

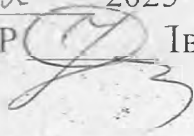
МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут права
Кафедра фінансового та податкового права

Затверджено

Науково-методична рада ДПУ,

від 11 12 2025 № 5

Голова НМР  Іван ШЕМЕЛИНЕЦЬ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Інформаційна безпека держави»

для підготовки здобувачів вищої освіти другого (магістерського) рівня

денної та заочної форми навчання

галузь знань К Безпека та оборона

спеціальність КЗ «Національна безпека (за окремими сферами забезпечення і
видами діяльності)»

освітньо-професійна програма «Національна фінансова безпека»

Статус дисципліни: обов'язкова

Робоча програма навчальної дисципліни «Інформаційна безпека держави» укладена на основі освітньо-професійної програми «Національна фінансова безпека» другого (магістерського) освітнього рівня спеціальності КЗ «Національна безпека (за окремими сферами забезпечення і видами діяльності)», затвердженої Вченою радою Університету 29.05.2025 протокол № 15.

Укладач:



А. ГАРБІНСЬКА-РУДЕНКО,
к.ю.н., доцент, доцент кафедри
фінансового та податкового
права

Гарант освітньої програми
«Національна фінансова
безпека»



А. ГАРБІНСЬКА-РУДЕНКО,
к.ю.н., доцент, доцент кафедри
фінансового та податкового
права

Робочу програму навчальної дисципліни розглянуто та схвалено кафедрою фінансового та податкового права, від 04.11.25 № 4/1

Завідувач кафедри



М. ГЛУХ, к.ю.н., професор

Розглянуто і схвалено вченою радою Навчально-наукового інституту права, від 04.11.25 № 8.

Голова вченої ради
Навчально-наукового інституту
права



В. ТОПЧІЙ,
д.ю.н., професор

Завідувач навчально-методичного
відділу



Г. ГРИЦУК,
доктор філософії

Реєстраційний № _____

Зміст

1. ПЕРЕДМОВА.....	4
2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....	5
3. КОМПЕТЕНТНОСТІ І РЕЗУЛЬТАТИ НАВЧАННЯ.....	5
4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....	6
5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....	8
6. ПИТАННЯ ПІДСУМКОВОГО КОНТРОЛЮ.....	11
7. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ	13
8. РЕКОМЕНДОВАНА ЛІТЕРАТУРА.....	15
9. ЛИСТ МОНІТОРИНГУ ТА ДОДАТКИ	17

1. ПЕРЕДМОВА

Анотація навчальної дисципліни. З кожним роком інформаційна безпека та інформаційна політика набувають все більш глобального характеру. Наразі виникає багато загальнодержавних проблем, що пов'язані із забезпеченням інформаційної безпеки. Інформаційна безпека – це захищеність (стан захищеності) основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об'єктивність, доступність і конфіденційність. Інформаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

Метою навчальної дисципліни є опанування майбутніми фахівцями науково-методичних знань та аналітико-розрахункових і управлінських навичок в сфері інформаційної безпеки держави, її ролі та значення у економіці держави, досвіду її забезпечення.

Завдання курсу полягає у вивченні основ інформаційної безпеки держави.

Міждисциплінарні зв'язки. Дисципліни-пререквізити: «Інституційні засади запобігання загрозам територіальній цілісності та екстремізму», «Державний розвиток в умовах загроз національній безпеці», «Методологія, організація та технологія наукових досліджень (з модулем «Академічне письмо»)». Дисципліни-постреквізит: «Стратегічне планування та впровадження інновацій у фінансовій безпеці», «Протидія ухилення від сплати податків».

