки. 7. Проблеми організаційного забезпечення у сфері кібербезпеки. **Завдання:** Осмислити інституційну архітектуру системи кібербезпеки та інформаційної безпеки, з'ясувати розподіл повноважень між її суб'єктами та значення координації в умовах кризових ситуацій. **Результат:** Розуміння здобувачами інституційної побудови системи забезпечення безпеки, а також вміння визначати роль координації та взаємодії між основними суб'єктами безпекової політики.	1
5.	**Тема 5. Загрози у сфері кібербезпеки та інформаційної безпеки: сутність, класифікація, тенденції розвитку.** 1. Поняття та ознаки кіберзагроз і інформаційних загроз. 2. Основні джерела загроз у цифровому середовищі. 3. Класифікація кібератак, інформаційних атак і операцій впливу. 4. Дезінформація та інформаційно-психологічні впливи. 5. Загрози державним інформаційним ресурсам і цифровим системам. 6. Гібридні загрози в сучасному безпековому середовищі. 7. Тенденції розвитку загроз у сфері цифрової безпеки. **Завдання:** Дослідити природу сучасних кіберзагроз та інформаційних загроз, опанувати їх класифікацію та визначити тенденції розвитку в умовах технологічних змін і гібридного протиборства. **Результат:** Розуміння здобувачами сутності та видів сучасних загроз, а також вміння аналізувати їх джерела, наслідки та вплив на державу, суспільство і цифрову інфраструктуру.	2

6.	**Тема 6. Стратегічне управління ризиками у сфері кібербезпеки та інформаційної безпеки.** 1. Поняття ризику в системі кібербезпеки та інформаційної безпеки. 2. Ризик-орієнтований підхід у державному управлінні. 3. Ідентифікація загроз, вразливостей і критичних активів. 4. Аналіз ймовірності та наслідків ризиків. 5. Матриця ризиків та пріоритети реагування. 6. Моніторинг ризиків і превентивне управління. 7. Роль стратегічного аналізу у виборі управлінських рішень. **Завдання:** Опанувати зміст ризик-орієнтованого підходу, з'ясувати методику виявлення та оцінювання ризиків, а також визначити значення стратегічного аналізу для вибору пріоритетів реагування. **Результат:** Розуміння здобувачами логіки стратегічного управління ризиками та вміння застосовувати базові підходи до аналізу ризиків у сфері кібербезпеки та інформаційної безпеки.	1
7.	**Тема 7. Критична інформаційна інфраструктура як об'єкт стратегічного захисту.** 1. Поняття критичної інформаційної інфраструктури. 2. Місце критичних цифрових систем у функціонуванні держави. 3. Основні вразливості критичної інформаційної інфраструктури. 4. Загрози державним реєстрам, цифровим платформам і мережам. 5. Кіберзахист і забезпечення стійкості критичних систем. 6. Безперервність функціонування і резервування ресурсів. 7. Відновлення критичних спроможностей після інцидентів. **Завдання:** Осмислити значення критичної інформаційної інфраструктури для державної стійкості, з'ясувати основні ризики її функціонування та опанувати підходи до її стратегічного захисту. **Результат:** Розуміння здобувачами ролі критичної інформаційної інфраструктури у забезпеченні безпеки держави та вміння визначати базові напрями її захисту, стійкості й відновлення.	2
8.	**Тема 8. Протидія дезінформації та інформаційно-психологічним операціям.** 1. Дезінформація як інструмент впливу на суспільство і державу. 2. Інформаційно-психологічні операції у сучасному безпековому середовищі. 3. Наративи, контрнаративи та маніпулятивні технології. 4. Стратегічні комунікації держави як елемент інформаційної безпеки. 5. Роль медіа та цифрових платформ у поширенні дезінформації. 6. Інструменти виявлення і нейтралізації інформаційних впливів. 7. Інформаційна стійкість суспільства як умова національної безпеки. **Завдання:** Опанувати механізми дезінформаційного впливу та інформаційно-психологічних операцій, визначити роль стратегічних комунікацій і суспільної стійкості у протидії таким загрозам. **Результат:** Розуміння здобувачами природи дезінформації та інформаційно-психологічних операцій, а також	1

	вміння визначати способи протидії інформаційним кампаніям і деструктивним наративам.	
9.	**Тема 9. Міжнародний досвід і стандарти у сфері кібербезпеки та інформаційної безпеки.** 1. Міжнародні підходи до формування стратегій кібербезпеки. 2. Стандарти та принципи міжнародної співпраці у сфері цифрової безпеки. 3. Європейські практики забезпечення інформаційної безпеки. 4. Досвід міжнародних організацій у реагуванні на кіберзагрози. 5. Обмін інформацією та координація між державами. 6. Адаптація міжнародних стандартів до національної системи безпеки. 7. Значення міжнародного співробітництва для розвитку кіберстійкості. **Завдання:** Проаналізувати міжнародний досвід та стандарти у сфері кібербезпеки та інформаційної безпеки, з'ясувати можливості їх імплементації в національну практику державного управління. **Результат:** Розуміння здобувачами ролі міжнародних стандартів і кооперації у сфері цифрової безпеки, а також вміння оцінювати перспективи адаптації зарубіжного досвіду до українських умов.	2
10.	**Тема 10. Перспективи розвитку стратегій кібербезпеки та інформаційної безпеки в умовах цифрової трансформації.** 1. Цифрова трансформація як чинник зміни безпекового середовища. 2. Роль штучного інтелекту в системі кібербезпеки. 3. Автоматизація та аналітика великих даних у сфері безпеки. 4. Хмарні технології та нові виклики інформаційній безпеці. 5. Прогнозне управління та адаптивні моделі безпеки. 6. Нові технології як джерело можливостей і ризиків. 7. Компетентності фахівця майбутнього у сфері кібербезпеки та інформаційної безпеки. **Завдання:** Осмислити перспективи розвитку стратегій кібербезпеки та інформаційної безпеки в умовах цифрової трансформації, визначити роль новітніх технологій і нових управлінських підходів у забезпеченні стійкості держави. **Результат:** Розуміння здобувачами основних тенденцій трансформації стратегій кібербезпеки та інформаційної безпеки, а також вміння оцінювати потенціал і ризики нових цифрових технологій для безпекової політики.	1

