

**ПРАТ «ВНЗ «МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ
ПЕРСОНАЛОМ»**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ІМЕНІ КНЯЗЯ ВОЛОДИМИРА ВЕЛИКОГО**

Кафедра правоохоронної та антикорупційної діяльності

«ЗАТВЕРДЖУЮ»

Завідувач кафедри правоохоронної
та антикорупційної діяльності

Володимир ЗАРОСИЛО

" 28 " 08 2025р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«СТРАТЕГІЧНЕ УПРАВЛІННЯ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ»

Галузь знань: **26 Цивільна безпека**

Спеціальність: **262 Правоохоронна діяльність**

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

Освітня програма **«Правоохоронна діяльність»**

Київ 2025

Робоча програма з навчальної дисципліни «Стратегічне управління у сфері безпеки та оборони» для здобувачів вищої освіти освітньої програми «Правоохоронна діяльність» спеціальності 262 Правоохоронна діяльність:

Розробник:

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



(підпис)

Сергій ЛИСЕНКО

Робочу програму погоджено

Гарант освітньої програми «Правоохоронна діяльність»



(підпис)

Олександр САВКА

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

Протокол № 1 від «24» 08 2025 року

Завідувач кафедри правоохоронної та антикорупційної діяльності



(підпис)

Володимир ЗАРОСИЛО

Загальна інформація про навчальну дисципліну

Найменування показників	Характеристика дисципліни за формами навчання	
	очна (денна)	заочна
Вид дисципліни (обов'язкова чи вибіркова)	обов'язкова	
Мова викладання	українська	
Загальний обсяг у кредитах ЄКТС/годинах	4 кредита/120 год Лекції : 20 Семінарські заняття: 14 Самостійна робота студентів: 86	
Курс	1	1
Семестр	1	1
Кількість змістових модулів	3	3
Обсяг кредитів із розподілом за семестрами	4	4
Обсяг годин, у тому числі:		
- Аудиторні	34	6
- Лекційні	20	4
- Семінарські	14	2
- Лабораторні	-	-
Самостійна робота, год	86	114
Форма семестрового контролю	екзамен	

Мета й завдання навчальної дисципліни

Метою навчальної дисципліни є формування у здобувачів вищої освіти системного бачення стратегічного управління у сфері безпеки та оборони, розуміння закономірностей функціонування сектору безпеки і оборони держави, а також здатності аналізувати сучасні виклики, загрози й ризики у безпековому середовищі та виробляти обґрунтовані управлінські рішення стратегічного рівня. Метою курсу є

також засвоєння теоретичних і прикладних засад стратегічного мислення, ризик-орієнтованого підходу, міжвідомчої координації, кризового реагування, забезпечення національної стійкості, захисту критичної інфраструктури, інформаційної та кібербезпеки, а також формування вмій застосовувати отримані знання для планування, організації й удосконалення механізмів державного управління у сфері безпеки та оборони в умовах воєнних, гібридних та інших сучасних загроз.

Завдання навчальної дисципліни:

Завданнями навчальної дисципліни є засвоєння понятійно-категоріального апарату стратегічного управління у сфері безпеки та оборони; вивчення теоретичних засад і сучасних підходів до формування державної безпекової та оборонної політики; оволодіння знаннями про архітектуру сектору безпеки і оборони, механізми міжвідомчої координації та демократичного цивільного контролю; формування вмій аналізувати загрози, вразливості, виклики та ризики у безпековому середовищі й застосовувати ризик-орієнтований підхід до прийняття стратегічних рішень; засвоєння принципів стратегічного планування, кризового управління, забезпечення національної стійкості, захисту критичної інфраструктури, інформаційної та кібербезпеки; набуття здатності використовувати аналітичні, прогностичні й організаційні інструменти для розроблення управлінських рішень у сфері безпеки та оборони; розвиток навичок оцінювання ресурсного забезпечення, оборонних спроможностей, кадрового потенціалу, правових і етичних меж стратегічної діяльності; а також формування готовності до практичного застосування набутих знань у процесі розроблення, реалізації та вдосконалення механізмів державного управління у сфері безпеки та оборони.

Компетентності та результати навчання за освітньою програмою

Основними завданнями вивчення дисципліни є формування таких загальних та спеціальних (предметних, фахових) компетентностей:

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» формує здатність до абстрактного мислення, аналізу та синтезу через опрацювання складних безпекових явищ, багаторівневих загроз і взаємозв'язків між суб'єктами сектору безпеки і оборони. Засвоєння теоретичних засад стратегічного мислення, ризик-орієнтованого підходу, кризового управління та національної стійкості дає змогу здобувачам узагальнювати різномірну інформацію, виявляти причинно-наслідкові зв'язки, формувати аналітичні висновки та синтезувати цілісне бачення механізмів державного управління у сфері безпеки та оборони.

ЗК8. Здатність приймати обґрунтовані рішення.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» розвиває здатність приймати обґрунтовані рішення на основі аналізу безпекового середовища, оцінювання ризиків, визначення стратегічних пріоритетів та прогнозування можливих наслідків управлінських дій. Вивчення стратегічного планування, розвідувально-аналітичного забезпечення, кризового реагування, інформаційної та кібербезпеки сприяє формуванню вмінь обирати оптимальні варіанти рішень у складних, нестабільних і багатофакторних умовах.

СК2. Здатність забезпечувати законність та правопорядок, безпеку особистості, суспільства, держави в межах виконання своїх посадових обов'язків.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» формує здатність забезпечувати законність і правопорядок, безпеку особистості, суспільства та держави через розуміння стратегічних засад функціонування сектору безпеки і оборони, правових меж діяльності його суб'єктів та механізмів реагування на сучасні загрози. Опрацювання питань правового забезпечення, кризового управління, захисту критичної інфраструктури, протидії гібридним загрозам, інформаційній і кібернетичній агресії дає можливість усвідомити роль посадової особи у формуванні безпечного середовища та підтриманні правопорядку.