Методи навчання: пояснювально-ілюстративний, репродуктивний, частково-пошуковий, метод проблемного викладу, робота в малих групах, методи інтерактивного навчання (ділові ігри, круглі столи тощо), блоковий метод, метод проєктів, використання комп'ютерних технологій тощо. Серед форм викладання навчальної дисципліни переважають лекційні, семінарські заняття, дискусії, презентації, моделювання професійних ситуацій, мозкові штурми, індивідуально-консультаційна робота під керівництвом викладача та самостійна робота здобувачів, при виконанні якої здобувач має звертатись до роботи в мережі Internet, працювати з першоджерелами, виконувати різні види завдань, звертатись до самостереження та самоаналізу.

Форми організації занять: лекційні заняття, семінарські заняття, самостійна та індивідуально-консультаційна робота, розгляд та аналіз ситуаційних завдань, кейсів, застосування інформаційних технологій та елементи дистанційного навчання в системі Moodle.

Форми та засоби діагностики результатів навчання. Контроль успішності навчання здобувачів проводиться у формах поточного і підсумкового контролю. Формами поточного контролю є:

- усне опитування;
- тестування;
- розв'язання задач, виконання вправ, певних розрахунків.
- письмові модульні контрольні роботи.

Підсумковий контроль проводиться у формі диференційованого заліку (2 семестр) та екзамену (3 семестр).

Організація поточного та підсумкового контролю здійснюється з використанням засобів дистанційного навчання в системі Moodle.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Характеристика навчальної дисципліни для здобувачів другого (магістерського) рівня вищої освіти (120 год/4 кредити ЄКТС)

Показник	Характеристика навчальної дисципліни	
	денна форма навчання	заочна форма навчання
Кількість кредитів ЄКТС - 4	Рік підготовки:	
Модулів - 2	1-й; 2-й	1-й; 2-й
Змістових модулів - 2	Семестр	
	2-й, 3-й	2-й, 3-й
	Лекції	
Загальна кількість годин – 120	(12+12) 24 год.	(4+2) 6 год.
	Семінарські	
	(8+8) 16 год.	(2+2) 4 год.
	Лабораторні	
		-
	Самостійна робота	
	(39+39) 76 год.	(54+54) 106 год.
	Індивід.-консультаційна робота: (1+1) 2 / (2+2) 4 год.	
	Форма семестрового контролю: диф.залік (2-й семестр); екзамен (3-й семестр)	

3. КОМПЕТЕНТНОСТІ І РЕЗУЛЬТАТИ НАВЧАННЯ

Після вивчення курсу здобувачі вищої освіти повинні володіти наступними компетентностями та програмними результатами навчання:

Компетентності	Результати
ІК. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (за окремими сферами забезпечення і видами діяльності).	РН3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.
<i>Спеціальні</i> СК 1. Здатність здійснювати професійну діяльність у відповідних сферах національної безпеки.	РН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища

СК 3. Здатність використовувати понятійно-категоріальний апарат теорії національної безпеки, аналізувати та розвивати структуру системи забезпечення національної безпеки та принципи її функціонування	РН11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності
СК 4. Здатність аналізувати та прогнозувати розвиток безпекового середовища (глобальний, регіональний та національний аспекти) за окремими сферами забезпечення та видами діяльності	РН12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки.
СК 7. Здатність інтегрувати знання та розв'язувати складні задачі національної безпеки (за окремими сферами забезпечення і видами діяльності) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	етичних норм.
Фахові ФК 4. Здатність до забезпечення національних інтересів держави у кіберпросторі.	РН18. Аналізувати міжнародний механізм у частині забезпечення процедур розшуку та арешту активів, що були отримані незаконним шляхом. РН19. Застосовувати спеціальні знання з метою забезпечення національних інтересів держави у кіберпросторі в умовах гібридних загроз національній фінансовій безпеці.

