

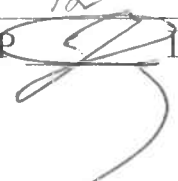
МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут права
Кафедра фінансового та податкового права

Затверджено

Науково-методичною радою ДПУ,

від «12» 12 2024 р. № 5

Голова НМР  Іван ШЕМЕЛИНЕЦЬ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Інформаційна безпека держави»

для підготовки здобувачів вищої освіти другого (магістерського) рівня
заочної форми навчання

галузь знань 25 «Воєнні науки, національна безпека, безпека державного
кордону»

спеціальність 256 «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» складена і
основі освітньо-професійної програми «Національна фінансова безпека», затверджені Вчено
радою Університету 29.08.2024 року, протокол № 1.

Укладачі

Альона ГАРБІНСЬКА-РУДЕНКО, к.ю.н., доцент

Гарант освітньо-професійної програми
«Національна фінансова безпека»

Олег БОДНАРЧУК, д.ю.н., професор

Робочу програму навчальної дисципліни розглянуто та схвалено кафедрою фінансового та
податкового права, протокол від « 7 » 11 2024 р. № 5.

Завідувача кафедри

Марина ГЛУХ, к.ю.н., професор

Розглянуто і схвалено вченою радою Навчально-наукового інституту права
протокол від « 13 » 11 2024 р. № 4.

Голова вченої ради ННІ права

Василь ТОПЧІЙ, д.ю.н., професор

Завідувач навчально-методичного
відділу

Ірина Качур, к.біол.н., доцент

Реєстраційний № _____

ЛИСТ ОНОВЛЕННЯ ТА ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

РОЗГЛЯНУТО ТА СХВАЛЕНО
на засіданні кафедри фінансового та
податкового права
від _____ 202__ р. № _____.

Лист оновлення та перезатвердження РПНД

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри	Підпис гаранта ОП

Зміст робочої програми навчальної дисципліни

1. ПЕРЕДМОВА.....	4
2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	5
2.1. КОМПЕТЕНТНОСТІ І РЕЗУЛЬТАТИ НАВЧАННЯ.....	5
2.2. ПРЕРЕКВІЗИТИ ТА ПОСТРЕКВІЗИТИ.....	6
2.3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....	7
3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....	10
4. КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ.....	14
5. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ.....	16
6. ФОРМИ ТА ПИТАННЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ.....	16
7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА	20

1. ПЕРЕДМОВА

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 курсу є досконале 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.

Об'єктом вивчення курсу є інформаційна безпека та процеси, що відбуваються різні аспекти інформаційної безпеки України.

Предметом вивчення курсу є сукупність форм та методів виявлення та попередження загроз інформаційній безпеці країни, видів і класифікації загроз, дестабілізуючих факторів; методів та засобів забезпечення інформаційної безпеки держави.

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, індивідуальна-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 самопостереження та самоаналізу.

Організація поточного та підсумкового контролю знань: контроль роботи здобувача вищої освіти є необхідним компонентом навчального процесу, який має на меті визначення реального рівня професійної підготовки здобувача, а також надання необхідних рекомендацій, які будуть сприяти подальшому розвитку його творчої особистості. Об'єктами контролю є отримані здобувачами знання у процесі засвоєння матеріалу дисципліни на лекціях, семінарських заняттях, диспутах та під час виконання індивідуальних завдань. Логічним завершенням процесу контролю є процедура оцінювання отриманих здобувачем знань. Підсумковий контроль проводиться у формі диференційованого заліку (2 семестр) та екзамену (3 семестр).

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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

2.1. КОМПЕТЕНТНОСТІ І РЕЗУЛЬТАТИ 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 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. етичних норм.

СК 4. Здатність аналізувати та прогнозувати розвиток безпекового середовища (глобальний, регіональний та національний аспекти) за окремими сферами забезпечення та видами діяльності 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	
<i>Фахові</i> ФК 4. Здатність до забезпечення національних інтересів держави у кіберпросторі.	РН18. Аналізувати міжнародний механізм в 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.