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

Дисципліна «Стратегічне управління у сфері безпеки та оборони» сприяє формуванню спроможності організовувати і керувати діяльністю підрозділів через засвоєння принципів стратегічного планування, міжвідомчої координації, управління ресурсами, кризового реагування та забезпечення безперервності функціонування. Вивчення архітектури сектору безпеки і оборони, підходів до визначення цілей, завдань, ресурсного забезпечення та показників ефективності дає змогу здобувачам розуміти логіку управління підрозділами в різних умовах оперативної та стратегічної обстановки.

СК6. Здатність управляти самостійною роботою осіб та бути наставником для молодших колег у процесі набуття і вдосконалення ними професійних навичок.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» розвиває здатність управляти самостійною роботою осіб та здійснювати наставництво через формування системного бачення професійної діяльності у сфері безпеки, вироблення навичок постановки завдань, контролю результатів і оцінювання ефективності виконаної роботи. Засвоєння змісту стратегічного управління, кадрової безпеки, лідерства, безпекової культури та організаційної стійкості сприяє підготовці здобувачів до ролі керівника і наставника у професійному середовищі.

СК7. Здатність ефективно здійснювати правове виховання молодших колег у процесі набуття і вдосконалення ними професійних навичок.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» забезпечує формування здатності до ефективного правового виховання молодших колег шляхом засвоєння правових та етичних засад стратегічного управління, принципів законності, легітимності, пропорційності та відповідальності у сфері безпеки й оборони. Розгляд правового режиму діяльності сектору безпеки і оборони, захисту прав людини, меж застосування управлінських рішень та професійної доброчесності сприяє утвердженню правосвідомості та готовності передавати ці орієнтири іншим.

СК11. Здатність взаємодіяти з представниками інших органів виконавчої влади та місцевого самоврядування, громадськістю з питань правоохоронної діяльності.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» формує здатність взаємодіяти з представниками інших органів виконавчої влади, місцевого самоврядування та громадськістю завдяки вивченню міжвідомчої координації, стратегічних комунікацій, кризового управління та механізмів забезпечення національної стійкості. Опрацювання ролі суб'єктів сектору безпеки і оборони, принципів узгодження дій, інформаційної взаємодії та комунікації у кризових умовах дозволяє усвідомити значення партнерства і координації в реалізації правоохоронних та безпекових функцій.

Згідно з вимогами освітньо-професійної програми, здобувачі вищої освіти мають досягти таких *результатів навчання*:

РН1. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців, зокрема під час публічних виступів, дискусій, проведення занять.

Опанування дисципліни «Стратегічне управління у сфері безпеки та оборони» забезпечує здатність зрозуміло і недвозначно доносити знання, висновки та аргументацію з питань безпеки й оборони до фахівців і нефахівців. Робота з категоріальним апаратом, стратегічними документами, аналітичними моделями, кризовими сценаріями та управлінськими рішеннями сприяє розвитку вмінь логічно структурувати матеріал, формулювати висновки, аргументувати позицію та презентувати її в усній і письмовій формах.

РН2. Координувати і керувати функції суб'єктів забезпечення публічної безпеки і правопорядку, а також здійснювати взаємодію з представниками інших органів виконавчої влади та місцевого самоврядування, громадськістю з питань правоохоронної діяльності.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» забезпечує формування результату навчання, пов'язаного з координацією і керівництвом

функціями суб'єктів забезпечення публічної безпеки і правопорядку. Вивчення інституційної архітектури сектору безпеки і оборони, принципів міжвідомчої взаємодії, кризового управління, стратегічних комунікацій та координаційних механізмів дозволяє здобувачам усвідомити алгоритми узгодження дій різних суб'єктів і практику налагодження взаємодії з іншими органами та громадськістю.

РН3. Організовувати і управляти діяльністю органів, підрозділів та осіб, які здійснюють правоохоронну діяльність.

Опанування дисципліни «Стратегічне управління у сфері безпеки та оборони» сприяє здатності організовувати і управляти діяльністю органів, підрозділів та осіб, які здійснюють правоохоронну діяльність, на засадах стратегічного бачення, планування, координації та контролю. Засвоєння положень щодо стратегічного управління, управління ресурсами, кадрового забезпечення, аналізу ризиків, кризового реагування та оцінювання ефективності формує у здобувачів розуміння сучасних механізмів управління правоохоронними структурами.

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

Дисципліна «Стратегічне управління у сфері безпеки та оборони» формує здатність оцінювати та забезпечувати якість виконуваних робіт у процесі управління правоохоронним підрозділом завдяки вивченню підходів до стратегічного аналізу, моніторингу ризиків, оцінювання спроможностей, визначення показників ефективності та підготовки аналітичних матеріалів. Опрацювання розвідувально-аналітичного забезпечення, кризового менеджменту, стратегічного планування та процедур звітності сприяє розвитку навичок підготовки аргументованих звітів, доповідей і висновків у різних умовах обстановки.

РН14. Розробляти стратегічні плани та управляти проектами у сфері правоохоронної діяльності, в дотичних міждисциплінарних напрямках, аналізувати вимоги, визначати цілі, завдання, ресурси, строки та виконавців.

Опанування дисципліни «Стратегічне управління у сфері безпеки та оборони» безпосередньо забезпечує формування здатності розробляти стратегічні плани та управляти проектами у сфері правоохоронної діяльності й суміжних напрямках. Засвоєння логіки стратегічного планування, аналізу загроз, визначення пріоритетів, оцінювання ресурсів, встановлення часових меж, координації виконавців і моніторингу реалізації дає змогу здобувачам опанувати механізми проектування та впровадження стратегічних рішень у безпековій сфері.

РН18. Мати навички вирішення завдань у складі міжвідомчих органів з проблем забезпечення суспільної безпеки та підтримання правопорядку.

Дисципліна «Стратегічне управління у сфері безпеки та оборони» сприяє формуванню навичок вирішення завдань у складі міжвідомчих органів через вивчення механізмів міжвідомчої координації, розподілу повноважень, спільного кризового реагування, стратегічних комунікацій і управління національною стійкістю. Здобувачі опановують підходи до колективного аналізу загроз, узгодження рішень, розроблення спільних дій і забезпечення взаємодії між різними суб'єктами сектору безпеки та оборони з метою підтримання суспільної безпеки і правопорядку.