Самостійна робота

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Актуальні питання стратегій кібербезпеки та інформаційної безпеки» 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.

Вимоги до написання рефератів та есе

Загальні положення:

Реферат та есе є формами самостійної роботи здобувачів вищої освіти і спрямовані на поглиблення теоретичних знань, розвиток навичок науково-правового аналізу, аргументації правових позицій, критичного мислення та академічного письма.

Під час виконання рефератів та есе здобувачі повинні дотримуватися принципів академічної доброчесності, вимог чинного законодавства України, стандартів вищої освіти та внутрішніх нормативних актів закладу вищої освіти.

Мета та навчальні завдання:

- формування здатності здійснювати самостійний аналіз доктринальних і нормативних джерел у сфері права;
- розвиток умінь формулювати та аргументовано обґрунтовувати власну правову позицію;
- набуття навичок наукового письма та коректного використання правової термінології;
- удосконалення навичок систематизації, узагальнення та критичної оцінки правової інформації.

Вимоги до змісту

Реферат

Реферат має аналітико-узагальнювальний характер і повинен:

- розкривати теоретичні підходи до обраної правової проблеми;
- містити аналіз норм законодавства, практики Європейського суду з прав людини (за наявності);
- відображати сучасні наукові позиції українських та зарубіжних дослідників;
- завершуватися обґрунтованими висновками.

Структура реферату:

1. Титульна сторінка
2. Зміст
3. Вступ (обґрунтування актуальності, мета і завдання)
4. Основна частина (2–3 логічно пов’язані розділи)
5. Висновки
6. Список використаних джерел

Есе

Есе має аналітично-дискусійний характер і спрямоване на виклад та обґрунтування власної позиції здобувача щодо конкретної правової проблеми.

Есе повинно:

- містити чітко сформульовану авторську правову позицію;
- демонструвати здатність до критичного аналізу правових явищ;
- містити аргументацію з посиланням на нормативні акти, доктрину та судову практику;
- відображати логічну цілісність і самостійність мислення.

Рекомендована структура есе:

1. Вступ (постановка проблеми)
2. Основна частина (аргументація позиції, аналіз альтернативних підходів)
3. Висновки (узагальнення та власні висновки)

Вимоги до обсягу:

- Реферат – 7–15 сторінок друкованого тексту
- Есе – 4–8 сторінок друкованого тексту

(без урахування титульної сторінки та списку використаних джерел)

Вимоги до оформлення:

- формат сторінки – А4;
- шрифт – Times New Roman;
- розмір шрифту – 14;
- міжрядковий інтервал – 1,5;
- поля: ліве – 30 мм, праве – 15 мм, верхнє і нижнє – 20 мм;
- нумерація сторінок – арабськими цифрами (з другої сторінки);
- абзацний відступ – 1,25 см.

Посилання на джерела оформлюються відповідно до чинних національних стандартів бібліографічного опису (ДСТУ 8302:2015).

Вимоги до джерельної бази:

Кількість використаних джерел:

- реферат – не менше 10 джерел;
- есе – не менше 5 джерел.

До джерел належать:

- Конституція України;
- закони та підзаконні нормативно-правові акти;
- рішення Конституційного Суду України;
- практика Європейського суду з прав людини;
- наукові монографії, статті фахових видань;
- офіційні міжнародні документи.

Академічна доброчесність:

Робота повинна бути виконана самостійно.

Не допускаються:

- плагіат, використання програмних засобів штучного інтелекту;
- некоректне цитування;
- використання недостовірних або неперевірених джерел.

У разі виявлення порушень принципів академічної доброчесності робота не зараховується та підлягає доопрацюванню відповідно до внутрішніх положень ПрАТ «ВНЗ «МАУП».

Зміст завдань для самостійної роботи здобувача (СРЗ)

