



**ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ЮРИДИЧНИЙ ФАКУЛЬТЕТ**

Кафедра конституційного, адміністративного та фінансового права

**ІНФОРМАЦІЙНА БЕЗПЕКА
Силабус навчальної дисципліни**

Реквізити навчальної дисципліни

Рівень вищої освіти	Другий (магістерський)
Галузь знань	D Бізнес, адміністрування та право
Спеціальність	D8 Право
Освітня програма	Магістр права https://surl.li/cfhosd
Статус дисципліни	Вибіркова
Форма навчання	Денна
Рік підготовки, семестр	1 курс, 3 семестр
Обсяг дисципліни	3 кредити ЄКТС / 90 годин, у тому числі: лекційних занять – 18 годин, семінарських занять – 18 годин, самостійної роботи – 54 години
Форма семестрового контролю	Залік
Мова викладання	Українська
Інформація про викладачів	Лекції, семінарські заняття, консультації: Сторожук Ірина Петрівна – кандидат юридичних наук, професор, професор кафедри конституційного, адміністративного та фінансового права i_storozhuk@univer.km.ua https://univer.km.ua/profile/krushynskyy-serhiy-antonovych Профілі у наукових базах даних: ORCID https://orcid.org/0000-0002-1583-226X Web of Science https://www.webofscience.com/wos/author/record/16302650 Scopus https://www.scopus.com/authid/detail.uri?authorId=57226294838 Google Scholar https://scholar.google.com/citations?user=Jp01y3gAAAAJ&hl=uk

Розміщення курсу	Google classroom «Інформаційна безпека» https://classroom.google.com/u/3/c/ODY2NDIwMjUyNjQ1?hl Код класу: cp3xsde7
-------------------------	---

Програма навчальної дисципліни

1. Опис навчальної дисципліни

Програмні компетентності, які здобуваються під час вивчення навчальної дисципліни	Загальні компетентності ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу; ЗК 3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел; ЗК 6. Здатність генерувати нові ідеї (креативність); ЗК 7. Здатність приймати обґрунтовані рішення; ЗК 8. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань); ЗК 9. Здатність працювати в міжнародному контексті. Спеціальні компетентності СК 1. Здатність застосовувати принципи верховенства права для розв'язання складних задач і проблем, у тому числі, у ситуаціях правової невизначеності; СК 6. Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію; СК 8. Здатність застосовувати медіацію та інші правові інструменти альтернативного позасудового розгляду та вирішення правових спорів; СК 9. Здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності; СК 10. Здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування; СК 13. Здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією.
Програмні результати навчання	РН 1. Оцінювати природу та характер суспільних процесів і явищ, і виявляти розуміння меж та механізмів їх правового регулювання; РН 2. Співвідносити сучасну систему цивілізаційних цінностей з правовими цінностями, принципами та професійними етичними стандартами; РН 3. Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, цифрові, статистичні, тестові та інші, та перевіряти їх на достовірність, використовуючи сучасні методи дослідження; РН 6. Обґрунтовано формулювати свою правову позицію, вміти опонувати, оцінювати докази та наводити переконливі аргументи; РН 7. Дискутувати зі складних правових проблем, пропонувати і обґрунтовувати варіанти їх розв'язання; РН 10. Аналізувати взаємодію міжнародного права та міжнародно-правових систем з правовою системою України на основі усвідомлення основних сучасних правових доктрин, цінностей та принципів функціонування права; РН 13. Аналізувати та оцінювати практику застосування окремих