Програма навчальної дисципліни

Тема 1. Стратегічне управління у сфері безпеки та оборони 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. Стратегічне мислення і стратегічна культура у сфері безпеки

Вивчаються співвідношення понять стратегія, політика, доктрина, концепція, план; класичні та сучасні школи стратегічного мислення; проблеми невизначеності, туману війни, багатодоменності та швидкості прийняття рішень; особливості стратегічної культури держави та безпекових інституцій.

Тема 3. Архітектура системи безпеки й оборони держави

Розкривається інституційна побудова сектору безпеки і оборони, розподіл повноважень між воєнними, правоохоронними, розвідувальними та кібербезпековими структурами, механізми міжвідомчої координації та принципи демократичного цивільного контролю.

Тема 4. Ризик-орієнтоване управління у сфері безпеки та оборони

Аналізуються ідентифікація загроз, викликів, небезпек і вразливостей, стратегічний аналіз ризиків, матриці ризиків, сценарне прогнозування, ранжування пріоритетів, а також застосування підходів ISO 31000, COSO ERM, NIST CSF 2.0 у безпековій сфері.

Тема 5. Стратегічне планування у сфері безпеки та оборони

Розглядаються цикл стратегічного планування, формування цілей, пріоритетів, ресурсних меж і показників досягнення, документи стратегічного рівня у сфері безпеки та оборони, а також узгодження довгострокового планування з оперативним і кризовим реагуванням.

Тема 6. Гібридні загрози та багатодоменне безпекове середовище

Вивчається природа гібридних загроз, поєднання воєнних, інформаційних, економічних, кібернетичних і психологічних впливів, багатодоменні операції, комплексний характер сучасного конфлікту та механізми державної протидії гібридним впливам.

Тема 7. Інформаційна безпека, стратегічні комунікації та протидія дезінформації

Розглядаються інформаційний простір як поле стратегічного суперництва, стратегічні комунікації держави, операції впливу, дезінформація, інформаційно-психологічні кампанії та репутаційна безпека державних інституцій і сил безпеки.

Тема 8. Кібербезпека і кіберстійкість у стратегічному управлінні

Вивчаються кіберпростір як домен безпеки й оборони, кіберстримування, кіберзахист, кіберреагування, захист державних інформаційних ресурсів і критичних систем, кіберстійкість, Zero Trust, SOC/SIEM та управління кіберінцидентами.

Тема 9. Розвідувально-аналітичне забезпечення стратегічних рішень

Розкриваються стратегічна аналітика в системі безпеки та оборони, роль розвідки, контррозвідки, кримінального аналізу та OSINT, обробка великих масивів даних для ухвалення стратегічних рішень, аналітичні продукти для політичного й оперативного рівнів.

Тема 10. Кризове управління, національна стійкість і безперервність функціонування

Аналізуються кризи безпекового характеру та їх класифікація, національна стійкість як управлінська категорія, плани безперервності діяльності, резервування ресурсів, відновлення спроможностей, а також робота кризових штабів та міжвідомчих координаційних центрів.

Тема 11. Захист критичної інфраструктури та забезпечення стратегічної стійкості держави

Розглядаються поняття критичної інфраструктури та критичних функцій держави, уразливості енергетики, транспорту, зв'язку, фінансів, охорони здоров'я, цифрових сервісів, безпека ланцюгів постачання та відновлення критичних спроможностей після атак і криз.

Тема 12. Управління ресурсами, оборонне планування та спроможності

Вивчаються ресурсне забезпечення стратегії безпеки й оборони, поняття оборонних спроможностей, планування бюджетів, закупівель, резервів та розвитку персоналу, оборонно-промислова база, інновації та стандартизація.

Тема 13. Людський капітал, кадрова безпека та лідерство у сфері безпеки

Розкриваються питання підготовки кадрів для сектору безпеки і оборони, професійної доброчесності, стресостійкості, кадрового резерву, лідерства в умовах

невизначеності та кризи, а також формування безпекової культури в державних і силових інституціях.

Тема 14. Правове та етичне забезпечення стратегічного управління

Розглядаються конституційні та законодавчі засади функціонування сектору безпеки і оборони, правові режими надзвичайного і воєнного стану, захист прав людини у безпековій діяльності, етика стратегічних рішень, пропорційність, легітимність та відповідальність посадових осіб.

Тема 15. Майбутнє стратегічного управління у сфері безпеки та оборони

Аналізуються роль штучного інтелекту у безпековому управлінні, автоматизація аналітики, predictive security, data-driven governance, безпілотні системи, автономність, роботизація безпекових процесів, а також етичні, правові та організаційні межі технологізації безпеки.

Структура навчальної дисципліни

Назви тем	Кількість годин							
	очна (денна) форма				заочна форма			
	Усього	у тому числі			Усього	у тому числі		
		Лекції	Семінари	Самостійна робота		Лекції	Семінари	Самостійна робота
ЗМІСТОВИЙ МОДУЛЬ 1. Теоретико-методологічні засади стратегічного управління у сфері безпеки та оборони								
Тема 1. Стратегічне управління у сфері безпеки та оборони як наукова і практична категорія	8	2	-	6	10	2	2	6
Тема 2. Стратегічне мислення і стратегічна культура у сфері безпеки.	8		2	6	6			6
Тема 3. Архітектура системи безпеки й оборони держави.	8	2	2	4	8			8
Тема 4. Ризик-орієнтоване управління у сфері безпеки та оборони.	8	2	2	4	6			6
Тема 5. Стратегічне планування у сфері безпеки та оборони	6			6	8			8