4.СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

для здобувачів другого (магістерського) рівня вищої освіти денної форми навчання
(120 год/4 кредити ЄКТС)

№ п/п	ЗМІСТОВІ МОДУЛІ	Кількість годин					Всього
		Лекції	Семінарські заняття	Практичні заняття	індивідуальна робота	Самостійна робота	
МОДУЛЬ 1= 2 з.к. (60 год.) ЗМ 1. Категорії інформаційної безпеки (Теми. 1-3)							
1	Поняття інформаційної безпеки держави, суспільства та особи	4	2			12	18
2	Небезпеки для інформаційної безпеки держави	4	4			12	20
3	Принципи, форми та методи забезпечення інформаційної безпеки держави	4	2		1	15	22
Всього по модулю		12	8		1	39	60
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - 40 хв.) Форма підсумкового контролю: диф.залік							

МОДУЛЬ 2= 2 з.к. (60 год.) ЗМ 2. Забезпечення інформаційної безпеки держави (Т. 4-8)							
4	Поняття та зміст інформаційного протиборства	2	1			7	10
5	Джерела загроз безпеці інформації	2	1			7	10
6	Забезпечення інформаційної безпеки України	2	2			8	12
7	Система та політика забезпечення інформаційної безпеки України	2	2			8	12
8	Інформаційна безпека України у сфері прав і свобод людини	4	2		1	9	16
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - 40 хв.)							
Всього по модулю		12	8		1	39	60
Форма підсумкового контролю : екзамен							
Разом годин з курсу		24	16		2	78	120

для здобувачів другого (магістерського) рівня вищої освіти заочної форми навчання
(120 год/4 кредити ЄКТС)

№ п/п	ЗМІСТОВІ МОДУЛІ	Кількість годин					Всього
		Лекції	Семінарські заняття	Практичні заняття	індивідуальна робота	Самостійна робота	
МОДУЛЬ 1= 2 з.к. (60 год.) ЗМ 1. ЗМ 1. Категорії інформаційної безпеки (Теми. 1-3)							
1	Поняття інформаційної безпеки держави, суспільства та особи	2	2			20	24
2	Небезпеки для інформаційної безпеки держави	2				20	22
3	Принципи, форми та методи забезпечення інформаційної безпеки держави				2	12	14
Всього по модулю		4	2		2	52	60
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - 40 хв.) Форма підсумкового контролю: диф.залік							
МОДУЛЬ 2= 2 з.к. (60 год.) ЗМ 2. Забезпечення інформаційної безпеки держави (Т. 4-8)							
4	Поняття та зміст інформаційного протиборства					10	10
5	Джерела загроз безпеці інформації					10	10
6	Забезпечення інформаційної безпеки України	2	2			10	14
7	Система та політика забезпечення інформаційної безпеки України					10	10

8	Інформаційна безпека України у сфері прав і свобод людини				2	14	16
	Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - 40 хв.)						
Всього по модулю		2	2		2	54	60
Форма підсумкового контролю : екзамен							
Разом годин з курсу		6	4		4	106	120

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МОДУЛЬ 1

ЗМ 1. (Теми. 1-3). Категорії інформаційної безпеки

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи

План лекційного заняття

1. Інформаційна безпека (поняття і визначення)
2. Підходи до визначення поняття «інформаційна безпека»
3. Інтереси особи, суспільства та держави в інформаційній сфері
4. Об'єкти, суб'єкти та види інформаційної безпеки
5. Співвідношення понять інформаційної та кібербезпеки

План семінарського заняття

1. Інформаційна безпека (поняття і визначення)
2. Підходи до визначення поняття «інформаційна безпека»
3. Інтереси особи, суспільства та держави в інформаційній сфері
4. Об'єкти, суб'єкти та види інформаційної безпеки
5. Співвідношення понять інформаційної та кібербезпеки

Самостійна робота здобувачів вищої освіти

1. Організаційно-правові засади становлення та розвитку системи інформаційної безпеки в Україні.
2. Механізм та системи забезпечення інформаційної безпеки держави.
3. Концепція, стратегія, політика і тактика забезпечення інформаційної безпеки держави.

Рекомендована література: [3; 6; 1; 8].