№ п/п	Зміст самостійної роботи здобувача вищої освіти	Форми контролю СРЗ
1	**Тема 1. Актуальні питання стратегій кібербезпеки та інформаційної безпеки як наукова і практична категорія** Підготувати короткий аналітичний опис сутності стратегій кібербезпеки та інформаційної безпеки, визначивши їх місце в системі державного управління та взаємозв'язок із національною стійкістю, оборонною політикою й інформаційним суверенітетом держави. Скласти глосарій із 20 ключових термінів: кібербезпека, інформаційна безпека, стратегія, державне управління, національна стійкість, інформаційний простір, кіберпростір, загроза, виклик, небезпека, вразливість, ризик, безпекове середовище, суб'єкт безпеки, цифрова інфраструктура, стратегічне рішення, державна політика, критична система, інформаційний вплив, стійкість.	Презентація результатів
2	**Тема 2. Теоретичні засади формування стратегій кібербезпеки та інформаційної безпеки** Підготувати короткий текстовий матеріал про роль стратегічного мислення, стратегічного планування та стратегічної культури у формуванні державних рішень у сфері кібербезпеки та інформаційної безпеки. Скласти глосарій із 20 ключових термінів: стратегія, політика, доктрина, концепція, план, стратегічне мислення, стратегічна культура, планування, прогнозування, сценарій, адаптація, пріоритет, стратегічна ціль, середовище безпеки, управлінська гнучкість, рішення, модель безпеки, аналітика, реалізація, оцінювання.	Презентація результатів
3	**Тема 3. Нормативно-правове забезпечення кібербезпеки та інформаційної безпеки** Підготувати короткий аналітичний опис системи нормативно-правового регулювання у сфері кібербезпеки та інформаційної безпеки, визначивши місце законів, стратегій, концепцій і підзаконних актів у механізмі забезпечення безпеки. Скласти глосарій із 20 ключових термінів: нормативно-правове регулювання, законодавство, стратегічний документ, концепція, правова норма, компетенція, повноваження, суб'єкт забезпечення безпеки, державна політика, правовий механізм, регулювання, інституція, законність, підзаконний акт, правовий режим, відповідальність,	Презентація результатів

	координація, адміністративний механізм, правове забезпечення, безпекова політика.	
4	**Тема 4. Інституційна система забезпечення кібербезпеки та інформаційної безпеки** Підготувати короткий аналітичний опис інституційної системи забезпечення кібербезпеки та інформаційної безпеки, визначивши її структуру, розподіл повноважень та механізми координації між основними суб'єктами. Скласти глосарій із 20 ключових термінів: інституційна система, суб'єкт безпеки, координація, міжвідомча взаємодія, державний орган, компетенція, повноваження, управлінська система, сектор безпеки, кібербезпекова структура, інформаційна політика, контроль, підзвітність, ієрархія, інституційна узгодженість, функція, управлінський механізм, центр реагування, міжсекторальна взаємодія, архітектура безпеки.	Презентація результатів
5	**Тема 5. Загрози у сфері кібербезпеки та інформаційної безпеки: сутність, класифікація, тенденції розвитку** Підготувати короткий аналітичний опис сучасних кіберзагроз та інформаційних загроз, визначивши їх джерела, форми прояву та наслідки для держави, суспільства і цифрових систем. Скласти глосарій із 20 ключових термінів: кіберзагроза, інформаційна загроза, кібератака, дезінформація, інформаційно-психологічний вплив, шкідливе програмне забезпечення, фішинг, витік даних, маніпуляція, ворожий наратив, кіберінцидент, вразливість, цифровий ризик, загроза критичній інфраструктурі, дестабілізація, інформаційна атака, операція впливу, кібероборона, захист даних, загрозове середовище.	Презентація результатів
6	**Тема 6. Стратегічне управління ризиками у сфері кібербезпеки та інформаційної безпеки** Підготувати короткий аналітичний опис risk-based approach у сфері кібербезпеки та інформаційної безпеки з визначенням етапів аналізу ризиків, вразливостей і механізмів вибору пріоритетів реагування. Скласти глосарій із 20 ключових термінів: ризик, загроза, виклик, небезпека, вразливість, ризик-орієнтований підхід, аналіз ризику, карта ризиків, матриця ризиків, сценарне прогнозування, ранжування, критичний ризик, наслідок, ймовірність, пріоритет реагування, моніторинг ризику, стратегічний ризик, управління ризиками, стійкість, превенція.	Презентація результатів
7	**Тема 7. Критична інформаційна інфраструктура як об'єкт стратегічного захисту** Підготувати короткий текстовий матеріал про значення критичної інформаційної інфраструктури для функціонування держави, визначивши основні вразливості та механізми забезпечення її стійкості й відновлення після	Презентація результатів

	інцидентів. Скласти глосарій із 20 ключових термінів: критична інформаційна інфраструктура, критична система, цифровий сервіс, державний реєстр, вразливість, резервування, кіберзахист, стійкість, безперервність функціонування, відновлення, інформаційний ресурс, мережа, інцидент, доступність, цілісність, конфіденційність, критичний об’єкт, захист інфраструктури, технічна стійкість, функціональна спроможність.	
8	**Тема 8. Протидія дезінформації та інформаційно-психологічним операціям** Підготувати короткий аналітичний опис значення інформаційної безпеки та стратегічних комунікацій у протидії дезінформації, маніпуляціям та інформаційно-психологічним впливам. Скласти глосарій із 20 ключових термінів: інформаційна безпека, стратегічні комунікації, дезінформація, інформаційна атака, операція впливу, інформаційно-психологічна кампанія, репутаційна безпека, державна комунікація, інформаційний простір, наратив, контрнаратив, кризова комунікація, медіасередовище, публічне повідомлення, моніторинг, верифікація, інформаційна стійкість, суспільна довіра, комунікаційна стратегія, реагування.	Презентація результатів
9	**Тема 9. Міжнародний досвід і стандарти у сфері кібербезпеки та інформаційної безпеки** Підготувати короткий матеріал про міжнародні підходи до забезпечення кібербезпеки та інформаційної безпеки, визначивши роль міжнародних організацій, стандартів, кооперації та обміну практиками. Скласти глосарій із 20 ключових термінів: міжнародний стандарт, міжнародне співробітництво, кіберполітика, цифровий суверенітет, міжнародна організація, координація, кіберінцидент, реагування, стандартизація, інтероперабельність, захист даних, міжнародна безпека, кібердипломатія, спільна політика, транскордонна загроза, обмін інформацією, міжнародна практика, адаптація досвіду, цифрова стійкість, колективна безпека.	Презентація результатів
10	**Тема 10. Перспективи розвитку стратегій кібербезпеки та інформаційної безпеки в умовах цифрової трансформації** Підготувати короткий аналітичний опис перспектив розвитку стратегій кібербезпеки та інформаційної безпеки в умовах цифрової трансформації, визначивши роль штучного інтелекту, автоматизації, великих даних та прогнозного управління. Скласти глосарій із 20 ключових термінів: цифрова трансформація, штучний інтелект, автоматизація, великі дані, прогнозне управління, адаптивна система, цифрова аналітика, кіберстійкість, інновація, технологічний ризик, цифровий актив, data-driven governance, алгоритм, автономна система, хмарна	Презентація результатів