	правових інститутів; РН 14. Обґрунтовувати правову позицію на різних стадіях правозастосування; РН 17. Інтегрувати необхідні знання та розв'язувати складні задачі правозастосування у різних сферах професійної діяльності.
Місце дисципліни в логічній схемі	<i>Дисципліна пов'язана з такими вибірковими дисциплінами:</i> –Практика цивільного судочинства –Теорія і практика адміністративного судочинства –Застосування Конвенції про захист прав людини та основоположних свобод
Зміст навчальної дисципліни	Тема 1. Концептуальні засади інформаційної безпеки. Тема 2. Інформаційний вплив та його значення. Тема 3. Загрози безпеці держави в інформаційній сфері. Тема 4. Загрози в інформаційній безпеці суспільства. Тема 5. Загрози людині в інформаційній сфері. Тема 6. Загрози інформаційній безпеці в інформаційнокомунікаційних мережах. Тема 7. Захист персональних даних та цифрова безпека. Тема 8. Штучний інтелект та ризики інформаційної безпеки. Тема 9. Інформаційна агресія: виклики для національного та міжнародного права.
Рекомендовані джерела для вивчення навчальної дисципліни	<i>Нормативно-правові акти та судова практика</i> 1. Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text. 2. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (zakon.rada.gov.ua in Bing). 3. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII.URL: https://zakon.rada.gov.ua/laws/show/3855-12 4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-ВР.URL: https://zakon.rada.gov.ua/laws/show/80/94-вр 5. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII.URL: https://zakon.rada.gov.ua/laws/show/2163-19 6. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VIURL:https://zakon.rada.gov.ua/laws/show/2297-17Bing) 7. Про затвердження Правил забезпечення захисту інформації в інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.URL: https://zakon.rada.gov.ua/laws/show/373-2006-п 8. Про затвердження Типової інструкції щодо обліку, зберігання та знищення документів із службовою інформацією : Постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736.URL: https://zakon.rada.gov.ua/laws/show/736-2016-п 9. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2016. 28 с. URL: https://uas.org.ua/ua/services/standart-iso-iec-27001-2015 10. Д ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в

комп'ютерних системах від несанкціонованого доступу. Київ : Держкомзв'язку України, 1999. 45 с. URL: <https://cip.gov.ua/ua/normativni-dokumenti>

Література

1. Тихомиров О.О. Права людини: інформаційний вимір : монографія. Одеса: Юридика, 2023. 304 с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf
2. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с. URL: <http://ippi.org.ua/natsionalna-bezpeka-svitoglyadni-ta-teoretiko-metodologichni-zasadi>
3. Арістова І. В., Баранов О. А., Дзьобань О. П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія / за заг. ред. проф. К. І. Белякова. Київ : КВІЦ, 2019. 344 с. URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf
4. Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони : зб. док. і матеріалів / упоряд. М. В. Беланюк, І. М. Доронін, О. В. Лебединська, О. Г. Радзієвська, В. Г. Пилипчук, О. В. Шамара, В. М. Фурашев. Київ : АртЕк, 2020. 756 с. URL: http://ippi.org.ua/sites/default/files/verstka_zbirnuk_zakoniv.pdf
5. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання : посіб. / за заг. ред. Д. В. Ланде. Київ ; Одеса : Фенікс, 2021. 276 с. URL: <http://ippi.org.ua/sites/default/files/posibnik.pdf>
6. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань» : монографія. Київ ; Одеса : Фенікс, 2021. 176 с. URL: <http://ippi.org.ua/kiberbezpeka-%C2%ABsusilstva-znan%C2%BB>
7. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства : монографія / за заг. ред. В. Пилипчука. Київ ; Одеса : Фенікс, 2022. 140 с. URL: <http://ippi.org.ua/problemi-protidii-negativnim-informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus>
8. Баранов О. А. Соціальні та цифрові трансформації: нова парадигма кібербезпеки : монографія. Київ, 2021. 86 с. URL: <https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsii-nova-paradigma-kiberbezpeki>
9. Баранов О. А. Трансформація: соціальна & цифрова & правова : монографія у 3 т. Т. 1 : Порятунки цивілізації: економіка результату. Одеса : Гельветика, 2022. 272 с. URL: <https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova>

Навчальний контент

№ теми	Назва теми	Кількість годин					
		Усього	у тому числі				
			Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС
1.	Концептуальні засади інформаційної безпеки	10	2	2	–	–	6
2.	Інформаційний вплив та його значення	10	2	2	–	–	6
3	Загрози безпеці держави в інформаційній сфері	10	2	2	–	–	6
4	Загрози в інформаційній безпеці суспільства	10	2	2	–	–	6
5	Загрози людині в інформаційній сфері	10	2	2	–	–	6
6	Загрози інформаційній безпеці в інформаційно–комунікаційних мережах	10	2	2		–	6
7	Захист персональних даних та цифрова безпека	10	2	2	–	–	6
8	Штучний інтелект та ризики інформаційної безпеки	10	2	2	–	–	6
9	Інформаційна агресія: виклики для національного та міжнародного права	10	2	2	–	–	6
	Усьогогодин:	90	18	18	–	–	54