ЗМІСТОВИЙ МОДУЛЬ 2. Функціональні напрями стратегічного управління у сфері безпеки та оборони								
Тема 6. Гібридні загрози та багатодоменне безпекове середовище.	10	2	2	6	8			8
Тема 7. Інформаційна безпека, стратегічні комунікації та протидія дезінформації	8	2		6	8			8
Тема 8. Кібербезпека і кіберстійкість у стратегічному управлінні.	8	2		6	8			8
Тема 9. Розвідувально-аналітичне забезпечення стратегічних рішень.	10	2	2	6	8			8
Тема 10. Кризове управління, національна стійкість і безперервність функціонування.	6			6	8			8
ЗМІСТОВИЙ МОДУЛЬ 3. Організаційно-правові та перспективні аспекти стратегічного управління у сфері безпеки та оборони								
Тема 11. Захист критичної інфраструктури та забезпечення стратегічної стійкості держави.	10	2	2	6	10	2		8
Тема 12. Управління ресурсами, оборонне планування та спроможності.	8	2		6	8			8
Тема 13. Людський капітал, кадрова безпека та лідерство у сфері безпеки.	10	2	2	6	8			8
Тема 14. Правове та етичне забезпечення стратегічного управління.	6			6	8			8
Тема 15. Майбутнє стратегічного управління у сфері безпеки та оборони	6			6	8			8
Модульна контрольна робота								
Всього:	120	20	14	86	120	4	2	114
Форма контролю: екзамен								

Теми семінарських занять

№ Семінар. заняття	Назва теми	Кількість годин	
		очна (денна) форма	заочна форма
Семінарське заняття №1	<p>Тема 1. Стратегічне управління у сфері безпеки та оборони як наукова і практична категорія</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити сутність понять безпека, оборона, національна стійкість і стратегічне управління. • Охарактеризувати еволюцію підходів від секторного реагування до інтегрованого безпекового управління. • Скласти схему взаємозв'язку: національна безпека → воєнна безпека → громадська безпека → інформаційна безпека → кібербезпека. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати предметну сферу стратегічного управління у безпеково-оборонній сфері. • Здатність показувати місце дисципліни в системі державного управління. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому сучасна безпека більше не може розглядатися лише в межах окремого сектору? • Чи можлива ефективна оборонна політика без інтегрованого безпекового управління? <p>Тема 2. Стратегічне мислення і стратегічна культура у сфері безпеки</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити співвідношення понять стратегія, політика, доктрина, концепція, план. 	2	2

	<ul style="list-style-type: none"> • Охарактеризувати значення стратегічного мислення в умовах невизначеності, туману війни і багатодоменності. • Скласти порівняльну схему: стратегія → політика → концепція → план → реалізація. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння розкривати сутність стратегічного мислення у сфері безпеки. • Здатність пояснювати роль стратегічної культури держави та інституцій у прийнятті рішень. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому стратегічні помилки у сфері безпеки мають довгострокові наслідки? • Наскільки стратегічна культура впливає на здатність держави реагувати на загрози? 		
Семінарське заняття №2	<p>Тема 3. Архітектура системи безпеки й оборони держави</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити структуру сектору безпеки і оборони держави. • Охарактеризувати розподіл повноважень між воєнними, правоохоронними, розвідувальними та кібербезпековими структурами. • Скласти схему міжвідомчої координації та цивільного контролю в системі безпеки і оборони. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння бачити систему безпеки не як набір органів, а як керовану архітектуру. • Здатність пояснювати значення інституційної узгодженості в безпеково-оборонній сфері. <p>Дискусія:</p>	2	

	<ul style="list-style-type: none"> • Чи може сильний сектор безпеки бути ефективним без належної координації? • Наскільки демократичний цивільний контроль є умовою ефективної безпеки держави? 		
Семінарське заняття №3	<p>Тема 4. Ризик-орієнтоване управління у сфері безпеки та оборони</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити зміст ризик-орієнтованого підходу у сфері безпеки та оборони. • Охарактеризувати етапи ідентифікації загроз, вразливостей, аналізу наслідків та ранжування пріоритетів. • Скласти базову матрицю стратегічних ризиків для державного органу або об'єкта критичної інфраструктури. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати логіку стратегічного аналізу ризиків. • Здатність обирати пріоритети реагування на підставі ризик-орієнтованого підходу. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чи може державна система безпеки повністю усунути стратегічні ризики? • Де проходить межа між прийнятним і критичним ризиком у сфері безпеки та оборони? <p>Тема 5. Стратегічне планування у сфері безпеки та оборони</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити етапи циклу стратегічного планування. • Охарактеризувати порядок формування цілей, пріоритетів, ресурсних меж і показників досягнення. • Скласти схему узгодження стратегічного, 	2	

	<p>оперативного та кризового планування.</p> <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати логіку побудови стратегічних документів у сфері безпеки та оборони. • Здатність визначати взаємозв'язок довгострокового планування з оперативним реагуванням. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому стратегічне планування не може обмежуватися лише формальним документом? • Наскільки реалістичність ресурсних меж визначає якість стратегії? 		
Семінарське заняття №4	<p>Тема 6. Гібридні загрози та багатодоменне безпекове середовище</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити природу гібридних загроз і багатодоменного конфлікту. • Охарактеризувати поєднання воєнних, інформаційних, економічних, кібернетичних і психологічних впливів. • Скласти схему комплексної державної протидії гібридним впливам. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати сутність гібридних загроз у сучасному безпековому середовищі. • Здатність визначати комплексний характер сучасних конфліктів. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому гібридні впливи є складнішими за традиційні форми загроз? • Чи достатньо однієї силової відповіді для протидії багатодоменним загрозам? 	2	

Тема 7. Інформаційна безпека, стратегічні комунікації та протидія дезінформації

Завдання:

- Визначити значення інформаційного простору як поля стратегічного суперництва.
- Охарактеризувати стратегічні комунікації держави та механізми реагування на дезінформацію.
- Скласти модель реагування на масштабну дезінформаційну атаку.

Очікуваний результат:

- Вміння пояснювати роль інформаційної безпеки та стратегічних комунікацій у державному управлінні.
- Здатність визначати способи протидії операціям впливу й інформаційно-психологічним кампаніям.

Дискусія:

- Чи може дезінформація становити загрозу, співмірну з традиційними силовими впливами?
- Наскільки репутаційна стійкість державних інституцій є елементом національної безпеки?