2.2. ПРЕРЕКВІЗИТИ ТА ПОСТРЕКВІЗИТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Пререквізити дисципліни: «Інституційні засади запобігання загрозам територіальної цілісності та екстремізму», «Державний розвиток в умовах загроз національній безпеці», «Правове забезпечення діяльності сектору безпеки та оборони», «Теорія національної безпеки».

Постреквізити вивчення дисципліни є: «Міжнародне співробітництво у сфері розшуку активів, що одержані незаконним шляхом», «Стратегічне планування та впровадження інновацій у фінансовій безпеці», «Виявлення та розшук активів у кримінальному провадженні».

2.3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Академічна група ПМНБЗ-24-1

№ п/п	ЗМІСТОВІ МОДУЛІ	Кількість годин					Всього
		Лекції	Семінарські заняття	Практичні заняття	індивідуальн а робота	Самостійна робота	
МОДУЛЬ 1= 2 з.к. (60 год.) ЗМ 1 (Темп. 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 (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 : екзамєн							
Разом годин з курсу		6	4		4	106	120

РЕЙТИНГ-ПЛАН

Заочна форма навчання

Одиниці	Тема	Форма заняття та діяльності (лекція, семінар, практична робота, лабораторна робота, самостійна робота здобувача, контрольний захід, підсумкове тестування, індивідуальна робота)	Результати навчання	Вага оцінки (кількість балів)
			Модуль 1 (ЗМ 1. Т.1-3)	
2	1.Поняття інформаційної безпеки держави, суспільства та особи	Лекція	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.	0
2		Семінар		15
20		Самостійна робота		0
2	2. Небезпеки для інформаційної безпеки держави	Лекція	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..	0
0		Семінар		0
20		Самостійна робота		0
0	3.Принципи, форми та методи забезпечення інформаційної безпеки держави	Лекція	РН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища	0
0		Семінар		0
12		Самостійна робота		0
2		Індивідуальна консультаційна робота		10
	Тема 1-3	Модульний контроль		20
	Комп'ютерне тестування на платформі дистанційного навчання ДПУ MOODLE			5
60	Усього за модулем 1			50
	Диференційований залік			50
	Усього за курсом (2-й семестр)			100
			Модуль 2 (ЗМ 1. Т.4-8)	0
2	4. Поняття та зміст інформаційного протиборства	Лекція	РН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища	0
0		Семінар		0
10		Самостійна робота		0
0	5.Джерела загроз безпеці інформації	Лекція	РН11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності	0
0		Семінар		0
10		Самостійна робота		0

			PH12. 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. етичних норм.	
2	6. Забезпечення інформаційної безпеки України	Лекція	PH11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності	0
		Семінар		15
10		Самостійна робота	PH12. 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. етичних норм.	0
0	7. Система та політика забезпечення інформаційної безпеки України	Лекція	PH18. Аналізувати міжнародний механізм в частині забезпечення процедур розшуку та арешту активів, що були отримані незаконним шляхом.	0
0		Семінар		0
10		Самостійна робота	PH19. Застосовувати спеціальні знання з метою забезпечення національних інтересів держави у кіберпросторі в умовах гібридних загроз національній фінансовій безпеці.	0
0	8. Інформаційна безпека України у сфері прав і свобод людини	Лекція	PH18. Аналізувати міжнародний механізм в частині забезпечення процедур розшуку та арешту активів, що були отримані незаконним шляхом.	0
0		Семінар		0
14		Самостійна робота	PH19. Застосовувати спеціальні знання з метою забезпечення національних інтересів держави у кіберпросторі в умовах гібридних загроз національній фінансовій безпеці.	0
2		Індивідуальна консультаційна робота		10
	Т. 4-8	Модульний контроль		20
	Комп'ютерне тестування на платформі дистанційного навчання ДІТУ MOODLE			5
60	Усього за модулем 2			50
	Екзамен			50
	Усього за курсом (3-й семестр)			100

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Модуль 1 (ЗМ 1. Т.1-3)

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.