Методи навчання та форми поточного контролю	1) традиційний усний виклад змісту теми; 2) слайдова презентація; 3) дискусія. На семінарських (практичних) заняттях застосовуються: 1) дискусійне обговорення проблемних питань; 2) вирішення ситуаційних завдань; 3) складання та розгляд окремих процесуальних документів. Поточний контроль знань студентів з навчальної дисципліни проводиться у таких формах: 1) усне або письмове опитування на семінарських заняттях; 2) перевірка виконання поточних контрольних робіт у формі тестування; 3) розв’язування творчих завдань, проведення дискусій тощо; 4) захист підготовленого індивідуального завдання.
---	--

Лекційні заняття	Лекційне заняття 1 Тема: Концептуальні засади інформаційної безпеки 1. Еволюція поняття інформаційної безпеки. 2. Зв'язок інформаційної безпеки та кібербезпеки. 3. Концепція інформаційного суверенітету держави. 4. Інформаційна політика держави. 5. Правові засади інформаційної безпеки.
	Лекційне заняття 2 Тема: Інформаційний вплив та його значення 1. Інформаційний вплив та його різновиди. 2. Визначення об'єктів інформаційного впливу. 3. Механізми та інструменти інформаційного впливу. 4. Правові та етичні межі інформаційного впливу. 5. Соціальне та стратегічне значення інформаційного впливу.
	Лекційне заняття 3 Тема: Загрози безпеці держави в інформаційній сфері 1. Поняття та види загроз безпеці держави в інформаційній сфері. 2. Інформаційні війни як джерело загроз безпеці держави в інформаційній сфері. 3. Спеціальні інформаційні операції в міжнародній політиці. 4. Інформаційна зброя як засіб ведення інформаційного протистояння.
	Лекційне заняття 4 Тема: Загрози в інформаційній безпеці суспільства 1. Суспільна свідомість та її роль. 2. Чинники ескалації інформаційних загроз суспільству. 3. Сучасні технології маніпуляції суспільною свідомістю. 4. Інформаційно-пропагандистський вплив на суспільство. 5. PR-технології на службі маніпуляції суспільною свідомістю. 6. Нейролінгвістичне програмування. 7. Сучасні засоби впливу на суспільство.
	Лекційне заняття 5 Тема: Загрози людині в інформаційній сфері 1. Поняття і сутність маніпулювання свідомістю людини. 2. Способи та технології маніпулювання свідомістю людини. 3. Поняття та напрями реалізації технологій маніпулятивного впливу. 4. Вплив на людину певних фізичних факторів інформаційного середовища. 5. Вікна Овертона в аспекті інформаційної безпеки. 6. Інформаційно-психологічна безпека особи.
	Лекційне заняття 6 Тема: Загрози інформаційній безпеці в інформаційнокомунікаційних мережах 1. Інтернет як арена сугестивного маніпулятивного впливу. 2. Соціальна інженерія в аспекті маніпулятивного впливу. 3. Комп'ютерна злочинність та кібертероризм як загрози інформаційній безпеці.