Тема 8. Кібербезпека і кіберстійкість у стратегічному управлінні

Завдання:

- Визначити кіберпростір як домен безпеки й оборони.
- Охарактеризувати кіберструмування, кіберзахист, кіберреагування, а також принципи Zero Trust, SOC/SIEM.
- Скласти схему управління кіберінцидентом у державній системі.

Очікуваний результат:

	<ul style="list-style-type: none"> • Вміння пояснювати місце кібербезпеки у стратегічному управлінні. • Здатність визначати основні підходи до забезпечення кіберстійкості державних систем. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому кібербезпека стала самостійним доменом безпеки та оборони? • Чи може кіберстійкість існувати без належного управлінського рівня Govern? 		
Семінарське заняття №5	<p>Тема 9. Розвідувально-аналітичне забезпечення стратегічних рішень</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити роль стратегічної аналітики у системі безпеки та оборони. • Охарактеризувати місце розвідки, контррозвідки, кримінального аналізу та OSINT у підготовці рішень. • Підготувати коротку стратегічну аналітичну записку для суб'єкта ухвалення рішень. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати роль аналітики в ухваленні стратегічних рішень. • Здатність готувати стислий аналітичний продукт для політичного або оперативного рівня. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чи може стратегічне рішення бути якісним без належного аналітичного забезпечення? • Що важливіше у стратегічній аналітиці: швидкість чи глибина опрацювання даних? <p>Тема 10. Кризове управління, національна стійкість і безперервність функціонування</p> <p>Завдання:</p>	2	

	<ul style="list-style-type: none"> • Визначити класифікацію криз безпекового характеру. • Охарактеризувати національну стійкість як управлінську категорію та механізм безперервності функціонування. • Скласти схему роботи кризового штабу і міжвідомчого координаційного центру. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати значення кризового управління та національної стійкості. • Здатність визначати ключові умови збереження функціонування державних інституцій у кризі. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому стійкість є не лише ресурсною, а й управлінською категорією? • Наскільки ефективність реагування залежить від підготовки до кризи ще до її виникнення? 		
Семінарське заняття №6	<p>Тема 11. Захист критичної інфраструктури та забезпечення стратегічної стійкості держави</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити поняття критичної інфраструктури та критичних функцій держави. • Охарактеризувати ключові уразливості інфраструктурних секторів і безпеку ланцюгів постачання. • Скласти схему відновлення критичних спроможностей після атаки або кризи. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати значення захисту критичної інфраструктури для стратегічної стійкості держави. • Здатність визначати основні напрями відновлення критичних функцій після 	2	

	<p>порушення.</p> <p>Дискусія:</p> <ul style="list-style-type: none"> • Чому критична інфраструктура є одним із головних об'єктів сучасних загроз? • Чи можлива стратегічна стійкість держави без захищених ланцюгів постачання? <p>Тема 12. Управління ресурсами, оборонне планування та спроможності</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити сутність ресурсного забезпечення стратегії безпеки й оборони. • Охарактеризувати поняття оборонних спроможностей, планування бюджетів, закупівель, резервів та розвитку персоналу. • Скласти схему зв'язку між ресурсами, спроможностями та результатом безпеково-оборонної політики. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати значення оборонного планування та ресурсного забезпечення. • Здатність визначати взаємозв'язок між інвестиціями, інноваціями, стандартизацією та безпековою ефективністю. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чи може сильна стратегія компенсувати нестачу ресурсів? • Наскільки стандартизація й інтегрованість впливають на оборонні спроможності? 		
Семінарське заняття №7	<p>Тема 13. Людський капітал, кадрова безпека та лідерство у сфері безпеки</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити значення людського капіталу та кадрової безпеки для сектору безпеки і оборони. • Охарактеризувати роль доброчесності, 	2	

стресостійкості, кадрового резерву та лідерства в умовах кризи.

- Скласти схему формування безпекової культури в державній або силовій інституції.

Очікуваний результат:

- Вміння пояснювати роль кадрової безпеки та лідерства у стратегічному управлінні.
- Здатність визначати значення безпекової культури та професійної доброчесності.

Дискусія:

- Чи є людський фактор головною вразливістю чи головним ресурсом системи безпеки?
- Наскільки лідерство впливає на стійкість інституції під час кризи?

Тема 14. Правове та етичне забезпечення стратегічного управління

Завдання:

- Визначити правові засади функціонування сектору безпеки і оборони.
- Охарактеризувати правові режими надзвичайного і воєнного стану, а також значення захисту прав людини у безпековій діяльності.
- Скласти схему співвідношення законності, легітимності, пропорційності та відповідальності посадових осіб.

Очікуваний результат:

- Вміння пояснювати роль правового та етичного забезпечення стратегічних рішень.
- Здатність визначати межі допустимості безпекових рішень у демократичній державі.

Дискусія:

- Чи може ефективність безпекового рішення виправдовувати відступ від правових принципів?

	<ul style="list-style-type: none"> • Де проходить межа між безпековою необхідністю та надмірним обмеженням прав людини? <p>Тема 15. Майбутнє стратегічного управління у сфері безпеки та оборони</p> <p>Завдання:</p> <ul style="list-style-type: none"> • Визначити основні напрями технологізації стратегічного управління у сфері безпеки та оборони. • Охарактеризувати роль AI, predictive security, data-driven governance, безпілотних і автономних систем. • Скласти схему трансформації безпекового управління: класична модель → цифрова аналітика → прогнозне управління → адаптивна система. <p>Очікуваний результат:</p> <ul style="list-style-type: none"> • Вміння пояснювати перспективи розвитку стратегічного управління у сфері безпеки та оборони. • Здатність оцінювати нові технології як джерело можливостей і нових ризиків. <p>Дискусія:</p> <ul style="list-style-type: none"> • Чи зробить технологізація безпеки управління більш ефективним або більш залежним від складних систем? • Якими мають бути ключові компетентності майбутнього фахівця у сфері безпеки та оборони? 		
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Самостійна робота

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Стратегічне управління у сфері безпеки та оборони» 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 науковоправового аналізу; виконання індивідуальних завдань; підготовку до усіх видів контролю, у тому числі модульних контрольних робіт і підсумкової атестації; підготовку юридичних документів, інші види діяльності, що використовуються в Академії, Інституті і кафедрі.

