МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут права
Кафедра приватного права

Затверджено
Науково-методичною радою ДПУ,
від «16» 03 2023 р. № 4
Голова НМР _____ І.І. Шемелинець

Робоча програма навчальної дисципліни
«Правове забезпечення інформаційної безпеки»
для підготовки здобувачів вищої освіти третього рівня
денної та заочної форми навчання
галузь знань 08 «Право»
спеціальність 081 «Право»
освітня програма: «Право»
статус дисципліни: обов'язкова

Ірпінь 2023

Робоча програма обов'язкової навчальної дисципліни «Правове забезпечення інформаційної безпеки» укладена на основі освітньої програми «Право» третього рівня галузі знань 08 «Право», спеціальність 081 «Право», затвердженої Вченою радою Університету «29» вересня 2022 року, протокол № 3.

Укладач _____ Н. Новицька д.ю.н., с.н.с., доцент, професор кафедри приватного права

Гарант освітньої програми _____ Ю.Аністратенко д.ю.н., професор

Робочу програму навчальної дисципліни розглянуто і схвалено кафедрою приватного права від «03» 03. 2023 № 15.

Завідувач кафедри
приватного права _____ І. Чеховська, професор, с.н.с., д.ю.н

Розглянуто і схвалено Вченою радою навчально-наукового інституту права від «06.» 03. 2023 р. № 10.

Голова вченої ради ННІ права _____ В. Топчій

Завідувач навчально-методичного відділу _____ І. Качур

Реєстраційний №_____

Зміст

ПЕРЕДМОВА

Одним із головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен має змогу створювати і накопичувати інформацію та знання, мати до неї вільний доступ, користуватися і обмінюватись ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові, та підвищувати якість життя. На сучасному етапі розвитку суспільства, пов'язаного з масовим використанням інформаційних технологій і створенням єдиного інформаційного простору, в рамкам якого відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми інформаційної безпеки набувають першорядного значення в усіх сферах суспільної і державної діяльності.

Нормальне функціонування суспільних інститутів та інших форм соціальної діяльності пов'язують із безпекою: для забезпечення безпеки суспільства створюються органи законодавчої, виконавчої та судової влади, силові структури забезпечення безпеки; у сфері підприємницької діяльності самі фірми створюють спеціальні структури забезпечення своєї безпеки, розробляють відповідний комплекс управлінських заходів і дій; у сфері екологічної та техногенної безпеки застосовуються як адміністративно-організаційні, техніко-технологічні засоби і системи, так і системи, котрі не допускають негативного впливу на навколишнє середовище.

Актуальність проблеми правового регулювання суспільних відносин у сфері інформаційної безпеки зумовлена підвищенням ролі інформації в усіх сферах і видах діяльності особистості та держави в умовах впливу зовнішніх і внутрішніх викликів, загроз, ризиків і небезпек, а також розвитком нових інформаційних відносин, котрі вимагають дотримання і захисту конституційних прав, законних інтересів суб'єктів в інформаційно-комунікаційній сфері.

Важливе місце у вирішенні проблеми забезпечення інформаційної безпеки займає реалізація системи комплексного захисту інформації, котра є поєднанням у єдине ціле окремих елементів, механізмів, процесів, явищ, заходів, засобів і програм захисту інформації, взаємозв'язок яких сприяє реалізації цілей, концептуального підходу до питань тимчасового функціонування і структурної побудови системи інформаційного забезпечення охорони і захисту. Особлива роль у реалізації інформаційної безпеки належить правовому захисту

Метою викладання навчальної дисципліни є забезпечення достатнього рівня теоретичних знань про сутність інформаційної безпеки, сформувати у здобувачів вищої освіти систему знань по інформаційній безпеці і захисту інформації, а також ознайомити їх із загальними принципами системи захисту інформації, концептуальною моделлю інформаційної безпеки, видами забезпечення системи захисту інформації: правовим, організаційним, апаратним, інформаційним, програмним, математичним, лінгвістичним, нормативно-методичним та формування практичних навичок захисту інформації у процесі здійснення публічної управлінської діяльності та адміністрування.

Завданнями навчальної дисципліни «Правове забезпечення інформаційної безпеки» є ознайомлення із загальні положення правового забезпечення інформаційної безпеки; вивчення правових аспектів інформаційної безпеки; поглиблене вивчення інформаційного законодавства як правової бази забезпечення інформаційної безпеки.

Методи навчання: При викладанні навчальної дисципліни застосовуються такі методи навчання, як: репродуктивний; проблемного навчання; евристичний (частково-пошуковий); дослідницький. Активізація навчально-пізнавальної діяльності здобувачів здійснюється через застосування таких форм навчання, як: проблемні лекції; семінари-дискусії, семінари-практикуми, семінари - розгорнуті бесіди; презентації навчальних матеріалів, виконаних творчих завдань; застосування наочних засобів (схеми, таблиці тощо); моделюючі вправи, розв'язування творчих завдань; роботу в Інтернеті, бібліотеці; консультації (настановні, контрольні, проблемні).

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 передбачає складання здобувачами диференційованого заліку.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Показники	Характеристика навчальної дисципліни	
	Денна форма навчання	Заочна форма навчання
Кількість кредитів ЄКТС	3	3
Модулів 2	Рік підготовки	
Змістовних модулів - 2	1-й	1-й
Загальна кількість годин	Семестр	
	2-й	2-й
	Лекції	
	16 год.	4 год.
	Практичні, семінарські	
	14 год.	2 год.
	Індивідуально-консультаційна робота	
	2 год.	2 год.
	Самостійна робота	
	58 год.	82 год.
	Форма семестрового контролю – диф. залік	

2.1. КОМПЕТЕНТНОСТІ І РЕЗУЛЬТАТИ НАВЧАННЯ

компетентності	**результати**
Загальні компетентності:	
ЗК 1. Здатність генерувати нові ідеї (креативність).	ПРН 1.4. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні аргументи, зокрема, результати теоретичного аналізу, прикладних досліджень, наявні наукові джерела; аналізувати досліджувану проблему з урахуванням широкого правового та загальносоціального контекстів.
ЗК 2. Здатність виявдяти, ставити та вирішувати проблеми.	ПРН 1.8. Розробляти та реалізовувати наукові та інноваційні проєкти, які дають можливість створити нове цілісне знання, законопроєктну та правозастосовну практику і розв'язувати значущі наукові та прикладні правові проблеми з врахуванням етичних, соціально-управлінських, соціально-економічних, екологічних та духовно-культурних аспектів.
ЗК 3. Здатність працювати в міжнародному контексті та адаптувати його у вітчизняне.	ПРН 1.1. Мати передові концептуальні та методологічні знання щодо обраної для дослідження проблеми у сфері права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних

	досліджень, отримання нових знань та здійснення інновацій.
ЗК 5. Здатність розв'язувати комплексні проблеми у сфері права на основі системного наукового світогляду, професійної етики, та загального культурного кругозору.	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.
ЗК 6. Здатність до безперервного саморозвитку та самовдосконалення, генерування нових ідей та досягнення наукових цілей.	ПРН 1.2. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях.
ЗК 8. Здатність дотримуватись етичних зобов'язань та етики поведінки, академічної доброчесності під час проведення наукових досліджень та презентації їх результатів.	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.
Фахові компетентності	
ФК 1. Здатність знаходити, контекстуалізувати та інтерпретувати значну кількість теоретичного та нормативного матеріалу;	ПРН 1.11. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, статистичні методи аналізу даних, спеціалізовані бази даних та інформаційні системи; використовувати спеціалізоване програмне забезпечення у науковій, викладацькій, правотворчій та правозастосовній діяльності.
ФК 2. Набуття глибоких, обґрунтованих фахових знань; детальні або дуже детальні знання спеціальної області дослідження в галузі права у поєднанні зі знаннями загальної наукової дискусії та внеску до індивідуальної області дослідження;	ПРН 1.6. Розуміти загальні принципи та методи юридичної науки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері права та у викладацькій практиці.
ФК 3. Здатність аналізувати методологічні проблеми загальної теорії права, галузевих юридичних наук;	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та

	української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права.
ФК 4. Набуття глибокого розуміння та здатності використовувати окладові та інструментарій доказування в окремих видах юридичних процесів, а також в процесі наукових досліджень в галузі права;	ПРН 1.8. Розробляти та реалізовувати наукові та інноваційні проєкти, які дають можливість створити нове цілісне знання, законопроєктну та правозастосовну практику і розв'язувати значущі наукові та прикладні правові проблеми з врахуванням етичних, соціально-управлінських, соціально-економічних, екологічних та духовно-культурних аспектів.
ФК 5. Здатність використовувати практичний досвід країн ЄС у вирішенні теоретичних та практичних проблем галузевих юридичних наук.	ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.
Спеціальні компетентності:	
СК 1. Здатність до критичного аналізу знань та розуміння предметної області дослідження з оцінкою та синтезом нових комплексних ідей.	ПРН 1.1. Мати передові концептуальні та методологічні знання щодо обраної для дослідження проблеми у сфері права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень, отримання нових знань та здійснення інновацій.
СК 2. Здатність планувати та виконувати сучасні інтелектуальні дослідження, як на запити стейкхолдерів так і сучасної світової наукової спільноти для досягнення науково обґрунтованих теоретичних або експериментальних наукових результатів, які розв'язують конкретне наукове завдання, що має істотне значення для правничої сфери;	ПРН 1.11. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, статистичні методи аналізу даних, спеціалізовані бази даних та інформаційні системи; використовувати спеціалізоване програмне забезпечення у науковій, викладацькій, правотворчій та правозастосовній діяльності.
СК 3. Здатність планувати та виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі права та дотичних до неї міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з права та суміжних галузей.	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права.
СК 4. Здатність усно і письмово презентувати результати власного наукового дослідження українською та іноземною мовами, глибоко розуміти	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних

іншомовні наукові та професійні тексти за напрямом досліджень.	напрямів та провідних тенденцій у розвитку права.
СК 6. Здатність здійснювати науково-педагогічну діяльність у вищій освіті та проектах правничої та громадянської освіти у системі освіти дорослих.	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права.
СК 6. Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері права та забезпечувати якість виконуваних досліджень; дотримання права інтелектуальної власності та стандартів академічної доброчесності.	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.
СК 8. Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері права та забезпечувати якість виконуваних досліджень; дотримання права інтелектуальної власності та стандартів академічної доброчесності.	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.
СК 9. Здатність здійснювати доктринальне тлумачення норм національного, міжнародного та права Європейського Союзу, моделювати оптимальні варіанти вирішення складних правових проблем, прогнозувати можливі наслідки їх реалізації.	ПРН 1.4. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні аргументи, зокрема, результати теоретичного аналізу, прикладних досліджень, наявні наукові джерела; аналізувати досліджувану проблему з урахуванням широкого правового та загальносоціального контекстів.
СК 10. Здатність розробляти проєкти нормативно-правових та правозастосовних актів, здійснювати експертну діяльність та надавати висновки спеціаліста у сфері права.	ПРН 1.10. Готувати правові висновки, пропозиції та рекомендації за результатами правового дослідження.
СК 11. Здатність застосовувати нові технології та інструменти, сучасні цифрові технології, бази даних та інші ресурси, спеціалізоване програмне забезпечення у науковій, викладацькій та професійній діяльності.	ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури,

	спеціалізовані бази даних та інформаційні системи.
СК 12. Здатність виявляти нові інституційні етичні виклики та етичні виклики в житті суспільства і пропонувати для них механізми розв'язання	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.

2.2. ПРЕРЕКВІЗИТИ ТА ПОСТРЕКВІЗИТИ

Передумовами вивчення навчальної дисципліни «Правове забезпечення інформаційної безпеки» є вивчення такої навчальної дисципліни як: «Діджиталізація наукової діяльності».

Дисципліна «Правове забезпечення інформаційної безпеки» є основою для вивчення таких дисциплін як: «Доктрина публічного права» «Методологія приватного права».

2.3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Денна форма навчання

№ з/п	Змістові модулі	Кількість годин				
		Всього	Лекції	Семінарські\практичні заняття	Індивідуально - консультацій на робота	СРС
МОДУЛЬ І						
ЗМ-1 (Теми № 1.1.-1.4.) Загальні положення інформаційної безпеки						
Т.1.1.	Теоретико-методологічні та законодавчі засади інформаційної безпеки	10	2	-	-	8
Т.1.2.	Правове забезпечення безпеки різних видів інформації	12	2	2	-	8
Т.1.3.	Суб'єкти та об'єкти забезпечення інформаційної безпеки України	12	2	2	-	8
Т.1.4.	Загрози інформацій безпеці людини, суспільства, держави	12	2	2	-	8
Всього по модулю		46	8	6	-	32
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - (40хв.)						
МОДУЛЬ ІІ						
ЗМ 2 (Теми 2.1.-2.4) Особливості правового забезпечення інформаційної безпеки окремих суспільних інститутів						
Т.2.1.	Правові засоби забезпечення інформаційної безпеки особи	11	2	2	-	7
Т.2.2.	Правові засоби забезпечення інформаційної безпеки суспільства	11	2	2	-	7
Т.2.3.	Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері. Основні положення інформаційної безпеки держави.	12	2	2	2	6
Т.2.4.	Міжнародний та зарубіжний досвід правового забезпечення інформаційної безпеки людини, суспільства, держави	10	2	2		6
Всього по модулю		44	8	8	2	26
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - (40хв.)						