	Лекційне заняття 7 Тема: Захист персональних даних та цифрова безпека 1. Правові засади захисту персональних даних в Україні та в праві ЄС. 2. Процедурно-правова складова захисту персональних даних. 3. Організаційно-технічна складова захисту персональних даних. 4. Цифрова безпека як складова інформаційної безпеки. 5. Відповідальність за порушення у сфері захисту персональних даних і цифрової безпеки. Лекційне заняття 8 Тема: Штучний інтелект та ризики інформаційної безпеки 1. Штучний інтелект як джерело загроз інформаційній безпеці: правова характеристика. 2. Правове регулювання штучного інтелекту в контексті інформаційної безпеки: національний та міжнародний виміри. 3. Deepfake, синтетичний контент та дезінформація як правові виклики. 4. Юридична відповідальність та інституційні механізми управління ризиками ШІ. Лекційне заняття 9 Тема: Інформаційна агресія: виклики для національного та міжнародного права 1. Поняття та правова природа інформаційної агресії. 2. Національно-правові механізми протидії інформаційній агресії. 3. Міжнародно-правові механізми протидії інформаційній агресії.
	Семінарське заняття 1. Тема: Концептуальні засади інформаційної безпеки <i>Питання для усного опитування та дискусії</i> 1.1. Поняття і сутність інформаційної безпеки 1.2. Зв'язок інформаційної безпеки та кібербезпеки 1.3. Концепція інформаційного суверенітету держави 1.4. Інформаційна політика держави 1.5. Правові засади інформаційної безпеки <i>Аудиторна письмова робота</i> Виконання студентами тестових завдань за темою заняття. <i>Усна дискусія</i> ➤ Які наукові підходи до визначення поняття «інформаційна безпека» існують у доктрині та чим відрізняються нормативний і системний виміри цього поняття? ➤ Як співвідносяться поняття «інформаційна безпека», «кібербезпека» та «безпека інформації» у законодавстві України? ➤ Яку систему утворює законодавство України у сфері інформаційної безпеки та наскільки воно є системним і несутеречливим? ➤ Межі допустимого обмеження інформаційних прав у кризових умовах. ➤ Визначення меж інформаційного та електронного суверенітету.

Семінарські заняття	Семінарське заняття 2. Тема: Інформаційний вплив та його значення <u>Питання для усного опитування та дискусії</u> 2.1. Інформаційний вплив та його різновиди. 2.2. Визначення об'єктів інформаційного впливу 2.3. Механізми та інструменти інформаційного впливу 2.4. Правові та етичні межі інформаційного впливу 2.5. Соціальне та стратегічне значення інформаційного впливу
	<u>Аудиторна письмова робота</u> Виконання студентами тестових завдань з питань теми заняття. <u>Усна дискусія</u> ➤ Межі між легітимним інформуванням та маніпуляцією. ➤ Допустимі обмеження інформаційного впливу в умовах війни, пандемії чи кризових ситуацій. ➤ Чи можна вважати алгоритми соціальних мереж інструментами інформаційного впливу, і хто має нести відповідальність за їх наслідки? ➤ Чи є допустимим використання інформаційного впливу державою для мобілізації суспільства, і де межа між легітимною політикою та маніпуляцією?
	Семінарське заняття 3 Тема: Загрози безпеці держави в інформаційній сфері <u>Питання для усного опитування та дискусії</u> 3.1. Поняття та види загроз безпеці держави в інформаційній сфері. 3.2. Інформаційні війни як джерело загроз безпеці держави в інформаційній сфері. 3.3. Спеціальні інформаційні операції в міжнародній політиці. 3.4. Інформаційна зброя як засіб ведення інформаційного протиборства.
	<u>Аудиторна письмова робота</u> Виконання студентами тестових завдань з питань теми заняття. <u>Усна дискусія</u> ➤ Використання соціальних мереж для впливу на громадську думку та політичні процеси. ➤ Несанкціоноване втручання у роботу державних інформаційних систем. ➤ Порухнення інформаційного суверенітету через залежність від іноземних платформ та технологій. ➤ Використання інформаційних технологій для радикалізації, підриву довіри до влади. ➤ Формування «інформаційних бульбашок» та поляризація суспільства. ➤ Використання інформаційних потоків як інструменту збройної боротьби.
	Семінарське заняття 4 Тема: Загрози в інформаційній безпеці суспільства <u>Питання для усного опитування та дискусії</u> 4.1. Суспільна свідомість та її роль

- 4.1.1. Види колективної свідомості та їх роль в життєдіяльності суспільства;
- 4.1.2. Моделі інформаційно-психологічного впливу, що діють у суспільстві
- 4.2. Чинники ескалації інформаційних загроз суспільству
- 4.3. Сучасні технології маніпуляції суспільною свідомістю
- 4.4. Інформаційно-пропагандистський вплив на суспільство
- 4.5. ПР-технології на службі маніпуляції суспільною свідомістю
- 4.6. Нейролінгвістичне програмування
- 4.7. Сучасні засоби впливу на суспільство

Аудиторна письмова робота

Виконання студентами тестових завдань з питань теми заняття.