Зміст завдань для самостійної роботи здобувача (СРЗ)

№ п/п	Зміст самостійної роботи здобувача вищої освіти	Форми контролю СРЗ
1	<p>Тема 1. Стратегічне управління у сфері безпеки та оборони як наукова і практична категорія</p> <p>Підготувати короткий аналітичний опис сутності стратегічного управління у сфері безпеки та оборони, визначивши його місце в системі державного управління та взаємозв'язок із національною стійкістю.</p> <p>Скласти глосарій із 20 ключових термінів: безпека, оборона, стратегічне управління, національна стійкість, загроза, виклик, небезпека, вразливість, суб'єкт безпеки, сектор безпеки, інтегроване управління, державна політика, громадська безпека, воєнна безпека, інформаційна безпека, кібербезпека, управлінське рішення, безпекова система, пріоритет, стійкість.</p>	Презентація результатів
2	<p>Тема 2. Стратегічне мислення і стратегічна культура у сфері безпеки</p> <p>Підготувати короткий текстовий матеріал про роль стратегічного мислення та стратегічної культури у формуванні безпекових рішень держави.</p> <p>Скласти глосарій із 20 ключових термінів: стратегія, політика, доктрина, концепція, план, стратегічне мислення, стратегічна культура, туман війни, невизначеність, багатодоменність, пріоритет, стратегічна помилка, сценарій, прогнозування,</p>	Презентація результатів

	адаптація, стратегічна ціль, середовище безпеки, управлінська гнучкість, рішення, культура безпеки.	
3	<p>Тема 3. Архітектура системи безпеки й оборони держави</p> <p>Підготувати короткий аналітичний опис архітектури сектору безпеки і оборони, визначивши її інституційну побудову, розподіл повноважень та механізми координації.</p> <p>Скласти глосарій із 20 ключових термінів: сектор безпеки і оборони, інституційна архітектура, повноваження, координація, суб'єкт безпеки, розвідувальна структура, правоохоронний орган, воєнна організація, кібербезпекова структура, міжвідомча взаємодія, демократичний цивільний контроль, управлінська система, компетенція, ієрархія, контроль, підзвітність, орган державної влади, функція, управлінський механізм, архітектура безпеки.</p>	Презентація результатів
4	<p>Тема 4. Ризик-орієнтоване управління у сфері безпеки та оборони</p> <p>Підготувати короткий аналітичний опис risk-based approach у безпеково-оборонній сфері з визначенням етапів аналізу ризиків і механізмів вибору пріоритетів реагування.</p> <p>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.</p>	Презентація результатів
5	<p>Тема 5. Стратегічне планування у сфері безпеки та оборони</p> <p>Підготувати короткий матеріал про цикл стратегічного планування у сфері безпеки та оборони, визначивши його етапи та місце стратегічних документів у системі державного управління.</p>	Презентація результатів

	<p>Скласти глосарій із 20 ключових термінів: стратегічне планування, стратегічна ціль, пріоритет, показник досягнення, ресурсна межа, стратегічний документ, планування, реалізація, моніторинг, оцінювання, корекція, безпекова політика, дорожня карта, індикатор, державна стратегія, програма, узгодження, управлінський цикл, кризове реагування, довгострокове планування.</p>	
6	<p>Тема 6. Гібридні загрози та багатодоменне безпекове середовище</p> <p>Підготувати короткий аналітичний опис сутності гібридних загроз та багатодоменного середовища безпеки, визначивши їх вплив на державне управління.</p> <p>Скласти глосарій із 20 ключових термінів: гібридна загроза, багатодоменність, інформаційний вплив, психологічна операція, економічний тиск, кібератака, дезінформація, диверсія, конфлікт, стійкість, комплексна протидія, багатодоменна операція, стратегічний вплив, маніпуляція, ворожий наратив, асиметричний вплив, нестабільність, дестабілізація, кризове середовище, державна реакція.</p>	Презентація результатів
7	<p>Тема 7. Інформаційна безпека, стратегічні комунікації та протидія дезінформації</p> <p>Підготувати короткий текстовий матеріал про значення інформаційної безпеки та стратегічних комунікацій у протидії дезінформації та інформаційно-психологічним впливам.</p> <p>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, контрнاراتив, кризова комунікація, медіасередовище, публічне повідомлення, моніторинг, верифікація, інформаційна стійкість, суспільна довіра, комунікаційна стратегія, реагування.</p>	Презентація результатів

8	<p>Тема 8. Кібербезпека і кіберстійкість у стратегічному управлінні</p> <p>Підготувати короткий аналітичний опис кібербезпеки як складової стратегічного управління у сфері безпеки та оборони, визначивши основні підходи до кіберстійкості.</p> <p>Скласти глосарій із 20 ключових термінів: кібербезпека, кіберстійкість, кіберпростір, кіберзахист, кіберстримування, кіберреагування, кіберінцидент, державний інформаційний ресурс, критична система, Zero Trust, SOC, SIEM, контроль доступу, кіберризик, цифровий актив, відновлення, реагування на інцидент, захист системи, кіберзагроза, кібероборона.</p>	Презентація результатів
9	<p>Тема 9. Розвідувально-аналітичне забезпечення стратегічних рішень</p> <p>Підготувати короткий матеріал про роль розвідувально-аналітичного забезпечення у прийнятті стратегічних рішень у сфері безпеки та оборони.</p> <p>Скласти глосарій із 20 ключових термінів: стратегічна аналітика, розвідка, контррозвідка, кримінальний аналіз, OSINT, джерело інформації, аналітичний продукт, стратегічна записка, великий масив даних, обробка даних, індикатор загрози, прогноз, верифікація, аналітичний висновок, суб'єкт ухвалення рішення, політичний рівень, оперативний рівень, інформаційне забезпечення, аналітичний цикл, безпекова аналітика.</p>	Презентація результатів
10	<p>Тема 10. Кризове управління, національна стійкість і безперервність функціонування</p> <p>Підготувати короткий аналітичний опис кризового управління та національної стійкості, визначивши їх роль у забезпеченні безперервності функціонування державних інституцій.</p> <p>Скласти глосарій із 20 ключових термінів: криза, кризове управління, національна стійкість, безперервність функціонування, кризовий штаб, координаційний центр, резервування ресурсів,</p>	Презентація результатів