Форма підсумкового контролю – диф. залік						
Усього за навчальною дисципліною	90	16	14	2	58	

Заочна форма

№ з/п	Змістові модулі	Кількість годин				
		Всього	Лекції	Семінарські\практичні заняття	Індивідуально - консультацій на робота	СРС
МОДУЛЬ І						
ЗМ 1 (Теми № 1.1.-1.4.) Загальні положення інформаційної безпеки .						
Т.1.1.	Теоретико-методологічні та законодавчі засади інформаційної безпеки	10	2	-	-	8
Т.1.2.	Правове забезпечення безпеки різних видів інформації	12	-	-	-	12
Т.1.3.	Суб'єкти та об'єкти забезпечення інформаційної безпеки України	12	-	-	-	12
Т.1.4.	Загрози інформацій безпеці людини, суспільства, держави	12	-	2	-	10
Всього по модулю		46	2	2	-	42
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - (40хв.)						
МОДУЛЬ ІІ						
ЗМ 2 (Теми 2.1.-2.4) Особливості правового забезпечення інформаційної безпеки окремих суспільних інститутів						
Т.2.1.	Правові засоби забезпечення інформаційної безпеки особи	11	-	-	-	11
Т.2.2.	Правові засоби забезпечення інформаційної безпеки суспільства	11	-	-	-	11
Т.2.3.	Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері. Основні положення інформаційної безпеки держави.	12	-	-	2	10
Т.2.4.	Міжнародний та зарубіжний досвід правового забезпечення інформаційної безпеки людини, суспільства, держави	10	2	-		8
Всього по модулю		44	2	-	2	40

Форма контролю: модульна контрольна робота (за рахунок семінарського заняття - (40хв.)					
Форма підсумкового контролю – диф. залік					
Усього за навчальною дисципліною	90	4	2	2	82

РЕЙТИНГ-ПЛАН

Денна форма навчання.

Години	Тема	Форма заняття та діяльності	Результати навчання	Вага оцінки (кількість балів)
	Модуль 1			
2	Т. 1.1. Теоретико-методологічні та законодавчі засади інформаційної безпеки	Лекція	ПРН 1.1. Мати передові концептуальні та методологічні знання щодо обраної для дослідження проблеми у сфері права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень, отримання нових знань та здійснення інновацій.	0
2	Т. 1.2. Правове забезпечення безпеки різних видів інформації	Лекція	ПРН 1.11. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, статистичні методи аналізу даних, спеціалізовані бази даних та інформаційні системи; використовувати спеціалізоване програмне забезпечення у науковій, викладацькій, правотворчій та правозастосовній діяльності.	0
2	Т. 1.2. Правове забезпечення безпеки різних видів інформації	Семінар	ПРН 1.11. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, статистичні методи аналізу даних, спеціалізовані бази даних та інформаційні системи; використовувати спеціалізоване програмне забезпечення у науковій, викладацькій, правотворчій та правозастосовній діяльності.	3
2	Т. 1.3. Суб'єкти та об'єкти забезпечення інформаційної безпеки України	Лекція	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та логічних міждисциплінарних	0

			напрямів з використанням сучасного інструментарію, критично аналізувати результати власних дослідженьі результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики. ПРН 1.4. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні аргументи, зокрема, результати теоретичного аналізу, прикладних досліджень, наявні наукові джерела; аналізувати досліджувану проблему з урахуванням широкого правового та загальносоціального контекстів.	
2	Т. 1.3. Суб'єкти та об'єкти забезпечення інформаційної безпеки України	Семінар	ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики. ПРН 1.4. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні аргументи, зокрема, результати теоретичного аналізу, прикладних досліджень, наявні наукові джерела; аналізувати досліджувану проблему з урахуванням широкого правового та загальносоціального контекстів.	3

2	Т. 1.4. Загрози інформацій безпеці людини, суспільства, держави	Лекція	ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.	0
2	Т. 1.4. Загрози інформацій безпеці людини, суспільства, держави	Семінар	ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.	3
	Проміжн. модульн. контроль 1			7
	Усього за модулем 1			16
	Модуль 2			
2	Т. 2.1. Правові засоби забезпечення інформаційної безпеки особи	Лекція	ПРН 1.6. Розуміти загальні принципи та методи юридичної науки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері права та у викладацькій практиці. ПРН 1.8. Розробляти та реалізовувати наукові та інноваційні проєкти, які дають можливість створити нове цілісне знання, законопроєктну та правозастосовну практику і розв'язувати значущі наукові та прикладні правові проблеми з врахуванням етичних, соціально-управлінських, соціально-економічних, екологічних та духовно-культурних аспектів.	0
2	Т. 2.1. Правові засоби забезпечення безпеки людини	Семінар	ПРН 1.8. Розробляти та реалізовувати наукові та інноваційні проєкти, які дають можливість створити нове цілісне знання, законопроєктну та правозастосовну практику і	3

			розв'язувати значущі наукові та прикладні правові проблеми з врахуванням етичних, соціально-управлінських, соціально-економічних, екологічних та духовно-культурних аспектів. ПРН 1.10. Готувати правові висновки, пропозиції та рекомендації за результатами правового дослідження.	
2	Т. 2.2. Правові засоби забезпечення інформаційної безпеки суспільства.	Лекція	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права. ПРН 1.6. Розуміти загальні принципи та методи юридичної науки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері права та у викладацькій практиці.	0
2	Т. 2.2. Правові засоби забезпечення інформаційної безпеки суспільства.	Семінар	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права. ПРН 1.6. Розуміти загальні принципи та методи юридичної науки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері права та у викладацькій практиці.	3
2	Т. 2.3. Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері. Основні положення інформаційної безпеки держави.	Лекція	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права.	0

			ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.	
2	Т. 2.3. Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері. Основні положення інформаційної безпеки держави.	Семінар	ПРН 1.3. Ефективно застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права. ПРН 1.5. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.	3
2	Індивідуально-консультаційна робота			10
2	Т.2.4. Міжнародний та зарубіжний досвід правового забезпечення інформаційної безпеки людини, суспільства, держави	Лекція	ПРН 1.2. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях.	

			ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.	
2	Т.2.4. Міжнародний та зарубіжний досвід правового забезпечення інформаційної безпеки людини, суспільства, держави	Семінар	ПРН 1.2. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях. ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.	3
	Проміжний модульний контроль			7
Компютерне тестування на платформі дистанційного навчання ДПУ MOODLE				5
	Усього за модулем 2			34
	Диф.залік			50
Усього				100

Заочна форма навчання.

Години	Тема	Форма заняття та діяльності	Результати навчання	Вага оцінки (кількість балів)
	Модуль 1			
2	Т. 1.1. Теоретико-методологічні та законодавчі засади інформаційної безпеки	Лекція	ПРН 1.1. Мати передові концептуальні та методологічні знання щодо обраної для дослідження проблеми у сфері	0

			права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень, отримання нових знань та здійснення інновацій.	
2	Т. 1.4. Загрози інформацій безпеці людини, суспільства, держави	Семінар	ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.	15
	Проміжний модульний контроль 1.			10
	Усього за модулем 1			25
	Модуль 2			
2	Індивідуально-консультаційна робота			10
2	Т.2.4. Міжнародний та зарубіжний досвід правового забезпечення інформаційної безпеки людини, сусіпільства, держави	Лекція	ПРН 1.2. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях. ПРН 1.7. Застосовувати сучасні цифрові інструменти і технології пошуку, оброблення та аналізу інформації, збереження й аналізу даних та інформації, зокрема, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані бази даних та інформаційні системи.	0
	Проміжний модульний контроль			10
Компютерне тестування на платформі дистанційного навчання ДПУ MOODLE				5
	Усього за модулем 2			25
	Диф.залік			50
Усього				100

2.4. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

Персональний комп'ютер, мультимедійний проектор.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВНИЙ МОДУЛЬ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 1.1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ЗАКОНОДАВЧІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

План лекційного заняття

1. Забезпечення інформаційної безпеки при побудові інформаційного суспільства.
2. Підходи до дослідження інформаційної безпеки.
3. Статичний, діяльнісний, комплексний підходи.
4. Система забезпечення інформаційної безпеки.
5. Національний інтерес, класифікація національних інтересів, національний інтерес в інформаційній сфері.

План самостійної роботи здобувачів вищої освіти

1. Співвідношення понять інформаційна сфера, інформаційна безпека, національна безпека, кібернетична безпека.
2. Концепції інформаційної безпеки.
3. . Глобальна інформаційна безпека.
4. Проблеми інформаційного суспільства.
5. Проблеми забезпечення інформаційної безпеки при формуванні єдиного інформаційного простору.

Перелік питань для самоконтролю

1. Які загрози інформаційній безпеці при побудові інформаційного суспільства?
2. Які заходи вживаються щоб мінімізувати загрози інформаційній безпеці при побудові інформаційного суспільства?
3. Які підходи до дослідження інформаційної безпеки застосовуються в Україні та світі.
3. Розкрийте сутність статичного підходу.
4. Розкрийте сутність діяльнісного підходу.
5. Розкрийте сутність комплексного підходу.
4. Проаналізуйте систему забезпечення інформаційної безпеки.
5. Здійсніть класифікацію національних інтересів в інформаційній сфері.

Рекомендована література:

Основна: [1]; [3]; [4]; [5]; [6]; [7]; [9]; [13].
Допоміжна: [1]; [3]; [5]; [7]; [8];
Інформаційні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [6]; [7];
Міжнародні видання: [1]; [2]; [3]; [4]; [5] [7]; [8]; [9]; [10].
Монографії: [1]; [3]; [4]

ТЕМА 1.2. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РІЗНИХ ВИДІВ ІНФОРМАЦІЇ

План лекційного заняття

1. Інформація як об'єкт правового захисту.
2. Класифікація інформації.
3. Нормативно-правове забезпечення захисту інформації.
4.Особливості правового регулювання захисту державної таємниці в Україні та за її межами.
5. Відповідальність за правопорушення в інформаційній сфері.

План семінарського заняття

1. Інформація як об'єкт правового захисту..
2. Правові підстави захисту відкритої інформації.
3. Правові підстави захисту інформації з обмеженим доступом.
4. Основна спрямованість національчого законодавства у сфері забезпечення захисту

інформації.

5. Порядок створення комплексної системи захисту відкритої інформації.

6. Особливості правового регулювання захисту державної таємниці в Україні та за її межами.

7. Відповідальність за правопорушення в інформаційній сфері.

План самостійної роботи здобувачів вищої освіти

1. Інформація – основа інформаційного суспільства
2. Інформація як об'єкт правових відносин
3. Правове регулювання захисту та обмеження доступу до інформації
4. Міжнародна відповідальність встановлено за правопорушення в сфері безпеки інформації.

Перелік питань для самоконтролю

1. Доведіть, що інформація є об'єктом правового захисту.
2. Проаналізуйте правові підстави захисту відкритої інформації.
3. Охарактеризуйте правові підстави захисту інформації з обмеженим доступом.
4. Яка основна спрямованість національного законодавства у сфері забезпечення захисту інформації?
5. Порядок створення комплексної системи захисту відкритої інформації.
6. У чому полягають особливості правового регулювання захисту державної таємниці в Україні та за її межами?
7. Яку відповідальність встановлено за правопорушення в сфері безпеки інформації?

Рекомендована література:

Основна: [1]; [2]; [3]; [4]; [5]; [8]; [10]; [11];
Допоміжна: [2]; [3]; [9]; [10]; [11];
Інформаційні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [6]; [7];
Міжнародні видання: [1]; [2]; [3]; [4]; [5].
Монографії: [1]; [2]; [4]

ТЕМА 1.3. СУБ'ЄКТИ ТА ОБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ.

План лекційного заняття

1. Загальна характеристика суб'єктів забезпечення інформаційної безпеки України.
2. Органи публічного управління як суб'єкти забезпечення інформаційної безпеки України.
3. Інституції громадянського суспільства як суб'єкти забезпечення інформаційної безпеки України.
4. Об'єкти та їх види забезпечення інформаційної безпеки держави.
5. Інформація як основний об'єкт інформаційної безпеки.

План семінарського заняття

1. Загальна характеристика суб'єктів забезпечення інформаційної безпеки України.
2. Органи публічного управління як суб'єкти забезпечення інформаційної безпеки України.
3. Інституції громадянського суспільства як суб'єкти забезпечення інформаційної безпеки України.
4. Об'єкти та їх види забезпечення інформаційної безпеки держави.
5. Інформація як основний об'єкт інформаційної безпеки.