Усна дискусія

- Викрадення персональних даних, фінансових ресурсів.
- Атаки на електронні сервіси, що підривають довіру до цифрових технологій.
- Масове стеження, неконтрольований збір даних.
- Використання технологій для обмеження свободи особистості.
- Обмежений доступ до якісної інформації для окремих груп населення.
- Відсутність навичок критичного мислення та медіаграмотності.

Семінарське заняття 5

Тема: Загрози людині в інформаційній сфері

Питання для усного опитування та дискусії

- 5.1. Поняття і сутність маніпулювання свідомістю людини
- 5.2. Способи та технології маніпулювання свідомістю людини
- 5.3. Технології масового маніпулятивного впливу
- 5.4. Поняття та напрями реалізації сугестивних технологій маніпулятивного впливу
- 5.5. Реалізація маніпулятивних технологій в засобах масової інформації
- 5.6. Фактори впливу на діяльність засобів масової інформації
- 5.7. Вплив на людину певних фізичних факторів інформаційного середовища
- 5.8. Інформаційно-психологічна безпека особи
- 5.9. Базові стратегії та механізми психологічного захисту

Аудиторна письмова робота

Виконання студентами тестових завдань з питань теми заняття.

Усна дискусія

- Неконтрольований збір, зберігання та використання персональних даних.
- Поширення паніки, страху чи радикальних ідей.
- Ризик витоку конфіденційної інформації (медичні, фінансові дані).
- Фішинг, соціальна інженерія, шахрайські схеми.
- Постійний потік інформації, що призводить до когнітивного виснаження.
- Ризик соціальної ізоляції та втрати навичок живої комунікації.

Семінарське заняття 6

Тема: Загрози інформаційній безпеці в інформаційно-комунікаційних мережах

Питання для усного опитування та дискусії

- 6.1. Інтернет як арена сугестивного маніпулятивного впливу
- 6.2. Соціальна інженерія в аспекті маніпулятивного впливу
- 6.3. Комп'ютерна злочинність та кібертероризм як загрози інформаційній безпеці

Аудиторна письмова робота

Виконання студентами тестових завдань з питань теми заняття

Усна дискусія

- Використання ботнетів та шкідливого програмного забезпечення.
- Віруси, трояни, програми-шпигуни.
- Неконтрольований збір та використання персональних даних.
- Контент, що підриває моральні та культурні цінності.
- Залежність від іноземних технологій та платформ.
- Використання мереж для гібридних операцій проти держави.

Семінарське заняття 7

Тема: Захист персональних даних та цифрова безпека

Питання для усного опитування та дискусії

- 7.1. Правові засади захисту персональних даних в Україні та в праві ЄС.
- 7.2. Процедурно-правова складова захисту персональних даних.
- 7.3. Організаційно-технічна складова захисту персональних даних.
- 7.4. Цифрова безпека як складова інформаційної безпеки.
- 7.5. Відповідальність за порушення у сфері захисту персональних даних і цифрової безпеки

Аудиторна письмова робота

Виконання студентами тестових завдань з питань теми заняття

Усна дискусія

- Чи можливо забезпечити повний захист персональних даних у цифрову епоху?
- Чи допустиме обмеження права на приватність у кризових умовах (війна, пандемія, терористичні загрози)?
- Чи повинні соціальні мережі та технологічні компанії нести юридичну відповідальність за витік даних і маніпуляцію інформацією?
- чи допустиме використання даних для комерційних або політичних цілей без згоди особи, навіть якщо це приносить суспільну користь?