	<p>відновлення спроможностей, реагування, підготовленість, стрес-тестування, управлінська спроможність, резерв, адаптація, стабілізація, кризове планування, міжвідомча координація, надзвичайна ситуація, швидке реагування, цивільно-військова готовність.</p>	
11	<p>Тема 11. Захист критичної інфраструктури та забезпечення стратегічної стійкості держави Підготувати короткий матеріал про значення захисту критичної інфраструктури для стратегічної стійкості держави. Скласти глосарій із 20 ключових термінів: критична інфраструктура, критична функція, енергетика, транспорт, зв'язок, фінанси, охорона здоров'я, цифровий сервіс, уразливість, захист інфраструктури, стійкість, відновлення, ланцюг постачання, критичний ресурс, резервування, атака на інфраструктуру, інфраструктурний ризик, відновлення функцій, національна безпека, стратегічна стійкість.</p>	Презентація результатів
12	<p>Тема 12. Управління ресурсами, оборонне планування та спроможності Підготувати короткий аналітичний опис управління ресурсами та оборонного планування, визначивши їх роль у формуванні оборонних спроможностей. Скласти глосарій із 20 ключових термінів: ресурсне забезпечення, оборонне планування, оборонна спроможність, бюджет, закупівля, резерв, розвиток персоналу, стандартизація, інновація, оборонно-промислова база, ефективність ресурсу, інтероперабельність, пріоритет фінансування, спроможність, інвестиція в оборону, управлінський ресурс, резервування, логістика, оборонний потенціал, забезпечення стратегії.</p>	Презентація результатів
13	<p>Тема 13. Людський капітал, кадрова безпека та лідерство у сфері безпеки Підготувати короткий текстовий матеріал про значення людського капіталу, кадрової безпеки та лідерства у секторі безпеки і оборони.</p>	Презентація результатів

	<p>Скласти глосарій із 20 ключових термінів: людський капітал, кадрова безпека, добродесність, стресостійкість, кадровий резерв, професійна підготовка, лідерство, безпекова культура, етика служби, управління персоналом, мотивація, інституційна стійкість, компетентність, підготовка кадрів, морально-психологічний стан, кадровий ризик, служба, відповідальність, командна взаємодія, професійна культура.</p>	
14	<p>Тема 14. Правове та етичне забезпечення стратегічного управління</p> <p>Підготувати короткий аналітичний опис правового й етичного забезпечення стратегічного управління у сфері безпеки та оборони.</p> <p>Скласти глосарій із 20 ключових термінів: правове забезпечення, конституційна засада, законодавство, воєнний стан, надзвичайний стан, права людини, пропорційність, легітимність, відповідальність посадової особи, етика рішення, законність, контроль, обмеження прав, правовий режим, службова відповідальність, демократична держава, правовий баланс, публічний інтерес, підзвітність, правова межа.</p>	Презентація результатів
15	<p>Тема 15. Майбутнє стратегічного управління у сфері безпеки та оборони</p> <p>Підготувати короткий аналітичний опис основних тенденцій розвитку стратегічного управління у сфері безпеки та оборони в умовах технологізації.</p> <p>Скласти глосарій із 20 ключових термінів: штучний інтелект, predictive security, data-driven governance, автоматизація аналітики, безпілотна система, автономність, роботизація, цифрова трансформація, аналітика даних, смарт-управління, технологічний ризик, алгоритмічне рішення, цифрова безпека, інноваційна спроможність, етичний виклик, правова межа технологізації, адаптивна система, майбутнє безпеки, управління на основі даних, інтелектуальна безпекова система.</p>	Презентація результатів

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Стратегічне управління у сфері безпеки та оборони».

Тему реферату здобувач визначає за першою буквою за списком групи.

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

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

вибір теми;

розробка плану;

ознайомлення з рекомендованою літературою;

написання та оформлення роботи.

При написанні реферату та його оформленні варто керуватися такими критеріями:

обґрунтування вибраної теми;

опрацювання відповідної літератури;

наявність авторського розділу;

наявність списку використаних джерел.

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

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

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

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

Теми рефератів

1. Стратегічне управління у сфері безпеки та оборони як наукова категорія.
2. Сутність стратегічного управління у безпеково-оборонній сфері.
3. Національна стійкість як об'єкт стратегічного управління.
4. Взаємозв'язок національної, воєнної, громадської, інформаційної та кібернетичної безпеки.
5. Еволюція підходів до стратегічного управління у сфері безпеки та оборони.