Питання для самоконтролю

1. Що розуміють під інформаційною безпекою держави?
2. Чим стратегія інформаційної безпеки відрізняється від тактики?
3. Які загрози інформаційної безпеки держави можна пояснити процесами глобалізації?

Рекомендована література:

основні [3; 6; 1; 8],
допоміжні [7; 8; 9],
інформаційні ресурси Інтернет [1-4; 7; 8]
міжнародні видання [5; 6; 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.

Самостійна робота здобувачів вищої освіти

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

Питання для самоконтролю

1. Як соціальна політика пов'язана із загрозами інформаційній безпеці держави?
2. Які індикатори можуть говорити про низький рівень інформаційної безпеки?
3. У чому полягають такі соціальні явища як маргіналізація, люмпенізація, соціальна поляризація та як вони пов'язані з інформаційною безпекою держави?

Рекомендована література:

основні [1; 6; 7; 9],
допоміжні [1; 8; 11],
інформаційні ресурси Інтернет [1-4; 10; 14]

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

Самостійна робота здобувачів вищої освіти

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

План індивідуально-консультаційної роботи

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

Питання для самоконтролю

1. Чому інформаційна безпека є одним з ключових елементів національної безпеки держави?
2. Як визначаються ризики інформаційної безпеки?
3. Чи шкодить фінансова нестабільність інформаційній безпеці держави?

Рекомендована література:

основні [1-4; 5; 7],

допоміжні [1-4; 7; 10;]

інформаційні ресурси Інтернет [1-5; 11;]

міжнародні видання [5; 6; 8]

Модуль 2 (ЗМ 1. Т.4-8)

Тема 4. Поняття та зміст інформаційного протидіювання

Самостійна робота здобувачів вищої освіти

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

Питання для самоконтролю

1. Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?
2. Назвіть сферу застосування інформаційної зброї.
3. Назвіть основні об'єкти застосування інформаційної зброї.
4. Що таке комп'ютерні віруси?
5. Які існують особливості застосування інформаційної зброї?

Рекомендована література:

основні [1; 6; 7],

допоміжні [1-5; 7-9]

інформаційні ресурси Інтернет [1-4; 7; 8; 10]

міжнародні видання [5; 6; 8]

Тема 5. Джерела загроз безпеці інформації

Самостійна робота здобувачів вищої освіти

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.

Питання для самоконтролю

1. Що є джерелом та фактором загрози інформації?
2. Які є види загроз комп'ютерної інформації?
3. Які є групи джерел загроз безпеці інформації?
4. Наведіть класифікацію вразливостей безпеці інформації?
5. Які класи (види) загроз розрізняються в інформаційній сфері?
6. Які загрози відносяться до рівня порушення конфіденційності ?
7. Які загрози відносяться до рівня порушення цілісності ?
8. Які існують категорії джерел конфіденційної інформації?
9. Які є моделі порушень інформаційних ресурсів?

Рекомендована література:

основні [2-4; 7; 9],

допоміжні [1-4; 5; 7; 10;],

інформаційні ресурси Інтернет [1; 7; 8; 12-14]

міжнародні видання [1-4; 5; 7]

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.

Питання для самоконтролю

1. Що розуміється під «інформаційною безпекою України»?
2. Яке її місце в системі національної безпеки України?
3. Основні напрями політики інформаційної безпеки України?
4. Найважливіші завдання у сфері інформаційної безпеки?
5. В яких сферах проявляються реальні та потенційні загрози безпеці України?
6. Охарактеризуйте загрози інформаційній безпеці України у війсьній сфері.

Рекомендована література:

основні [3; 6; 7; 8],

допоміжні [1-3; 7; 11;],

інформаційні ресурси Інтернет [3-6; 7; 8; 11]

міжнародні видання [5; 6; 8]

Тема 7. Система та політика забезпечення інформаційної безпеки України

Самостійна робота здобувачів вищої освіти

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.