План самостійної роботи здобувачів вищої освіти

1. Правове регулювання захисту та обмеження доступу до інформації

2. Доктрина інформаційної безпеки України.
3. Міжнародні інституції як суб'єкти забезпечення інформаційної безпеки.

Перелік питань для самоконтролю

1. Охарактеризуйте суб'єктів забезпечення інформаційної безпеки України.
2. Які повноваження мають органи публічного управління як суб'єкти забезпечення інформаційної безпеки України?
3. В чому полягає роль інституцій громадянського суспільства у забезпеченні інформаційної безпеки України?
4. Назвіть об'єкти забезпечення інформаційної безпеки держави та їх види.
5. Чому інформація є основним об'єктом інформаційної безпеки?

Рекомендована література:

Основна: [1]; [2]; [3]; [4]; [5]; [7]; [9];
Допоміжна: [3]; [6]; [7]; [9]; [12];
Інформаціні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [7] [16];
Міжнародні видання: [1]; [2]; [3]; [4]; [5] [6]; [8]; [9]; [10];

ТЕМА 1.4. ЗАГРОЗИ ІНФОРМАЦІЙ БЕЗПЕЦІ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

План лекційного заняття

1. Класифікація загроз інформаційній безпеці України
2. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України.
3.Суб'єкти забезпечення інформаційної безпеки України.
4. Загрози інформаційній безпеці людини та шляхи їх подолання.
5. Загрози інформаційній безпеці суспільства та шляхи їх подолання.

План семінарського заняття

1. Класифікація загроз інформаційній безпеці України
2. Суб'єкти забезпечення інформаційної безпеки України.
3. Загрози інформаційній безпеці людини та шляхи їх подолання.
4. Загрози інформаційній безпеці суспільства та шляхи їх подолання.
5. Шляхи протидії загрозам інформацій безпеці людини, суспільства, держави

План самостійної роботи здобувачів вищої освіти

1. Види інформаційної небезпеки.
2. Концепція інформаційної безпеки держави.
3. Сучасні загрози інформаційній безпеці держави.
4. Міжнародний досвід протистояння загрозам інформаційної безпеки.
5. Перспективи використання іноземного досвіду для вдосконалення законодавства України у сфері інформаційної безпеки людини.

Перелік питань для самоконтролю

1. Охарактеризуйте загрози інформаційній безпеці України.
2. На яких правових засадах формується та розвивається система забезпечення інформаційної безпеки України.
3. Визначте права та обов'язки суб'єктів забезпечення інформаційної безпеки України.
4. Охарактеризуйте основні загрози інформаційній безпеці людини та шляхи їх подолання.
5. Які шляхи подолання загроз інформаційній безпеці суспільства?

Рекомендована література:

Основна: [1]; [2]; [3]; [4]; [5]; [7]; [9]; [12];
Допоміжна: [3]; [6]; [7]; [9];
Інформаційні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [6]; [7];
Міжнародні видання: [1]; [2]; [3]; [4]; [5] [6]; [7]; [8]; [10].
Монографії: [1]; [2]; [3]

ЗМІСТОВНИЙ МОДУЛЬ 2. ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОКРЕМИХ СУСПІЛЬНИХ ІНСТИТУТІВ

ТЕМА 2.1. Правові засоби забезпечення інформаційної безпеки особи.

План лекційного заняття

1. Правовий статус людини в інформаційному суспільстві
2. Реальні і потенційні виклики та загрози інформаційній безпеці особи
3. Особиста інформаційна безпека.

План семінарського заняття

1. Реальні і потенційні виклики та загрози інформаційній безпеці людини.
2. Особдивості правового забезпечення прав і безпеки окремих категорій осіб у інформаційній сфері.
3. Проблеми забезпечення інформаційної безпеки людини в умовах війни проти України.
4. Правове забезпечення інформаційної безпеки в законодавстві Україні.
5. Напрямки забезпечення особистої інформаційної безпеки.

План самостійної роботи здобувачів вищої освіти

1. Інформаційна безпека людини в міжнародному праві.
2. Правове регулювання відносин у сфері інформаційної безпеки людини в США, ЄС та країнах Східного партнерства
3. Перспективи використання іноземного досвіду для вдосконалення законодавства України у сфері інформаційної безпеки людини.

Перелік питань для самоконтролю

1. Назвіть та охарактеризуйте реальні і потенційні виклики та загрози інформаційній безпеці людини.
2. В чому полягають особливості правового забезпечення прав і безпеки окремих категорій осіб у інформаційній сфері.
3. Які на вашу думку реальні проблеми забезпечення інформаційної безпеки людини в умовах війни проти України.
4. Розкрийте сутність правового забезпечення інформаційної безпеки в законодавстві Україні.
5. Які напрямки забезпечення особистої інформаційної безпеки ви знаєте.

Рекомендована література

Основна: [1; 2; 3; 6; 9; 12-16];
Допоміжна: [1; 6;7];
Інформаційні ресурси Інтернет: [6-7];
Міжнародні видання: [1-2].
Монографії: [1]; [3]; [4]

ТЕМА 2.2. ПРАВОВІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУСПІЛЬСТВА

План лекційного заняття

1. Суспільство як складна інформаційна система.

2. Поняття та сутність інформаційної безпеки суспільства.
3. Загрози інформаційній безпеці суспільства.
3. Протидія масовим інформаційним впливам.
4. Формування інформаційної культури суспільства.

План семінарського заняття

1. Суспільство як складна інформаційна система.
2. Поняття та сутність інформаційної безпеки суспільства.
3. Загрози інформаційній безпеці суспільства.
3. Протидія масовим інформаційним впливам.
4. Формування інформаційної культури суспільства.

План самостійної роботи здобувачів вищої освіти

1. Психологічна війна та інформаційно-психологічна безпека.
2. Технології психологічної війни.
3. Форми психологічної війни.

Перелік питань для самоконтролю

1. Суспільство як складна інформаційна система.
2. Розкрийте поняття та сутність інформаційної безпеки суспільства.
3. охарактеризуйте загрози інформаційній безпеці суспільства.
3. Як відбувається протидія масовим інформаційним впливам.
4. У чому особливість формування інформаційної культури українського суспільства.

Рекомендована література:

Основна: [1]; [2]; [3]; [4]; [5]; [8]; [10]; [11].
Допоміжна: [2]; [3]; [9]; [10]; [11]; [12];
Інформаційні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [6]; [7] [8]; [9]; [10]; [11];
Міжнародні видання: [1]; [2]; [3]; [4]; [5].
Монографії: [1]; [3]; [4]

ТЕМА 2.3. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ТА СКЛАДОВИХ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ. ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ.