	технологія, цифрова безпека, технологізація, управлінське рішення, аналітична модель, майбутні загрози.	
	Усього за навчальною дисципліною	

Індивідуальні завдання

Індивідуальна робота здобувачів освіти включає в себе: підготовку наукових доповідей та есе; розробку порівняльних схем, таблиць; участь в роботі наукових конференцій та гуртків; опублікування тез наукових доповідей і статей.

Зазначений вище перелік видів індивідуальної роботи не є вичерпним та носить гнучкий характер. Вибір конкретної теми й виду індивідуальної роботи студента відбувається на початку навчального семестру за погодженням з завідувачем профільної кафедри або його заступником. Організацію, контроль та оцінку якості її виконання здійснює викладач та/або науковий керівник, закріплений кафедрою за академічною групою, до якого студентам потрібно звертатися в разі виникнення запитань. Результати виконаної індивідуальної роботи надаються студентом викладачу у паперовому або електронному вигляді до початку навчальної сесії.

Індивідуальні завдання є складовою частиною організації освітнього процесу з навчальної дисципліни та спрямовані на формування і розвиток у здобувачів вищої освіти навичок самостійної, дослідницької й аналітичної діяльності. Їх виконання забезпечує поглиблення та систематизацію теоретичних знань, отриманих під час аудиторних занять, а також сприяє набуттю практичних умінь застосування положень конституційно-правової науки для розв’язання актуальних професійних завдань.

Виконання індивідуальних завдань здійснюється здобувачем вищої освіти самостійно із можливістю отримання консультаційної підтримки з боку науково-педагогічного працівника. Консультації спрямовані на уточнення структури роботи, визначення джерельної бази, формування методологічних підходів та коригування змістового наповнення завдання. У разі виконання завдань комплексного або міждисциплінарного характеру допускається їх підготовка групою здобувачів із розподілом обов’язків та визначенням індивідуального внеску кожного учасника.

Консультація є формою своєрідного інтерв’ю викладача, на якому він відповідає на ті чи інші запитання студентів щодо проблемних або ж спірних аспектів навчального матеріалу. Консультації можуть бути як індивідуальними, так і груповими (передзаліковими). Короткі індивідуальні консультації з усіх питань навчального курсу, які цікавлять студентів, можна отримати як перед початком, так і після лекції чи практичного заняття, а в певних випадках і під час таких занять, а більш розгорнуті відповіді – на кафедрі згідно із затвердженим графіком чергувань викладача по кафедрі, у тому числі і з використанням засобів відеозв’язку, а також на груповій консультації, яка зазвичай проводиться перед іспитом або заліком.

З дисципліни «Актуальні питання стратегій кібербезпеки та інформаційної безпеки» індивідуальні завдання можуть реалізовуватися у різних формах, зокрема: підготовка та публікація наукової статті, підготовка доповіді й участь у роботі

наукової конференції, розроблення мультимедійної презентації, аналітичного огляду судової практики, порівняльно-правового дослідження тощо. Обрана форма виконання повинна відповідати змісту дисципліни та сприяти досягненню визначених програмних результатів навчання.

Тематика завдань формується з урахуванням сучасних тенденцій розвитку права, практики його застосування та наукових підходів до вирішення проблемних питань галузі.

Мінімальні та максимальні строки видачі, виконання та захисту індивідуальних завдань доводяться до відома здобувачів освіти викладачем на початку семестру. Дотримання визначених термінів є обов'язковою умовою належного оцінювання результатів навчання.

Оцінювання результатів виконання індивідуальних завдань здійснюється відповідно до встановлених критеріїв та передбачає нарахування додаткових (бонусних) балів: за підготовку та публікацію наукової статті – до 12 балів; за виступ із доповіддю на науковій конференції – до 8 балів; за підготовку та представлення презентації – до 10 балів. Конкретна кількість балів визначається з урахуванням якості змісту, рівня наукової аргументації, самостійності виконання та дотримання встановлених вимог до оформлення результатів роботи.

Підготовка тематичної презентації (тема, терміни тощо), а також виконання інших видів індивідуальних завдань погоджується здобувачем освіти із викладачем.

Критерії та умови підготовки, оформлення та публікації наукових матеріалів (статей, тез, доповідей) визначаються безпосередньо оргкомітетом наукової конференції, редакційною колегією видання або установою-організатором.