Питання для самоконтролю

1. Які об'єкти системи забезпечення інформаційної безпеки України Ви знаєте?
2. Які можна виділити основні функції системи забезпечення інформаційної безпеки у умовах надзвичайної ситуації?
3. Сформулюйте найважливіші завдання у сфері інформаційної безпеки.
4. Які органи забезпечують інформаційну безпеку й захист інформації?
5. Які завдання у сфері інформаційної безпеки?
6. З чого складається державна система захисту інформації?

Рекомендована література:

основні [1-5; 7],

допоміжні [1-7; 11:],

інформаційні ресурси Інтернет [1-4; 7; 8]

міжнародні видання [5; 7-8]

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

Самостійна робота здобувачів вищої освіти

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 індивідуально-консультаційної роботи

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

Питання для самоконтролю

1. Яка інформація входить до інформаційних ресурсів України?
2. Чим забезпечується інформаційний суверенітет України?
3. Які засади інформаційної безпеки держави закладено у Закон України «Про національну безпеку України»?
4. Які види планування закладено у Закон України «Про національну безпеку України»?

Рекомендована література:

основні [3; 6; 7:],

допоміжні [1-7; 11:],

інформаційні ресурси Інтернет [1-5; 8; 12-14]

міжнародні видання [1-5; 6; 8]

4. КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Загальний розподіл балів, які здобувач вищої освіти може отримати в межах 100-бальної системи оцінювання, представлено в наступних таблицях:

Таблиця 1

Розподіл балів за семінарське заняття (заочної форма навчання)

Критерії оцінювання	Кількість балів
У повному обсязі дав відповіді на всі питання. При цьому використовував актуальну наукову термінологію, належним чином обґрунтовував свої думки та зробив узагальнені підсумки.	15-7
В основному розкрив зміст теоретичних питань. Проте, при висвітленні деяких питань не вистачало достатньої аргументації, допускалися при цьому окремі неістотні неточності та незначні помилки.	6-4
Дав фрагментарні відповіді на теоретичні питання (без аргументації й обґрунтування, підсумків), у відповідях присутні неточності та помилки або відповідь дана лише на окремі питання.	3-1
Дав неправильну відповідь на всі теоретичні питання, допустив істотні помилки, оперував неактуальною застарілою інформацією або відповіді на питання відсутні взагалі.	0

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

Виконання самостійної роботи оцінюється під час проведення семінарського заняття у вигляді опитування в тому числі за питаннями, які виносяться на самостійну роботу.

Формою проміжного поточного контролю є контрольні роботи, які проводяться письмово

Таблиця 2

Розподіл балів за різні види завдань в межах контрольної роботи

Вид завдання	Максимальна кількість балів за виконання (заочна форма навчання)
Теоретичні питання	10
Тестовий блок	10
Всього	20

Критерії оцінювання індивідуально-консультаційної роботи

Виконання індивідуальної роботи передбачає розробку презентацій за тематикою навчальної дисципліни. Презентації мають містити схематичне відображення проблематики та містити не менше 15 слайдів.

Таблиця 3

Шкала оцінювання індивідуально-консультаційної роботи здобувачів вищої освіти

Кількість балів (заочна)	Критерії оцінювання
10-8	Послідовність, логічність підготовки презентації та її захист, виокремлення з різних джерел основних положень, які структурно об'єднанні, проаналізовані та узагальнені висновками.
7-4	Послідовність, логічність презентації, але без захисту.
0	Не зроблено презентацію.

Підсумкове оцінювання знань здобувачів вищої освіти здійснюється за результатами поточного контролю (від 0 до 50 балів) та диференційованого заліку чи екзамену (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 чи екзамену.

Переведення даних 100-бальної шкали оцінювання в національну шкалу та шкалу за системою ЄКТС здійснюється в такому порядку (табл.4.4).