Тема 2. Небезпеки для інформаційної безпеки держави

План лекційного заняття

1. Поняття загроз інформаційній безпеці.
2. Види загроз інформаційній безпеці.
3. Фактори загроз інформаційній безпеці.
4. Джерела загроз інформаційній безпеці.

План семінарського заняття

1. Поняття загроз інформаційній безпеці.
2. Види загроз інформаційній безпеці.
3. Фактори загроз інформаційній безпеці.
4. Джерела загроз інформаційній безпеці

Самостійна робота здобувачів вищої освіти

1. Етапи розвитку засобів інформаційних комунікацій.
2. Індикатори інформаційної безпеки.
3. Вплив соціальної політики на інформаційну безпеку.

Рекомендована література: [1; 6; 7; 9; 19].

Тема 3. Принципи, форми та методи забезпечення інформаційної безпеки держави

План лекційного заняття

1. Основні принципи забезпечення інформаційної безпеки держави.
2. Основні форми забезпечення інформаційної безпеки держави.
3. Методи забезпечення інформаційної безпеки.

План семінарського заняття

1. Основні принципи забезпечення інформаційної безпеки держави.
2. Основні форми забезпечення інформаційної безпеки держави.
3. Методи забезпечення інформаційної безпеки.

Самостійна робота здобувачів вищої освіти

1. Ключових елементів національної безпеки держави.
2. Ризики інформаційної безпеки.
3. Фінансова нестабільність та інформаційна безпека держави.

План індивідуально-консультаційної роботи

1. Розробити презентацію на тему «Забезпечення інформаційної безпеки держави». Презентація має містити схематичне відображення проблематики (не менше 15 слайдів).

Рекомендована література: [1-4; 5; 7;12]

Модуль 2

ЗМ 2. (Т.4-8). Забезпечення інформаційної безпеки держави

Тема 4. Поняття та зміст інформаційного протиборства

План лекційного заняття

1. Поняття «інформаційного протиборства».
2. Рівні проведення інформаційного протиборства.
3. Ступені інформаційного протиборства.
4. Основні форми інформаційної війни.

План семінарського заняття

1. Поняття «інформаційного протиборства».
2. Рівні проведення інформаційного протиборства.
3. Ступені інформаційного протиборства.
4. Основні форми інформаційної війни.

Самостійна робота здобувачів вищої освіти

1. Інформаційна зброя як сучасний засіб ураження.
2. Сфера застосування інформаційної зброї.
3. Об'єкти застосування інформаційної зброї.
4. Комп'ютерні віруси: поняття та види.

Рекомендована література: [1; 6; 7; 17;19]

Тема 5. Джерела загроз безпеці інформації

План лекційного заняття

1. Поняття та загальні властивості інформації.
2. Поняття загроз.
3. Загрози безпеки інформації та інформаційних ресурсів.
4. Класифікація вразливостей безпеки.
5. Моделі порушень інформаційних ресурсів.
6. Побудова моделі порушника.

План семінарського заняття

1. Поняття та загальні властивості інформації.
2. Поняття загроз.
3. Загрози безпеки інформації та інформаційних ресурсів.
4. Класифікація вразливостей безпеки.

5. Моделі порушень інформаційних ресурсів.
6. Побудова моделі порушника.

Самостійна робота здобувачів вищої освіти

1. Джерела та фактори загроз інформації.
2. Класифікація вразливостей безпеці інформації.
3. Класи (види) загроз в інформаційній сфері.
4. Категорії джерел конфіденційної інформації.

Рекомендована література: [2-4; 7; 9; 16]

Тема 6. Забезпечення інформаційної безпеки України

План лекційного заняття

1. Інформаційна безпека і її місце в системі національної безпеки України.
2. Основні реальні та потенційні загрози інформаційній безпеці України.
3. Стан та перспективи розвитку інформаційної безпеки України.
4. Заходи управління інформаційною безпекою.

План семінарського заняття

1. Інформаційна безпека і її місце в системі національної безпеки України.
2. Основні реальні та потенційні загрози інформаційній безпеці України.
3. Стан та перспективи розвитку інформаційної безпеки України.
4. Заходи управління інформаційною безпекою.