Умови підготовки, оформлення та критерії оцінювання презентацій визначаються цією програмою (кафедрою).

Індивідуальна робота також студентів включає в себе: підготовку наукових доповідей та есе; розробку порівняльних схем, таблиць; участь в роботі наукових конференцій та гуртків; опублікування тез наукових доповідей і статей.

Зазначений вище перелік видів індивідуальної роботи не є вичерпним та носить гнучкий характер. Вибір конкретної теми й виду індивідуальної роботи студента відбувається на початку навчального семестру за погодженням з завідувачем профільної кафедри або його заступником. Організацію, контроль та оцінку якості її виконання здійснює викладач та/або науковий керівник, закріплений кафедрою за академічною групою, до якого студентам потрібно звертатися в разі виникнення запитань. Результати виконаної індивідуальної роботи надаються студентом викладачу у паперовому або електронному вигляді до початку навчальної сесії.

Есе являє собою самостійно виконаний студентом науковий, критичний чи інший нарис, який вирізняється оригінальністю суджень і вишуканістю форми. Тема есе погоджується з викладачем, виконується письмово обсягом 3-5 сторінок.

Завершальним етапом вивчення навчальної дисципліни є залік, який відбувається в усній чи письмовій формі.

Методи навчання

Методи навчання становлять систему впорядкованих способів спільної діяльності науково-педагогічного працівника та здобувачів вищої освіти, спрямованих на досягнення визначених програмних результатів навчання, формування загальних і фахових компетентностей, а також ефективне розв'язання навчально-виховних завдань. Реалізація методів навчання здійснюється через сукупність дидактичних прийомів, організаційних форм та відповідних засобів освітньої діяльності.

Під час викладання та опанування навчальної дисципліни «Актуальні питання стратегій кібербезпеки та інформаційної безпеки» застосовується комплекс методів, що забезпечують поєднання теоретичної підготовки з практичною спрямованістю навчання.

1. Словесні методи

До словесних методів належать способи вербального викладення та опрацювання навчального матеріалу, зокрема: розповідь, пояснення, лекція, бесіда, дискусія. Зазначені методи передбачають описове розкриття змісту тем, тлумачення сутності правових явищ, категорій і процесів, аналіз нормативно-правових положень, а також перевірку рівня самостійного засвоєння матеріалу здобувачами освіти. Їх використання сприяє формуванню системного бачення проблем правового регулювання та розвитку навичок професійної аргументації.

2. Наочні методи

Наочні методи передбачають використання візуальних засобів навчання з метою підвищення ефективності сприйняття та осмислення інформації. У межах дисципліни застосовуються демонстрація схем, таблиць, структурно-логічних моделей, діаграм, ілюстративних матеріалів, відеофрагментів та інших засобів візуалізації. Використання наочності забезпечує кращу систематизацію складних правових конструкцій, сприяє формуванню аналітичного мислення та полегшує засвоєння теоретичних положень.

3. Практичні методи

Практичні методи орієнтовані на формування професійних умінь і навичок, зокрема здатності оперувати конституційно-правовими категоріями, аналізувати та застосовувати норми права, вирішувати практичні ситуації у сфері публічно-правових відносин. Реалізація зазначених методів здійснюється під час семінарських занять, виконання індивідуальних завдань, розв'язання кейсів, аналізу судової практики та моделювання правових ситуацій.

Практична складова навчання спрямована на інтеграцію теоретичних знань із реальними правозастосовними процесами, що забезпечує професійну орієнтацію здобувачів освіти.

Методи за рівнем самостійної пізнавальної діяльності

З метою активізації інтелектуальної діяльності здобувачів вищої освіти у процесі навчання застосовуються також методи, диференційовані за рівнем самостійності мислення:

- *метод проблемного викладу,* що передбачає постановку наукової або практичної проблеми та послідовне розкриття шляхів її вирішення;

- *частково-пошуковий (евристичний) метод*, спрямований на залучення здобувачів до самостійного пошуку окремих елементів розв'язання поставленого завдання;
- *дослідницький метод,* який передбачає виконання самостійних наукових досліджень, аналіз правових джерел, формулювання власних висновків і пропозицій.

Комплексне поєднання зазначених методів забезпечує належний рівень теоретичної підготовки, розвиток критичного мислення та формування стійких професійних компетентностей у сфері захисту прав людини.

Методи та форми контролю, критерії оцінювання результатів навчання. Розподіл балів, які отримують здобувачі освіти

Методи контролю є сукупністю способів діагностичної діяльності, спрямованих на забезпечення зворотного зв'язку в освітньому процесі та визначення рівня досягнення програмних результатів навчання. Їх застосування дає можливість отримати об'єктивні дані щодо успішності засвоєння навчального матеріалу, результативності організації навчального процесу та сформованості у здобувачів вищої освіти відповідних компетентностей.

Контрольні заходи покликані встановити відповідність рівня набутих знань, умінь і практичних навичок вимогам стандартів вищої освіти, освітньо-професійної програми та робочої програми навчальної дисципліни. Оцінювання здійснюється з урахуванням принципів системності, об'єктивності, прозорості та академічної доброчесності.

Самоконтроль

Самоконтроль є важливим елементом навчальної діяльності та спрямований на формування здатності здобувачів освіти до самооцінювання рівня засвоєння навчального матеріалу. Він передбачає самостійне виконання тестових завдань, аналіз правильності розв'язання практичних ситуацій, перевірку конспектів, підготовку до семінарських занять та інших форм роботи. Розвиток навичок самоконтролю сприяє підвищенню відповідальності здобувачів за результати власного навчання.