Таблиця 4.4

Відповідність підсумкової рейтингової оцінки в балах оцінки за національною шкалою та шкалою ЄКТС

Сума балів за 100-бальною шкалою	Оцінка в ЄКТС	Значення оцінки ЄКТС	Оцінка за національною шкалою	
			Екзамен, курсова робота, практика, диференційований залік	Залік
90-100	A	відмінно	відмінно	зараховано
80-89	B	дуже добре	добре	
70-79	C	добре		
60-69	D	задовільно	задовільно	
50-59	E	достатньо		
35-49	FX	незадовільно з можливістю повторного складання	незадовільно	не зараховано
0-34	F	незадовільно з обов'язковим повторним вивченням курсу		

Результати складання диференційованого заліку чи екзамену оцінюються та вносяться у відомість обліку успішності здобувача вищої освіти, залікову книжку, індивідуальний навчальний план здобувача вищої освіти (крім «незадовільно»).

Визнання результатів навчання, здобутих у неформальній та/або ін формальній освіті, проводиться з врахуванням індивідуальних потреб та можливостей здобувача освіти, за необхідності – з використанням дистанційних технологій комунікації.

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	Індивідуальна 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
15	Семінарське заняття	Оцінюється робота за результатами надання сертифікату за темою семінарського заняття	Масові онлайн курси на платформі EdERA, Прометеус тощо. Онлайн курси мережевої академії Cisco (https://www.netacad.com/) тощо.

Перелік питань до диференційованого заліку

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.
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 протиборства.
18. Основні форми інформаційної війни.
19. Інформаційна зброя в інформаційній війні .
20. Поняття «інформаційного протиборства».
21. Рівні проведення інформаційного протиборства.
22. Ступені інформаційного протиборства.
23. Основні форми інформаційної війни.
24. Поняття та загальні властивості інформації.
25. Поняття загроз.

0		Відсутній результат або результат не відповідає тематичі дисципліни	
---	--	--	--

5. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

При вивченні навчальної дисципліни використовуються наступні засоби оцінювання:

- диференційований залік/ екзамен;
- тести;
- комп'ютерне тестування на платформі MOODLE ДПУ;
- презентації результатів виконаних завдань та досліджень;
- командні проекти;
- доповіді;
- студентські презентації та виступи на наукових заходах;
- інші види індивідуальних та групових завдань.

6. ФОРМИ ТА ПИТАННЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Форми поточного контролю:

- 1) проміжний модульний контроль;
- 2) підсумкова модульна контрольна робота;
- 3) письмові, усні опитування на семінарських заняттях;
- 4) есе, тези;
- 5) презентація;
- 6) огляд спеціальної літератури;
- 7) тестування за темами;
- 8) проведення круглих столів, участь у конференціях;
- 9) ділова гра.

В процесі поточного контролю оцінюється СРС над досліджуваним матеріалом: повнота виконання завдань, рівень засвоєння навчальних матеріалів та окремих розділів навчальної дисципліни, робота з додатковою літературою, вміння і навички презентацій, оволодіння практичними навичками аналітичної, дослідницької роботи тощо.

Перелік питань до модульного контролю №1

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. Види загроз інформаційній безпеці.
6. Фактори загроз інформаційній безпеці.
7. Джерела загроз інформаційній безпеці.
8. Етапи розвитку засобів інформаційних комунікацій.
9. Основні принципи забезпечення інформаційної безпеки держави.
10. Основні форми забезпечення інформаційної безпеки держави.
11. Методи забезпечення інформаційної безпеки.
12. Основні форми інформаційного протиборства.
13. Основні форми інформаційної війни.
14. Інформаційна зброя в інформаційній війні.
15. Поняття «інформаційного протиборства».
16. Рівні проведення інформаційного протиборства.
17. Ступені інформаційного протиборства.
18. Основні форми інформаційної війни.
19. Поняття та загальні властивості інформації.