Самостійна робота здобувачів вищої освіти

1. Джерела конфіденційної інформації.
2. Інформаційна система як об'єкт захисту інформації.
3. Рівні захисту інформаційних систем.

Рекомендована література: [3; 6; 7; 8; 19]

Тема 7. Система та політика забезпечення інформаційної безпеки України

План лекційного заняття

1. Основні функції системи забезпечення інформаційної безпеки України.
2. Мета функціонування та завдання системи забезпечення інформаційної безпеки.
3. Органи забезпечення інформаційної безпеки і захисту інформації.
4. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.

План семінарського заняття

1. Основні функції системи забезпечення інформаційної безпеки України.
2. Мета функціонування та завдання системи забезпечення інформаційної безпеки.
3. Органи забезпечення інформаційної безпеки і захисту інформації.
4. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.

Самостійна робота здобувачів вищої освіти

1. Об'єкти системи забезпечення інформаційної безпеки України.
2. Функції системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації.
3. Державна система захисту інформації.

Рекомендована література: [1-5; 7; 11]

Тема 8. Інформаційна безпека України у сфері прав і свобод людини

План лекційного заняття

1. Забезпечення захисту прав і свобод людини в інформаційній сфері
2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.

3. Структура конституційного права на інформацію.
4. Нормативно-правове забезпечення інформаційної безпеки України.

План семінарського заняття

1. Забезпечення захисту прав і свобод людини в інформаційній сфері
2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.
3. Структура конституційного права на інформацію.
4. Нормативно-правове забезпечення інформаційної безпеки України.

Самостійна робота здобувачів вищої освіти

1. Зміст інформації, що входить до інформаційних ресурсів України.
2. Забезпечення інформаційного суверенітету України.
3. Засади інформаційної безпеки держави згідно Закону України «Про національну безпеку України».

План індивідуально-консультаційної роботи

1. Розробити презентацію на тему «Захисту прав і свобод людини в інформаційній сфері». Презентація має містити схематичне відображення проблематики (не менше 15 слайдів).

Рекомендована література: [3; 6; 7;15;21]

6. ПИТАННЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Підходи до визначення поняття «інформаційна безпека».
2. Інформаційна безпека (поняття і визначення).
3. Інтереси особи, суспільства та держави в інформаційній сфері.
4. Об'єкти, суб'єкти та види інформаційної безпеки.
5. Співвідношення понять інформаційної та кібербезпеки.
6. Організаційно-правові засади становлення та розвитку системи інформаційної безпеки в Україні.
7. Механізм та системи забезпечення інформаційної безпеки держави.
8. Концепція, стратегія, політика і тактика забезпечення інформаційної безпеки держави.
9. Поняття загроз інформаційній безпеці.
10. Види загроз інформаційній безпеці.
11. Фактори загроз інформаційній безпеці.
12. Джерела загроз інформаційній безпеці.
13. Етапи розвитку засобів інформаційних комунікацій .
14. Основні принципи забезпечення інформаційної безпеки держави.
15. Основні форми забезпечення інформаційної безпеки держави.
16. Методи забезпечення інформаційної безпеки.
17. Основні форми інформаційного протидіювання.
18. Основні форми інформаційної війни.
19. Інформаційна зброя в інформаційній війні .
20. Поняття «інформаційного протидіювання».
21. Рівні проведення інформаційного протидіювання.
22. Ступені інформаційного протидіювання.
23. Основні форми інформаційної війни.
24. Поняття та загальні властивості інформації.
25. Загрози безпеки інформації та інформаційних ресурсів.
26. Класифікація вразливостей безпеки.
27. Моделі порушень інформаційних ресурсів.
28. Інформаційна безпека і її місце в системі національної безпеки України.
29. Основні реальні та потенційні загрози інформаційній безпеці України.
30. Стан та перспективи розвитку інформаційної безпеки України.