Кафедральний контроль

Кафедральний контроль здійснюється з метою моніторингу якості підготовки здобувачів вищої освіти з навчальної дисципліни на різних етапах її вивчення. Він може реалізовуватися у формі:

- поточного контролю;
- рубіжного контролю;
- підсумкового семестрового контролю.

Такий підхід забезпечує поетапне відстеження динаміки навчальних досягнень та своєчасне коригування освітнього процесу.

Види контролю результатів навчання

В освітньому процесі застосовуються такі основні види контролю:

- поточний контроль протягом семестру;
- виконання та захист контрольних робіт, передбачених навчальним планом;

- приймання та оцінювання індивідуальних завдань;
- підсумковий семестровий контроль.

Поточний контроль здійснюється під час усіх видів аудиторних занять упродовж семестру. Його формами можуть бути усне опитування, письмові роботи, тестування, колоквіуми, аналіз практичних ситуацій, виступи здобувачів під час обговорення питань на семінарських заняттях тощо. Результати поточного оцінювання доводяться до відома здобувачів своєчасно та в установленому порядку.

Можливості поточного контролю є надзвичайно широкими: мотивація навчання, стимулювання навчально-пізнавальної діяльності, диференційований підхід до навчання, індивідуалізація навчання тощо.

Форми участі здобувачів вищої освіти у навчальному процесі, які підлягають поточному контролю:

-виступ з основного питання;

-усна доповідь;

- доповнення, запитання до того, хто відповідає;

- систематичність роботи на семінарських заняттях, активність під час обговорення питань;

- участь у дискусіях, інтерактивних формах організації заняття;

- аналіз законодавства та монографічної літератури;

- письмові завдання (тестові, контрольні, творчі роботи, реферати тощо);

- підготовка тез, конспектів навчальних або наукових текстів;

- самостійне опрацювання тем;

Методи поточного контролю: усний контроль (опитування, бесіда, доповідь, повідомлення тощо); письмовий контроль (контрольна робота, реферат, виклад матеріалу на задану тему в письмовій формі тощо); комбінований контроль; презентація самостійної/індивідуальної роботи; спостереження як метод контролю; тестовий контроль (тести закритої форми: тест-альтернатива, тест-відповідність); проблемні ситуації, метод самоконтролю та самооцінки; оцінювання кейс-завдань.

Система оцінювання та вимоги.

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 умов визначених Положенням про систему оцінювання результатів навчання здобувачів вищої освіти “ПрАт”ВНЗ”МАУП”	100
Робота на семінарському занятті	7		7		6	6	6	6	6	6			
Самостійна робота	3	3	3	3	3	3	3	3	3	3			

*Робота на семінарському занятті оцінюється у 6-7 балів.

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

Під час оцінювання засвоєння кожної теми за поточну навчальну діяльність здобувачу освіти виставляють оцінки з урахуванням затверджених критеріїв оцінювання для відповідної дисципліни.

Критерії оцінювання результатів навчання здобувачів освіти та розподіл балів, які вони отримують, регламентуються «Положенням про систему оцінювання результатів навчання здобувачів вищої освіти у «Приватному акціонерному товаристві «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» (https://maup.com.ua/assets/files/yakist/studcentr/polozhennya-pro-sistemu-ocinyuvannya-rezultativ-navchannya-zdobuvachiv-vishhoi-osviti.pdf).

Модульний контроль проводиться на останньому занятті модуля у письмовій формі, у вигляді тестування.

Підсумковий семестровий контроль з навчальної дисципліни «Актуальні проблеми конституційного права України» є обов'язковою формою оцінювання результатів навчання здобувача вищої освіти. Він проводиться в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни.

Підсумковий контроль проводиться у формі **заліку** (письмово). Здобувача освіти допускають до семестрового контролю за умови виконання ним усіх видів робіт.

Семестровий контроль у формі заліку передбачає, що підсумкова оцінка з дисципліни визначається як сума (проста або зважена) балів за змістовими модулями. Залік виставляється за результатами роботи здобувача освіти впродовж усього семестру. Рейтингова оцінка здобувача освіти складається з балів, отриманих здобувачем за результатами заходів поточного контролю, заохочувальних балів.

Здобувачі освіти, які виконали всі умови допуску до заліку та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань.

**Зі здобувачами, які виконали всі умови допуску до заліку та мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить підсумковий семестровий контроль у вигляді заліку.

Для заочної форми навчання залік є обов'язковою складовою підсумкового оцінювання.

Оцінювання додаткових (індивідуальних) видів навчальної діяльності. 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.

Для оцінювання результатів навчання здобувача вищої освіти впродовж семестру застосовується 100-бальна, національна та шкала ЄКТС оцінювання.