План лекційного заняття

1. Концептуальні засади інформаційної безпеки
2. Інформаційна безпека як складова національної безпеки України.
3. Види інформаційної безпеки держави.
4. Система забезпечення інформаційної безпеки в Україні.
5. Об'єкти та суб'єкти інформаційної безпеки держави.

План семінарського заняття

1. Концептуальні засади інформаційної безпеки
2. Інформаційна безпека як складова національної безпеки України.
3. Види інформаційної безпеки держави.
4. Система забезпечення інформаційної безпеки в Україні.
5. Об'єкти та суб'єкти інформаційної безпеки держави.

План самостійної роботи здобувачів вищої освіти

1. Поняття інформаційної безпеки в суб'єктивному та об'єктивному сенсі.
2. Закордонний досвід організації роботи інформаційних реєстрів органів юстиції.
3. Складові інформаційної безпеки держави.
4. Концепція інформаційної безпеки держави

План індивідуально-консультаційної роботи

Індивідуально-консультаційна робота виконується у формі реферату, есе, тез доповідей на одну з таких тем:

1. Інформаційна безпека України на сучасному етапі розвитку.
2. Нормативно-правове забезпечення інформаційної безпеки в Україні.
3. СБУ як суб'єкт захисту інформаційної безпеки держави.
4. Пріоритетні напрями впровадження концепції превентивних заходів в системі інформаційної безпеки Україна.

Перелік питань для самоконтролю

1. Проаналізуйте концептуальні засади інформаційної безпеки
2. Розкрийте сутність інформаційної безпеки як складової національної безпеки України.
3. Назвіть основні види інформаційної безпеки держави.
4. Система забезпечення інформаційної безпеки в Україні.
5. Назвіть права та обов'язки суб'єктів інформаційної безпеки держави.
6. Охарактеризуйте об'єкти інформаційної безпеки держави.

Рекомендована література:

Основна: [1]; [2]; [3]; [4]; [8]; [10]; [11].
Допоміжна: [3]; [4]; [6]; [9]; [10]; [11]; [12];
Інформаційні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [6]; [7] [11]; [12]; [13]; [14];
Міжнародні видання: [1]; [2]; [3]; [4]; [5].
Монографії: [2]; [3]; [4]

Тема 2.4. МІЖНАРОДНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

План лекційного заняття

1. Інформаційна безпека в міжнародному праві.
2. Система міжнародної інформаційної безпеки.
3. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.
4. Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері.
5. Правове регулювання відносин у сфері інформаційної безпеки в США; ЄС та країнах Східного партнерства.

План семінарського заняття

1. Інформаційна безпека в міжнародному праві.
2. Система міжнародної інформаційної безпеки.
3. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.
4. Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері.
5. Правове регулювання відносин у сфері інформаційної безпеки в США, ЄС та країнах Східного партнерства.

План самостійної роботи здобувачів вищої освіти

1. Теоретичні концепції інформаційної безпеки в міжнародних відносинах.
2. Роль ООН в системі міжнародної інформаційної безпеки.
3. Інформаційна безпека в практиці міжнародних відносин

4. Вплив інформаційної революції на систему міжнародної безпеки. Міжнародні програми миру і стабільності у контексті потенційних глобальних інформаційних конфліктів.

Перелік питань для самоконтролю

1. Розкрийте сутність інформаційної безпека в міжнародному праві.
2. Охарактеризуйте систему міжнародної інформаційної безпеки.
3. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.
4. Як застосовуються загальні принципи міжнародного права до боротьби в інформаційній сфері?
5. Як відбувається правове регулювання відносин у сфері інформаційної безпеки в США, ЄС та країнах Східного партнерства?

Рекомендована література:

Основна: [1]; [2]; [3]; [4]; [5]; [8]; [10]; [11];
Допоміжна: [2]; [3]; [9]; [10]; [11];
Інформаційні ресурси Інтернет: [1]; [2]; [3]; [4]; [5]; [6]; [7]; [14]; [16];
Міжнародні видання: [1]; [2]; [3]; [4]; [5] [10].
Монографії: [1]; [2]; [3]

4.КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

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).

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

Таблиця 4.1

Загальний розподіл балів

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.	90-100
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.	70-89
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	50-69
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.	0-49

Таблиця 4.2

Розподіл балів за різні види завдань в межах контрольної роботи

Вид завдання	Максимальна кількість балів за виконання	
	Денна форма	Заочна форма
Теоретичне питання	3	5
Практичний кейс	4	5
Всього	7	10

Критерії оцінювання роботи на семінарських заняттях

Таблиця 4.3

Шкала оцінювання роботи на семінарських заняттях

Кількість балів	Критерії оцінювання
3/15	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
1,5/7	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обгрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

Критерії оцінювання індивідуально-консультаційної роботи

Таблиця 4.4

Індивідуально-консультаційна робота проводиться у формі, написання тез доповіді на одну із запропонованих тем за вибором студента, есе, підготовки доповіді, підготовки виступу-презентації науково-дослідного проєкту, аналізу судової практики, вирішіення кейсів та, відповідно, їх захист, оцінюється від 0 до 10 балів для денної і заочної форм навчання.

Шкала оцінювання індивідуально-консультаційної роботи здобувачів

Кількість балів	Критерії оцінювання
10/10	Послідовність, логічність написання есе, тез, а також підготовка доповіді, презентації, аналізу судової практики, вирішення кейсів та, відповідно, їх захист, а також виокремлення з різних джерел основних положень, які структурно об'єднанні, проаналізовані та узагальнені висновками.
5/5	Послідовність, логічність написання ессе, доповіді, але без презентації.
0	Презентацію не підготовлено

Підсумкове оцінювання знань здобувачів вищої освіти здійснюється за результатами поточного контролю (від 0 до 50 балів) та диф.заліку (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 диф заліку. Переведення даних 100-бальної шкали оцінювання в національну шкалу та шкалу за системою ЄКТС здійснюється в такому порядку (табл.4.5):

Таблиця 4.5

Сума балів за 100-бальною шкалою	Оцінка в ЄКТС	Значення оцінки ЄКТС	Оцінка за національною шкалою	
			Екзамен, диф.залік, к.р., практика	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	незараховано
0-34	F	Незадовільно з обовязковим повторним вивченням курсу		

Результати складання екзаменів і диференційованих заліків оцінюються та вносяться у відомість обліку успішності здобувача вищої освіти, залікову книжку, індивідуальний навчальний план здобувача вищої освіти (крім «незадовільно» і «не зараховано»).

5. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

Контроль за рівнем та повнотою засвоєння матеріалу з навчальної дисципліни «Правове забезпечення інформаційної безпеки» здійснюється з використанням наступних засобів діагностики результатів навчання:

диференційований залік;
комп'ютерне тестування на платформі MOODLE ДПУ;
індивідуальне опитування здобувачів;
презентації результатів виконаних завдань та досліджень;
студентські презентації та виступи на наукових заходах;
розв'язування практичних кейсів.

6. ФОРМИ ТА ПИТАННЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Форми поточного контролю

1. Усні опитування на семінарських заняттях.

Здобувачі вищої освіти відповідають на запитання відповідно до плану семінарського заняття.

2. Доповіді.

Здобувачі вищої освіти роблять експрес-доповіді з актуальних питань в межах теми заняття. Після виголошення доповіді відбувається обговорення.

3. Презентація (за результатами індивідуального дослідницького завдання)

4. Неструктурований кейс (групове завдання)

Здобувачі вищої освіти розподілені на групи. Кожна група готує кейс на основі обраних судових рішень. Під час заняття кожна група пропонує свій кейс до розв'язання іншій групі.

ПЕРЕЛІК ПИТАНЬ ДЛЯ ПОТОЧНОГО КОНТРОЛЮ (МКР № 1):

1. Забезпечення інформаційної безпеки при побудові інформаційного суспільства.
2. Підходи до дослідження інформаційної безпеки.
3. Статичний, діяльнісний, комплексний підходи.
4. Система забезпечення інформаційної безпеки.
5. Національний інтерес, класифікація національних інтересів, національний інтерес в інформаційній сфері.
6. Правове забезпечення інформаційної безпеки України як складова

інформаційного права.

7. Об'єкт та предмет правового забезпечення інформаційної безпеки України.
8. Правова природа основних складових елементів інформаційної безпеки України
9. Правові засади організації системи інформаційної безпеки України
10. Класифікація загроз інформаційній безпеці України
11. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України.
12. Суб'єкти забезпечення інформаційної безпеки України.
13. Загрози інформаційній безпеці людини та шляхи їх подолання.
14. Загрози інформаційній безпеці суспільства та шляхи їх подолання.
15. Органи публічного управління як суб'єкти забезпечення інформаційної безпеки України.
16. Інституції громадянського суспільства як суб'єкти забезпечення інформаційної безпеки України.
17. Об'єкти та їх види забезпечення інформаційної безпеки держави.
18. Інформація як основний об'єкт інформаційної безпеки.
19. Інформація як об'єкт правового захисту.
20. Класифікація інформації.
21. Нормативно-правове забезпечення захисту інформації.
22. Особливості правового регулювання захисту державної таємниці в Україні та за її межами.
23. Відповідальність за правопорушення в інформаційній сфері.

ПЕРЕЛІК ПИТАНЬ ДЛЯ ПОТОЧНОГО КОНТРОЛЮ (МКР № 2):

1. Концептуальні засади інформаційної безпеки
2. Інформаційна безпека як складова національної безпеки України.
3. Види інформаційної безпеки держави.
4. Система забезпечення інформаційної безпеки в Україні.
5. Об'єкти та суб'єкти інформаційної безпеки держави.
6. Інформаційна безпека в сфері державного управління.
7. Загрози інформаційній безпеці в органах державної влади.
8. Захист електронного документообігу.
9. Електронний цифровий підпис як елемент забезпечення захисту електронного документа.
10. Правове забезпечення захисту таємної, секретної і конфіденційної інформації в державних органах.
11. Поняття інформаційної безпеки в фінансовій сфері як основи фінансової безпеки.
12. Правові аспекти захисту державної інформації у фінансовій сфері.
13. Основні загрози інформаційної безпеки в фінансовій сфері.
14. Правове забезпечення безпеки інформації в Автоматизованій інформаційно-аналітичній системі Міністерства фінансів України.
15. Суспільство як складна інформаційна система.
16. Поняття та сутність інформаційної безпеки суспільства.
17. Загрози інформаційній безпеці суспільства.
18. Протидія масовим інформаційним впливам.
19. Формування інформаційної культури суспільства.
20. Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу.
21. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки.
22. Основні засади політики інформаційної безпеки НАТО.

23. Діяльність спеціальних інституцій НАТО щодо забезпечення інформаційної безпеки.

24. Інформаційна безпека в міжнародному праві.

25. Система міжнародної інформаційної безпеки.

26. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.

27. Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері.

28. Правове регулювання відносин у сфері інформаційної безпеки в США, ЄС та країнах Східного партнерства.

ПЕРЕЛІК ПИТАНЬ З КУРСУ

1. Забезпечення інформаційної безпеки при побудові інформаційного суспільства.
2. Підходи до дослідження інформаційної безпеки.
3. Статичний, діяльнісний, комплексний підходи.
4. Система забезпечення інформаційної безпеки.
5. Національний інтерес, класифікація національних інтересів, національний інтерес в інформаційній сфері.
6. Правове забезпечення інформаційної безпеки України як складова інформаційного права.
7. Об'єкт та предмет правового забезпечення інформаційної безпеки України.
8. Правова природа основних складових елементів інформаційної безпеки України
9. Правові засади організації системи інформаційної безпеки України
10. Класифікація загроз інформаційній безпеці України
11. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України.
12. Суб'єкти забезпечення інформаційної безпеки України.
13. Загрози інформаційній безпеці людини та шляхи їх подолання.
14. Загрози інформаційній безпеці суспільства та шляхи їх подолання.
15. Органи публічного управління як суб'єкти забезпечення інформаційної безпеки України.
16. Інституції громадянського суспільства як суб'єкти забезпечення інформаційної безпеки України.
17. Об'єкти та їх види забезпечення інформаційної безпеки держави.
18. Інформація як основний об'єкт інформаційної безпеки.
19. Інформація як об'єкт правового захисту.
20. Класифікація інформації.
21. Нормативно-правове забезпечення захисту інформації.
22. Особливості правового регулювання захисту державної таємниці в Україні та за її межами.
23. Відповідальність за правопорушення в інформаційній сфері.
24. Концептуальні засади інформаційної безпеки
25. Інформаційна безпека як складова національної безпеки України.
26. Види інформаційної безпеки держави.
27. Система забезпечення інформаційної безпеки в Україні.
28. Об'єкти та суб'єкти інформаційної безпеки держави.
29. Інформаційна безпека в сфері державного управління.
30. Загрози інформаційній безпеці в органах державної влади.
31. Захист електронного документообігу.
32. Електронний цифровий підпис як елемент забезпечення захисту електронного документа.
33. Правове забезпечення захисту таємної, секретної і конфіденційної інформації в

державних органах.