31. Заходи управління інформаційною безпекою.
32. Джерела конфіденційної інформації.
33. Інформаційна система як об'єкт захисту інформації.
34. Рівні захисту інформаційних систем.
35. Основні функції системи забезпечення інформаційної безпеки України.
36. Мета функціонування та завдання системи забезпечення інформаційної безпеки.
37. Органи забезпечення інформаційної безпеки і захисту інформації.
38. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.
39. Забезпечення захисту прав і свобод людини в інформаційній сфері.
40. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.
41. Структура конституційного права на інформацію.
42. Нормативно-правове забезпечення інформаційної безпеки України.
43. Виклики для інформаційного суверенітету України в умовах гібридної війни.
44. Вплив зовнішніх інформаційних операцій на національну безпеку України.
45. Підвищення цифрової грамотності як частина стратегічної оборони держави.
46. Роль державних інституцій у захисті інформаційного суверенітету.
47. Застосування законодавчих ініціатив для забезпечення інформаційної безпеки України.
48. Проблеми боротьби з фейковими новинами та дезінформацією.
49. Співпраця з міжнародними партнерами у сфері інформаційної безпеки.
50. Захист національної інформаційної інфраструктури від кібератак.
51. Роль медіа у забезпеченні державної інформаційної безпеки.
52. Регулювання контенту та його вплив на інформаційну політику країни.
53. Оцінка ефективності інформаційної політики в Україні.
54. Захист персональних даних у цифровому середовищі.
55. Технології захисту інформації в умовах глобалізації та цифровізації.
56. Проблеми етики та прозорості в інформаційній сфері.
57. Роль національних ІТ-компаній у забезпеченні інформаційної незалежності.
58. Взаємодія між державним сектором та приватними компаніями в сфері кібербезпеки.
59. Використання технологій штучного інтелекту для боротьби з інформаційними загрозами.
60. Вплив інформаційних війн на репутацію держави на міжнародній арені.

7. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Денна форма навчання

Модулі	Змістовний модуль 1 - (50 балів) (2 семестр)					Контрольний захід	Диференційований залік - 50 балів	Загальна оцінка з курсу = 100 балів	
Загальна кількість балів за модулем №1	35								11
Теми	T.1	T.2	T.3						
Семінарське заняття	6	6+6	6						
Самостійна робота	Оцінювання самостійної роботи здійснюється під час семінарських занять та написання контрольної роботи								
Індивідуально-консультаційна робота	10								
Підсумковий тестовий контроль на порталі дистанційної освіти Moodle	5								
Модулі	Змістовний модуль 2 - (50 балів) (3 семестр)					Контрольний захід	Екзамен - 50 балів	Загальна оцінка з курсу = 100 балів	
Загальна кількість балів за модулем №2	35								11
Теми	T.4	T.5	T.6	T.7	T.8				
Семінарське заняття	3	3	6	6	6				
Самостійна робота	Оцінювання самостійної роботи здійснюється під час семінарських занять та написання контрольної роботи								
Індивідуально-консультаційна робота	10								
Підсумковий тестовий контроль на порталі дистанційної освіти Moodle	5								

Заочна форма навчання

Модулі		Змістовний модуль 1 - (50 балів) (2 семестр)				Контрольний захід	Диференційований залік - 50 балів	Загальна оцінка з курсу = 100 балів		
Загальна кількість балів за модулем №1		35							20	
Теми		T.1	T.2	T.3						
Семінарське заняття		15								
Самостійна робота		Оцінювання самостійної роботи здійснюється під час семінарських занять та написання контрольної роботи								
Індивідуально-консультаційна робота		10								
Підсумковий тестовий контроль на порталі дистанційної освіти Moodle		5								
Модулі		Змістовний модуль 2 - (50 балів) (3 семестр)					Контрольний захід	Екзамен - 50 балів	Загальна оцінка з курсу = 100 балів	
Загальна кількість балів за модулем №2		35								20
Теми		T.4	T.5	T.6	T.7	T.8				
Семінарське заняття				15						
Самостійна робота		Оцінювання самостійної роботи здійснюється під час семінарських занять та написання контрольної роботи								
Індивідуально-консультаційна робота		10								
Підсумковий тестовий контроль на порталі дистанційної освіти Moodle		5								