Шкала підсумкового оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	**Оцінка ECT8**	**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

Ресурсне забезпечення навчальної дисципліни

В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення лекційних та семінарських занять з елементам презентації. Вивчення окремих тем і виконання практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

Орієнтовний перелік питань для комплексного контролю:

1. Розкрийте сутність стратегічного управління у сфері безпеки та оборони.
2. Визначте місце стратегічного управління в системі державного управління.
3. Охарактеризуйте поняття безпеки та оборони у сучасному розумінні.
4. Розкрийте зміст поняття національної стійкості.
5. У чому полягає зв'язок між безпекою і обороною держави.
6. Назвіть основні суб'єкти системи безпеки і оборони держави.
7. У чому полягає взаємозв'язок воєнної, громадської, інформаційної та кібернетичної безпеки.
8. Охарактеризуйте еволюцію підходів від секторного реагування до інтегрованого безпекового управління.
9. Назвіть основні принципи стратегічного управління у сфері безпеки та оборони.
10. Чому стратегічне управління є необхідним у сучасному безпековому середовищі.
11. Розкрийте сутність стратегічного мислення у сфері безпеки.
12. У чому полягає відмінність між стратегією, політикою, доктриною, концепцією і планом.
13. Охарактеризуйте вплив невизначеності на стратегічні рішення.
14. Що таке туман війни і як він впливає на безпекове управління.
15. Розкрийте зміст поняття багатодоменності у сфері безпеки.
16. Охарактеризуйте стратегічну культуру держави.
17. Назвіть основні школи стратегічного мислення.
18. У чому полягає значення стратегічної культури безпекових інституцій.
19. Поясніть роль стратегічних помилок у розвитку безпекових криз.
20. Чому швидкість прийняття рішень має стратегічне значення.
21. Розкрийте сутність архітектури системи безпеки й оборони держави.
22. Назвіть основні елементи сектору безпеки і оборони.
23. Охарактеризуйте розподіл повноважень між воєнними і правоохоронними структурами.
24. Яке місце займають розвідувальні органи в системі безпеки держави.
25. Охарактеризуйте роль кібербезпекових структур у безпековому секторі.
26. У чому полягає значення міжвідомчої координації.
27. Розкрийте сутність демократичного цивільного контролю.
28. Поясніть роль інституційної узгодженості у функціонуванні сектору безпеки і оборони.
29. Чому система безпеки повинна розглядатися як керована архітектура.
30. У чому полягає значення підзвітності суб'єктів безпеки.
31. Розкрийте сутність ризик-орієнтованого управління у сфері безпеки та оборони.
32. Охарактеризуйте поняття загрози, виклику, небезпеки і вразливості.
33. Назвіть етапи стратегічного аналізу ризиків.
34. У чому полягає значення ідентифікації вразливостей.
35. Охарактеризуйте матрицю ризиків як інструмент стратегічного управління.
36. Розкрийте сутність сценарного прогнозування.
37. У чому полягає значення ранжування безпекових пріоритетів.
38. Яку роль відіграє карта ризиків у роботі державного органу.

39. У чому полягає відмінність між прийнятним і критичним ризиком.
40. Чому ризик-орієнтований підхід є необхідним для сучасної безпекової політики.
41. Розкрийте сутність стратегічного планування у сфері безпеки та оборони.
42. Назвіть основні етапи циклу стратегічного планування.
43. Охарактеризуйте значення цілей і пріоритетів у стратегічному плануванні.
44. У чому полягає роль ресурсних меж у безпековому плануванні.
45. Яке значення мають показники досягнення стратегічних цілей.
46. Розкрийте зміст документів стратегічного рівня у сфері безпеки та оборони.
47. У чому полягає значення узгодження довгострокового і кризового планування.
48. Чому стратегічний документ не може бути лише формальним актом.
49. Охарактеризуйте взаємозв'язок планування та реалізації безпекової політики.
50. Які чинники впливають на ефективність стратегічного планування.
51. Розкрийте сутність гібридних загроз.
52. Охарактеризуйте багатодоменне безпекове середовище.
53. У чому полягає поєднання воєнних, інформаційних, економічних і кібернетичних впливів.
54. Назвіть основні механізми державної протидії гібридним впливам.
55. Охарактеризуйте інформаційний простір як поле стратегічного суперництва.
56. Розкрийте сутність стратегічних комунікацій держави.
57. У чому полягає роль протидії дезінформації в системі національної безпеки.
58. Охарактеризуйте операції впливу та інформаційно-психологічні кампанії.
59. Яке значення має репутаційна безпека державних інституцій.
60. Чому інформаційна безпека є стратегічним напрямом державної політики.
61. Розкрийте сутність кібербезпеки як домену безпеки й оборони.
62. Охарактеризуйте поняття кіберстійкості.
63. У чому полягає зміст кіберстримування, кіберзахисту та кіберреагування.
64. Яке значення має захист державних інформаційних ресурсів.
65. Охарактеризуйте підходи Zero Trust, SOC і SIEM у державному секторі.
66. Розкрийте значення управління кіберінцидентами.
67. Яку роль відіграє розвідка у підготовці стратегічних рішень.
68. Охарактеризуйте місце контррозвідки в системі безпекової аналітики.
69. У чому полягає значення OSINT у сучасній системі безпеки та оборони.
70. Розкрийте сутність стратегічної аналітики в роботі суб'єкта ухвалення рішень.
71. Охарактеризуйте кризове управління у сфері безпеки та оборони.
72. Розкрийте сутність національної стійкості як управлінської категорії.
73. У чому полягає значення безперервності функціонування державних інституцій.
74. Охарактеризуйте роль кризових штабів і координаційних центрів.
75. Назвіть основні засади резервування ресурсів та відновлення спроможностей.
76. Розкрийте сутність критичної інфраструктури держави.
77. Охарактеризуйте основні уразливості критичної інфраструктури.
78. У чому полягає значення безпеки ланцюгів постачання.
79. Розкрийте роль управління ресурсами в оборонному плануванні.
80. Охарактеризуйте поняття оборонних спроможностей.
81. У чому полягає значення бюджетів, закупівель і резервів у сфері оборони.
82. Розкрийте роль оборонно-промислової бази в безпековій політиці держави.