6. Стратегічне мислення у сфері безпеки: теорія і практика.
7. Стратегічна культура держави в умовах сучасних загроз.
8. Співвідношення стратегії, політики, доктрини, концепції і плану в безпековій сфері.
9. Туман війни та невизначеність у стратегічному управлінні.
10. Архітектура сектору безпеки і оборони держави.
11. Інституційна побудова системи безпеки і оборони.
12. Демократичний цивільний контроль у секторі безпеки і оборони.
13. Міжвідомча координація як умова ефективної безпекової політики.
14. Ризик-орієнтоване управління у сфері безпеки та оборони.
15. Стратегічний аналіз ризиків у державному управлінні безпекою.
16. Матриця ризиків як інструмент безпекового планування.
17. Сценарне прогнозування у сфері безпеки та оборони.
18. Стратегічне планування у сфері безпеки та оборони.
19. Документи стратегічного рівня у безпековій політиці держави.
20. Узгодження довгострокового планування з кризовим реагуванням.
21. Гібридні загрози як сучасний виклик державній безпеці.
22. Багато domenне безпекове середовище та його особливості.
23. Механізми державної протидії гібридним впливам.
24. Інформаційна безпека держави як складова стратегічного управління.
25. Стратегічні комунікації держави в умовах інформаційного суперництва.
26. Протидія дезінформації у сфері національної безпеки.
27. Репутаційна безпека державних інституцій.
28. Кібербезпека як домен безпеки й оборони.
29. Кіберстійкість державних систем у стратегічному управлінні.
30. Управління кіберінцидентами в державному секторі.
31. Розвідувально-аналітичне забезпечення стратегічних рішень.
32. Роль OSINT у сучасній системі безпеки та оборони.
33. Кримінальний аналіз як елемент аналітичного забезпечення безпеки.
34. Стратегічна аналітична записка як форма підтримки ухвалення рішень.
35. Кризове управління у сфері безпеки та оборони.
36. Національна стійкість як управлінська категорія.
37. Безперервність функціонування державних інституцій у кризових умовах.
38. Робота кризових штабів та координаційних центрів.
39. Захист критичної інфраструктури держави.
40. Стратегічна стійкість держави та безпека ланцюгів постачання.
41. Управління ресурсами у сфері безпеки та оборони.
42. Оборонне планування та розвиток спроможностей.
43. Оборонно-промислова база як чинник національної безпеки.

44. Людський капітал у секторі безпеки і оборони.
45. Кадрова безпека та професійна добросовісність у силових інституціях.
46. Лідерство в умовах невизначеності та кризи у сфері безпеки.
47. Правове забезпечення стратегічного управління у сфері безпеки та оборони.
48. Захист прав людини у безпековій діяльності держави.
49. Етичні межі стратегічних рішень у безпековій сфері.
50. Майбутнє стратегічного управління у сфері безпеки та оборони в умовах технологізації.

Індивідуальні завдання та критерії їх оцінювання

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

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

Також, заохочувальні бали можуть нараховуватися, якщо здобувач освіти, наприклад, виконав і захистив певні види робіт, відвідував всі лекції, семінарські й практичні заняття, має власний рукописний конспект лекцій та опрацьований додатковий навчальний матеріал, немає пропусків занять без поважних причин, відвідував додаткові консультації за участі лектора тощо.

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

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

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

Технічне й програмне забезпечення/обладнання

В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення аудиторних занять з елементам презентацій Microsoft PowerPoint. Вивчення окремих тем і виконання

практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

Форми і методи навчання

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

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

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

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

Оцінювання знань здійснюється відповідно до:

1. Положення про організацію освітнього процесу в ПрАТ «ВНЗ «МАУП» <https://surl.li/bpxl bj>
2. Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП» <http://surl.li/fkfyue>

№ тем	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Заг.сума балів
Робота на сем.занятті		5	5	5			5		5		5			5		35
Сам.робота	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Всього																50

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

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

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

Критерії оцінювання:

правильність відповідей та розрахунків – від 0 до 5 балів;

відповідність оформлення практичних робіт вимогам – 1 бал.

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

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

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

Завдання для самостійної роботи та критерії її оцінювання.

Під час вивчення курсу виконуються завдання для самостійних робіт до 15 тем.

Критерії оцінювання:

Змістовність, відповідність темі та вимогам оформлення – 1 бал.

Максимальна кількість балів за одиницю самостійної роботи – 1 бали.

Максимальна кількість балів за самостійну роботу по курсу – 15 балів.

Форми проведення модульного контролю та критерії оцінювання

Проведення модульного контролю з дисципліни «Стратегічне управління у сфері безпеки та оборони».

здійснюється у формі тестового завдання.

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

Запитання формулюються з урахуванням принципів:

Лаконічність: чіткі та стислі формулювання.

Завершеність: відповіді охоплюють всі аспекти запитання.

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

Вибірковість: питання стосуються суттєвих аспектів вивченого матеріалу.

Завдання передбачають вибір одного правильного варіанта з трьох запропонованих.

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

Загальна максимальна можлива кількість балів за модульну контрольну роботу - 10 балів.

Час на виконання.

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

Мінімальний поріг.

Для успішного складання модульного контролю здобувач повинен набрати не менше 6 балів (60% від максимальної кількості).

Шкала підсумкового оцінювання: національна та ECTS

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

Форми проведення семестрового контролю та критерії оцінювання

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

Орієнтовний перелік питань для комплексного контролю:

1. 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.

Політика курсу:

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

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

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

В кінці вивчення курсу проводиться модульна контрольна робота 1. Результат модульної контрольної роботи для здобувача, який не з'явився на контрольні заходи,

є нульовим. У такому разі, здобувач має можливість повторно виконати модульну контрольну роботи.

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

Рекомендовані джерела (література):

Основні джерела:

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

Додаткові:

1. 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-cvds.nuou.org.ua/article/download/234021/232667/535345>

2. 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>

3. 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

4. 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-infrastruktury_0.pdf

5. Денежкін 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-cvds.nuou.org.ua/article/view/125129>

6. 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-cvds.nuou.org.ua/article/view/223827>

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

8. 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

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

10. 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-cvds.nuou.org.ua/article/view/290266>

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

12. 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
13. 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>
14. 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>
15. Руснак І. С. та ін. Оборонний огляд: український вимір 2014–2018 : монографія. Київ : НУОУ, 2018. URL: <https://nuou.org.ua/u/stru/centers/cvsvd/ord/scientific-works.html>
16. 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>
17. 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-cvsvd.nuou.org.ua/article/view/196649>
18. Семененко В. М. Культура стратегічних комунікацій як основа таргетингу цільових аудиторій. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2021. № 2. URL: <https://znp-cvsvd.nuou.org.ua/article/view/234021>
19. Федієнко О. П. Міжнародні стандарти оцінки кіберстійкості. Інформація і право. 2024. № 3(50). С. 124–135. URL: https://jnas.nbuuv.gov.ua/j-pdf/Infpr_2024_3_14.pdf
20. 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>

Інформаційні ресурси:

1. Бібліотека ім. В. І. Вернадського – <http://www.nbuuv.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://reestr.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/>