Критерії оцінювання роботи на семінарських заняттях

Максимальна кількість балів, отриманих здобувачем вищої освіти на семінарському занятті становить 6 балів (денна форма навчання) та 15 балів (заочна форма навчання). Виконання самостійної роботи оцінюється під час проведення семінарського заняття у вигляді опитування в тому числі за питаннями, які виносяться на самостійну роботу.

Таблиця 4.1

Шкала оцінювання роботи здобувачів вищої освіти на семінарських заняттях

Критерії оцінювання	Кількість балів
Оцінюється робота здобувача, який у повному обсязі дав відповіді на всі питання. При цьому використовував актуальну наукову термінологію, належним чином обґрунтовував свої думки та зробив узагальнені підсумки.	6/15
Оцінюється робота здобувача, який в основному розкрив зміст теоретичних питань. Проте, при висвітленні деяких питань не вистачало достатньої аргументації, допускалися при цьому окремі неістотні неточності та незначні помилки.	4/12
Оцінюється робота здобувача, який дав фрагментарні відповіді на теоретичні питання (без аргументації й обґрунтування, підсумків), у відповідях присутні неточності та помилки або відповідь дана лише на окремі питання.	2/7
Оцінюється робота здобувача вищої освіти, який дав неправильну відповідь на всі теоретичні питання, допустив істотні помилки, оперував неактуальною застарілою інформацією або відповіді на питання відсутні взагалі.	0

Критерії оцінювання модульних контрольних робіт

Формою проміжного поточного контролю є модульні контрольні роботи, які проводяться у письмовій формі та кожна з яких оцінюється від 0 до 11 балів (денна форма навчання) та від 0 до 20 балів (заочна форма навчання) (табл. 4.2).

Таблиця 4.2

Розподіл балів за різні види завдань в межах модульної контрольної роботи

Вид завдання	Максимальна кількість балів за виконання
Теоретичні питання	5/10
Тестовий блок	5/5
Практичні завдання	1/5
Всього	11/20

Критерії оцінювання індивідуально-консультаційної роботи

Індивідуально-консультаційна робота виконується у формі презентації на одну із запропонованих тем і оцінюється від 0 до 10 балів (денна та заочна форма навчання). (табл. 4.3).

Таблиця 4.3

Шкала оцінювання індивідуально-консультаційної роботи здобувачів вищої освіти

Критерії оцінювання	Кількість балів
Послідовність, логічність викладення інформації в презентації та, відповідно, її захист, а також виокремлення з різних джерел основних положень, які структурно об'єднанні, проаналізовані та узагальнені висновками.	10

Послідовність, логічність написання презентації, але без захисту.	7
Не підготовка презентації.	0

Підсумкове оцінювання знань здобувачів вищої освіти здійснюється за результатами поточного контролю (від 0 до 50 балів) та диференційованого заліку (2 семестр)/екзамену (3 семестр) (від 0 до 50 балів). Критерієм успішного проходження здобувачем освіти підсумкового оцінювання є отримання не менше 25 балів за поточний контроль та 25 балів за підсумковий контроль у формі диференційованого заліку/екзамену.

Загальний розподіл балів, які здобувач вищої освіти може отримати в межах 100-бальної системи оцінювання, включає обов'язкове комп'ютерне тестування на платформі дистанційного навчання ДПУ Moodle (максимально до 5 балів).