83. Охарактеризуйте людський капітал як чинник безпеки й оборони.
84. У чому полягає значення кадрової безпеки у секторі безпеки і оборони.
85. Розкрийте роль професійної доброчесності та стресостійкості кадрів.
86. Охарактеризуйте лідерство в умовах невизначеності та кризи.
87. Розкрийте значення правового забезпечення стратегічного управління.
88. У чому полягає роль захисту прав людини у безпековій діяльності.
89. Охарактеризуйте етичні межі стратегічних рішень у сфері безпеки та оборони.
90. Визначте основні тенденції розвитку стратегічного управління у сфері безпеки та оборони в умовах технологізації.

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:

Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с. URL: https://niss.gov.ua/sites/default/files/2011-07/Gorbulin_Kachynsky-e2dd0.pdf

Саганюк Ф. В., Фролов В. С., Павленко В. І. та ін. Сектор безпеки і оборони України: стратегічне керівництво та військове управління : монографія / за ред. І. С. Руснака. Київ : ЦЗ МО та ГШ ЗС України, 2018. 230 с. URL: https://nuou.org.ua/assets/monography/monog-sbou.pdf

Руснак І. С. та ін. Оборонний огляд: український вимір 2014–2018 : монографія. Київ : НУОУ, 2018. URL: https://nuou.org.ua/u/stru/centers/cvsd/ord/scientific-works.html

Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : вибрані наукові праці. Київ : НІСД, 2016. 528 с. URL: https://niss.gov.ua/sites/default/files/2017-01/Vlasuk-fin-99d56.pdf

Резнікова О. О. Розробка стратегії національної безпеки з урахуванням принципів національної стійкості. Стратегічна панорама. 2018. № 2. С. 29–35. URL: https://niss-panorama.com/index.php/journal/article/view/32

Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с. URL: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf

Резнікова О. О., Войтовський К. Є., Лепіхов А. В. Національна стійкість у регіональному вимірі : аналітична доповідь. Київ : НІСД, 2021. URL: https://niss.gov.ua/sites/default/files/2021-02/dopovid-natsionalna-stiykist-na-regionalnomu-rivni.pdf

Малишев О. В., Малишева Н. Р., Калмиков В. Г., Левчук О. В. Оборонне планування на основі спроможностей в Україні: поточний стан і перспективи. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2020. № 3(70). С. 54–61. URL: https://znp-cvsd.nuou.org.ua/article/view/223827

Дєнєжкін М. М., Наливайко А. Д., Поляєв А. І. Особливості оборонного планування у державах-членах НАТО на основі спроможностей. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2017. № 2. С. 34–38. URL: https://znp-cvsd.nuou.org.ua/article/view/125129

Полевий В. Оборонне планування у сфері стратегічних комунікацій сил оборони України на основі пріоритетних завдань та на основі спроможностей. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2023. № 2(78). С. 68–73. URL: https://znp-cvsd.nuou.org.ua/article/view/290266

Полевий В. Напрями розвитку спроможностей сил оборони України у сфері стратегічних комунікацій. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2024. URL: https://znp-cvsd.nuou.org.ua/article/view/305328

Сальнікова О. Ф., Іващенко А. М., Сівоха І. М. Застосування рефлексивного управління в стратегічних комунікаціях для протидії загрозам гібридного характеру. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2019. № 3(67). С. 16–22. URL: https://znp-cvsd.nuou.org.ua/article/view/196649

Вербицька А. М., Савченко В. А., Дзюба Т. М., Кацалап В. О. Система стратегічних комунікацій Міністерства оборони України та Збройних Сил України. Наука і оборона. 2017. № 1. С. 34–39. URL: https://znp-cvsd.nuou.org.ua/article/download/234021/232667/535345

Семененко В. М. Культура стратегічних комунікацій як основа таргетингу цільових аудиторій. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2021. № 2. URL: https://znp-cvsd.nuou.org.ua/article/view/234021

Федієнко О. П. Міжнародні стандарти оцінки кіберстійкості. Інформація і право. 2024. № 3(50). С. 124–135. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2024_3_14.pdf

Поляков О. М. Міжнародна взаємодія у сфері кібербезпеки: сучасні підходи до посилення захисту кіберпростору. Інформація і право. 2021. № 2. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2021_2_17.pdf

Мануілов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури: організаційно-правовий аспект. Інформація і право. 2023. № 1. URL: https://jnas.nbuv.gov.ua/j-pdf/Infpr_2023_1_15.pdf

Developing the critical infrastructure protection system in Ukraine : monograph / ed. by D. D. Biryukov, S. I. Kondratov. Kyiv : NISS, 2017. URL: https://niss.gov.ua/publikacii/monografii/developing-critical-infrastructure-protection-system-ukraine-monografiya

Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури в Україні : аналітична доповідь / за заг. ред. Д. Д. Бирюкова. Київ : НІСД, 2019. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

Державна система захисту критичної інфраструктури в Україні: актуальні проблеми організації та функціонування : аналітична доповідь. Київ : НІСД, 2020. URL: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastructury_0.pdf

Інформаційні ресурси:

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