34. Поняття інформаційної безпеки в фінансовій сфері як основи фінансової безпеки.

35. Правові аспекти захисту державної інформації у фінансовій сфері.

36. Основні загрози інформаційної безпеки в фінансовій сфері.

37. Правове забезпечення безпеки інформації в Автоматизованій інформаційно-аналітичній системі Міністерства фінансів України.

38. Суспільство як складна інформаційна система.

39. Поняття та сутність інформаційної безпеки суспільства.

40. Загрози інформаційній безпеці суспільства.

41. Протидія масовим інформаційним впливам.

42. Формування інформаційної культури суспільства.

43. Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу.

44. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки.

45. Основні засади політики інформаційної безпеки НАТО.

46. Діяльність спеціальних інституцій НАТО щодо забезпечення інформаційної безпеки.

47. Інформаційна безпека в міжнародному праві.

48. Система міжнародної інформаційної безпеки.

49. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.

50. Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері.

51. Правове регулювання відносин у сфері інформаційної безпеки в США, ЄС та країнах Східного партнерства.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Бобало Ю.Я. Інформаційна безпека : навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

2. 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.

3. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /О. В. Левченко. Житомир : Видавець ПП "Євро-Волинь". 2021. - 172 с.

4. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2021. – 264 с.

5. Конституція України: Закон України від 28.06.1996 р. №254к/96-ВР // БД «Законодавство України» / ВР України. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/ laws/show/254ic/96- вр.

6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

7. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17.

8. Про інформацію : Закон України від 02.10.1992 № 2657-XII – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

11. Про Стратегію інформаційної безпеки. Указ Президента України від 28 грудня 2021 року № 685/2021. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua.

12. Інформаційна безпека держави: навч. посіб. для студ. / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с

Допоміжна:

1. Проблеми захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій XXI сторіччя : монографія / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Х.: Право. – 2019. – 296 с.

2. Бобало Ю.Я. Інформаційна безпека : навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

3. Климчук О. О. Забезпечення інформаційної безпеки держави: підручник ; за заг.ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України»,2018. 672 с.

4. Климчук О. О. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. за заг. ред. В. М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2020. 260 с.

5. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: монографія. Харків : Цифрова друкарня № 1, 2021.– 270 с.

6. Мирошниченко М.М. Правове забезпечення інформаційної безпеки держави : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2018. 19 с.

7. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. Науковий вісник Львівського державного університету внутрішніх справ. Серія Право. №2. 2016. С. 244-252

8. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: моногр. К. : ВД «АртЕк», 2018. 422 с

9. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С.16-22 232.

10. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. Сучасний захист інформації. 2016. №4. С.65-70

11. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків: 2018. – 289 с.

12. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. Сучасний захист інформації. 2022. №4. С.65-70

Інформаційні ресурси Інтернет:

1. Офіційний портал Верховної Ради України – [Електронний ресурс]. – Режим доступу: http://rada.gov.ua

2. Правовий портал Ліга:Закон – [Електронний ресурс]. – Режим доступу: http://www.ligazakon.ua/ua/

3. Урядовий портал – [Електронний ресурс]. – Режим доступу :http://www.kmu.gov.ua

4. Ресурс з питань авторського права та промислової власності - [Електронний ресурс]. – Режим доступу: http://www.intelvlas.com.ua

5. Офіційний веб-портал Державної служби інтелектуальної власності України - [Електронний ресурс]. – Режим доступу: http://www.sdip.gov.ua.

6. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua

11. Єдиний державний реєстр судових рішень – [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua

12. Національна бібліотека ім. В.І. Вернадського – [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua

13. Наукометрична база Google Академія – [Електронний ресурс]. – Режим доступу: https://scholar.google.com.ua/?hl=uk

14. Юридичні послуги online – [Електронний ресурс]. – Режим доступу:http://yurist-online.com

15. ЛІГА: ЗАКОН – [Електронний ресурс]. – Режим доступу: http://company.ligazakon.ua

16. Міністерство фінансів України – [Електронний ресурс]. – Режим доступу: http://www.mof.gov.ua/

17. Міністерство юстиції України – [Електронний ресурс]. – Режим доступу: https://minjust.gov.ua

Міжнародні видання:

1. Акти acquis communautaire, перекладені на українську мову 04.04.2016. Регламент (ЄС) № 864/2007/ЄС Європейського парламенту та Ради «Про право, що застосовується до недоговірних зобов'язань ("Рим II")». – [Електронний ресурс]. – Режим доступу: http://old.minjust.gov.ua/45881

2. STATUS-QUO. – [Електронний ресурс]. – Режим доступу: http://www.s-quo.com/

3. Декларація щодо основних принципів, що стосуються внеску засобів масової інформації у зміцнення миру та міжнародного взаєморозуміння, у розвиток прав людини і у боротьбу проти расизму і апартеїду та підбурення до війни : Декларація Орг. об'єдн. націй з питань освіти, науки та культури від 28.11.1978. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_393#Text

4. Резолюція 2037 (XX) Генеральної Асамблеї ООН Декларація про розповсюдження серед молоді ідеалів миру, взаємної поваги та взаєморозуміння між народами : Резолюція Орг. Об'єдн. Націй від 07.12.1965. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_289#Text.

5. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних": Директива Європ. Союзу від 24.10.1995 № 95/46/ЄС : станом на 25 трав. 2018 р. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_242#Text.

6. Резолюція 110 (II) Генеральної Асамблеї ООН "Заходи, що повинні вживатися проти пропаганди та розпалювачів нової війни" : Резолюція Орг. Об'єдн. Націй від 03.11.1947. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_274#Text

7. Рекомендація Комісії (ЄС) 2019/534 від 26 березня 2019 року щодо кібербезпеки мереж 5G. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_025-19#Text

Монографії:

1. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім. «Гельветика», 2017. – 168 с.

2. Правові засади інформаційної безпеки України: монографія / П.Д. Білен- чук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с.

3. Золотар О.О. Інформаційна безпека людини:теорія і практика ; монографія. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

4. Шемчук В. В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз : монографія. Київ : Ліра-К, 2020. 352 с.

ЛИСТ ОНОВЛЕННЯ ТА ПЕРЕЗАТВЕРДЖЕННЯ
РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

РОЗГЛЯНУТО ТА СХВАЛЕНО
На засіданні кафедри приватного права
Від _____ 20____ р. № ___

Лист оновлення та перезатвердження РПНД

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