Неформальна освіта

Таблиця 4.4

Шкала та критерії перезарахування результатів навчання, здобутих в неформальній освіті здобувача (до 25% обсягу контактних годин дисципліни)

Кількість балів	Форма заняття та діяльності	Критерії оцінювання	Рекомендовані ресурси для здобуття результату
10	Індивідуально-консультаційна робота	Оцінюється робота за результатами надання сертифікату обсягом 30 годин (1 кредит ECTS) або більше	Масові онлайн курси https://www.dpu.edu.ua/osvita/neformalnainformalna-osvita
6/15	Семінарське заняття	Оцінюється робота за результатами надання сертифікату за темою заняття	Масові онлайн курси на платформі EdERA, Прометеус тощо. Онлайн курси мережевої академії Cisco (https://www.netacad.com/) тощо
0		Відсутній результат або результат не відповідає тематиці дисципліни	

8. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

1. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
2. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник. Київ: ТОВ «СІК ГРУП Україна», 2021. 449 с.
3. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2021. 172 с.
4. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
5. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

Допоміжна:

6. Білий В. І., Михальчук В. М. Основні напрями забезпечення національної безпеки держави. *Інвестиції : практика та досвід*. 2021. № 17. С. 92–98.
7. Гаврильців М. Т. Інформаційна безпека держави у системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203. URL : <https://dspace.lvduvs.edu.ua/handle/1234567890/2927>

8. Горулько В. В. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави. *Вісник Харківського національного В. Н. Каразіна*. Серія «Право». 2022. Вип. 34. С. 103–108.
9. Ніколаєнко Н. О., Комарчук О. О. Засоби масової комунікації як детермінанти гібридної війни : монографія / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2021. 217 с. 17.
10. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 331 с.
11. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України : підручник ; за ред. Г. П. Ситника. Київ : Міжрегіональна Академія управління персоналом, 2021. 372 с.
12. Ситник Г. П. Основи теорії управління у сфері національної безпеки : курс лекцій. Київ : «ТОВ САК ЛТД», 2023. 178 с.

Інформаційні ресурси Інтернет:

13. Офіційний веб-сайт Ради національної безпеки і оборони України URL: <https://www.rnbo.gov.ua/>
14. Офіційний веб-сайт Кіберполіції України URL: <https://cyberpolice.gov.ua/>
15. Офіційний веб-сайт Центру стратегічних комунікацій URL: <https://spravdi.gov.ua/>
16. Офіційний веб-сайт Міністерства оборони України URL: <http://www.mil.gov.ua/>
17. Офіційний веб-сайт Міністерства фінансів України [URL: <http://www.mof.gov.ua/>

Міжнародні видання:

18. Global Peace Index 2024. URL: https://globalexchange.org/a-growing-movement-for-peace-across-the-border/?gad_source=1&gclid=Cj0KCQjwjY64BhCaARIsAIfc7YbnluRkf8tBjWPB-7fuM6pytfRO3RYJGnQE8iGZH7yoNBDtwCm561AaAl0nEALw_wcB
19. Глобальний індекс тероризму 2023 р. URL: <https://finap.com.ua/gti-globalnyj-indeks-teroryzmu-2023/>
20. Economic freedom index. URL.: <https://www.heritage.org/index/> .
21. Nadežda Semjonova. View More Financial Security in the Baltic States: Comparison with Selected EU Countries. Economics and Business. <https://doi.org/10.1515/eb-2022-0026>

**ЛИСТ ОНОВЛЕННЯ ТА ПЕРЕЗАТВЕРДЖЕННЯ
РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

РОЗГЛЯНУТО ТА СХВАЛЕНО
на засіданні кафедри фінансового
та
податкового права
від _____ 20__ р. № ____.

Укладач:

А. ГАРБІНСЬКА-РУДЕНКО, к.ю.н.,
доцент, доцент кафедри фінансового
та податкового права

Лист оновлення та перезатвердження робочої програми навчальної дисципліни

(протягом 5 років після затвердження або до затвердження освітньої програми)

Навчальний рік	Дата засідання кафедри	Номер протоколу	Підпис завідувача кафедри	Підпис гаранта ОП