Перелік питань до модульного контролю №2

1. Основні реальні та потенційні загрози інформаційній безпеці України.
2. Стан та перспективи розвитку інформаційної безпеки України.
3. Заходи управління інформаційною безпекою.
4. Джерела конфіденційної інформації.
5. Інформаційна система як об'єкт захисту інформації.
6. Рівні захисту інформаційних систем.
7. Основні функції системи забезпечення інформаційної безпеки України.
8. Мета функціонування та завдання системи забезпечення інформаційної безпеки.
9. Органи забезпечення інформаційної безпеки і захисту інформації.
10. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.
11. Забезпечення захисту прав і свобод людини в інформаційній сфері.
12. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.
13. Структура конституційного права на інформацію.
14. Поняття загроз.
15. Загрози безпеки інформації та інформаційних ресурсів.
16. Класифікація вразливостей безпеки.
17. Моделі порушень інформаційних ресурсів.
18. Інформаційна безпека і її місце в системі національної безпеки України.
19. Нормативно-правове забезпечення інформаційної безпеки України.

Перелік питань до диференційованого заліку

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.
6. Організаційно-правові засади становлення та розвитку системи інформаційної безпеки України.
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 протиборства.
18. Основні форми інформаційної війни.
19. Інформаційна зброя в інформаційній війні.
20. Поняття «інформаційного протиборства».
21. Рівні проведення інформаційного протиборства.
22. Ступені інформаційного протиборства.
23. Основні форми інформаційної війни.
24. Поняття та загальні властивості інформації.
25. Поняття загроз.

Перелік питань до екзамену

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.
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 протиборства.
18. Основні форми інформаційної війни.
19. Інформаційна зброя в інформаційній війні.
20. Поняття «інформаційного протиборства».
21. Рівні проведення інформаційного протиборства.
22. Ступені інформаційного протиборства.
23. Основні форми інформаційної війни.
24. Поняття та загальні властивості інформації.
25. Поняття загроз.
26. Загрози безпеки інформації та інформаційних ресурсів.
27. Класифікація вразливостей безпеки.
28. Моделі порушень інформаційних ресурсів.
29. Побудова моделі порушника.
30. Інформаційна безпека і її місце в системі національної безпеки України.
31. Основні реальні та потенційні загрози інформаційній безпеці України.
32. Стан та перспективи розвитку інформаційної безпеки України.
33. Заходи управління інформаційною безпекою.
34. Джерела конфіденційної інформації.
35. Інформаційна система як об'єкт захисту інформації.
36. Рівні захисту інформаційних систем.
37. Основні функції системи забезпечення інформаційної безпеки України.
38. Мета функціонування та завдання системи забезпечення інформаційної безпеки.
39. Органи забезпечення інформаційної безпеки і захисту інформації.
40. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.
41. Забезпечення захисту прав і свобод людини в інформаційній сфері.
42. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.
43. Структура конституційного права на інформацію.
44. Нормативно-правове забезпечення інформаційної безпеки України.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна:

1. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Видавництво Львівської політехніки, 2017. 204 с.
2. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова Ніжин: ФОП Лук'яненко В.В. ТПІК «Орхідея», 2018. 166 с.
3. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
4. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України : Указ Президента України від 18.06.2009 р. № 462/2009. URL: <https://zakon.rada.gov.ua/laws/show/63/2002#Text>
5. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник. Київ: ТОВ «СІК ГРУПІ Україна», 2015. 449 с.
6. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2018. 172 с.
7. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
8. Виговська О., Белоусова Н. Інформаційна складова національної безпеки України : кол. монографія / Ін-т міжнар. відносин, Київ. нац. ун-т ім. Тараса Шевченка, Київ. ун-т ім. Бориса Грінченка. Київ : Київ. ун-т ім. Б. Грінченка, 2017. 166 с.
9. 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:

1. Альван А. Наукові підходи до системи понять «національна безпека» : міжнародно-правовий аспект. *Аспекти публічного управління*. 2020. №7 (12), 70–77. URL : <https://doi.org/10.15421/151966>
2. Білий В. І., Михальчук В. М. Основні напрями забезпечення національної безпеки держави. *Вісник Національного університету цивільного захисту України*. 2021. № 17. С. 92–98.
3. 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>
4. 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.
5. Ключко А. М., Неклюєвський І. М., Коханенко В. Б. Національна безпека: поняття, сутність, характеристика. *Вісник Національного університету цивільного захисту України*. 2020. № 2. (13). С. 57–66.
6. 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.
7. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 331 с.
8. Панченко О. А. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України*. Серія: Державне управління. 2019. Випуск 3. 2019. URL : <http://77.222.145.174/index.php/governance/article/view/296/297>.
9. 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.
10. Ситник Г. П. Основи теорії управління у сфері національної безпеки : курс лекцій. Київ : «ТОВ САК Лтд», 2023. 178 с.
11. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

11. Міжнародна інформаційна безпека: теорія і практика : підруч. для студентів ВНЗ/ Є. Макаренко та ін. ; Київ. нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. Київ : Центр вільної преси, 2016. 417 с.

Інформаційні ресурси Інтернет:

1. Офіційне інтернет-представництво Президента URL: <http://www.president.gov.ua/>
2. Офіційний веб-портал Верховної Ради України URL: <http://www.rada.gov.ua/>
3. Офіційний веб-сайт Ради національної безпеки і оборони України URL: <https://www.rnbo.gov.ua/>
4. Офіційний веб-сайт Кіберполіції України URL: <https://cyberpolice.gov.ua/>
5. Офіційний веб-сайт Міністерства внутрішніх справ України URL: <http://mvs.gov.ua/mvs/control/main/uk/index>
6. Офіційний веб-сайт Центру стратегічних комунікацій URL: <https://spravdi.gov.ua/>
7. Офіційний портал Міністерства економіки України URL: <http://www.me.gov.ua/>
8. Офіційний веб-сайт Міністерства закордонних справ України URL: <http://mfa.gov.ua/ua>
9. Офіційний веб-сайт Міністерства оборони України URL: <http://www.mil.gov.ua/>
10. Офіційний веб-сайт Міністерства фінансів України [URL: <http://www.mof.gov.ua/>
11. Офіційний веб-сайт Державної прикордонної служби України URL: <http://dpsu.gov.ua/ua/>
12. Офіційний веб-сайт Державної податкової служби України URL: <https://tax.gov.ua/>
13. Офіційний веб-сайт Всесвітньої митної організації URL: <http://www.wcoomd.org>
14. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України URL: <https://cip.gov.ua/ua>

Міжнародні видання:

1. Global Peace Index 2024. URL: https://globalexchange.org/a-growing-movement-for-peace-across-the-border/?gad_source=1&gclid=Cj0KCQjwjY64BhCaARIsAIfc7YbnluRkf8tBjWPB-7fuM6pytfRO3RYJGnQE8iGZH7yoNBDtwCm561AaAl0nEALw_wcB
2. Глобальний індекс тероризму 2023 р. URL: <https://finap.com.ua/gti-globalnyj-indeks-teroryzmu-2023/>
3. Economic freedom index. URL: <https://www.heritage.org/index/>
4. Dmitro Starodub. Anti-corruption declaration: comparative legal analysis of Ukraine and the CIS countries / International Law and Inegration Problems (scientific-analitical and practical jornal). 1 (49) 2017. Baku. P. 56-63.
5. Bilous V., Ternushchak M., Starodub D. Improvement of the procedure for providing administrative services to taxpayers in the context of public administration reform / V. Bilous, M. Ternushchak, D. Starodub// Baltic Journal of Economic Studies, Vol. 4 (2018) No. 4. P. 45-49. DOI: <https://doi.org/10.30525/2256-0742/2018-4-4-45-49>
6. Brehov S., Starodub D. The Problem Of Identification Of Fiscally Transparent Entities For Tax Purposes In Ukraine. Daně – teorie a praxe 2018 sborník referátů a abstraktů XXI. ročníku mezinárodní odborné conference. Brno: Akademie Sting. 2018. P. 11–16
7. National Security Strategy. URL: https://www.whitehouse.gov/sites/default/files/docs/2023national_security_strategy.pdf.
8. 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>