Семінарське заняття 8

Тема: Штучний інтелект та ризики інформаційної безпеки

Питання для усного опитування та дискусії

- 8.1. Штучний інтелект як джерело загроз інформаційній безпеці: правова характеристика.
- 8.2. Правове регулювання штучного інтелекту в контексті інформаційної безпеки: національний та міжнародний виміри.
- 8.3. Deepfake, синтетичний контент та дезінформація як правові

	виклики. 8.4. Юридична відповідальність та інституційні механізми управління ризиками ШІ <u>Аудиторна письмова робота</u> Виконання студентами тестових завдань з питань теми заняття <u>Усна дискусія</u> ➤ Чи може штучний інтелект стати самостійним джерелом загроз інформаційній безпеці, чи він лише інструмент у руках людини? ➤ Як забезпечити баланс між розвитком технологій AI та захистом прав людини (приватність, недискримінація, свобода слова)? ➤ Чи повинні держави та міжнародні організації створювати єдині стандарти контролю за використанням AI у сфері інформаційної безпеки? ➤ Наскільки допустимим є використання AI для масового моніторингу та аналізу поведінки громадян у контексті національної безпеки? ➤ Чи можна ефективно протидіяти дезінформації та deepfake-технологіям без ризику цензури та обмеження свободи слова? Семінарське заняття 9 Тема: Інформаційна агресія: виклики для національного та міжнародного права <u>Питання для усного опитування та дискусії</u> 9.1. Поняття та правова природа інформаційної агресії. 9.2. Національно-правові механізми протидії інформаційній агресії. 9.3. Міжнародно-правові механізми протидії інформаційній агресії. <u>Аудиторна письмова робота</u> Виконання студентами тестових завдань з питань теми заняття. <u>Усна дискусія</u> ➤ Чи потребує інформаційна агресія окремої правової дефініції у міжнародному праві, чи її слід розглядати як складову кіберзлочинів та інформаційних операцій? ➤ Як забезпечити баланс між свободою слова та необхідністю протидії дезінформації та пропаганді? ➤ Чи може інформаційна агресія бути кваліфікована як акт війни відповідно до міжнародного гуманітарного права? ➤ Які механізми міжнародної відповідальності держав та недержавних акторів можливі за здійснення інформаційної агресії? ➤ Чи здатне національне законодавство ефективно протидіяти інформаційній агресії без узгоджених міжнародних стандартів?
Самостійна робота студентів	Бали за самостійну роботу можна здобути такими шляхами: 1) проходження он-лайн курсу з отриманням сертифікату; 2) виконати індивідуальне завдання у формі науково-дослідної роботи на тему, погоджену із викладачем; 3) за результатами неформальної освіти.

Політика та контроль

Політика щодо дедлайнів та здобуття балів за пропущені заняття	Перескладання лекцій та семінарських занять відбувається у порядку, визначеному Положенням про організацію освітнього процесу у ХУУП імені Леоніда Юзькова (https://cutt.ly/FtC24tq0). Перескладання лекцій: виконання презентації по питаннях теми пропущеної лекції. Перескладання семінарського заняття: усне опитування по питаннях пропущеного семінару та проходження тестування.
Підсумковий контроль	Питання для підготовки до підсумкового контролю 1. Що таке інформаційна безпека та які її основні принципи? 2. Як визначається поняття «інформаційний суверенітет держави»? 3. Які основні джерела права регулюють інформаційну безпеку в Україні? 4. У чому полягає різниця між інформаційною безпекою та кібербезпекою? 5. Які основні концептуальні проблеми існують у визначенні інформаційної безпеки? 6. Як співвідносяться права людини та державний контроль у сфері інформаційної безпеки? 7. Які міжнародні стандарти регулюють захист інформації (GDPR, ISO/IEC 27001)? 8. Що таке інформаційна агресія та як вона кваліфікується у міжнародному праві? 9. Які основні завдання державної політики у сфері інформаційної безпеки? 10. Як інформаційна безпека інтегрується у систему національної безпеки України? 11. Які основні загрози інформаційній безпеці держави? 12. Які загрози існують для суспільства в інформаційній сфері? 13. Які загрози виникають для особистості у цифровому середовищі? 14. Що таке інформаційна війна та які її основні інструменти? 15. Як проявляється дезінформація та пропаганда у сучасних комунікаційних мережах? 16. Які ризики створює штучний інтелект для інформаційної безпеки? 17. Як впливають соціальні мережі на інформаційну безпеку суспільства? 18. Які загрози виникають у сфері захисту персональних даних? 19. Що таке «цифровий розрив» і як він впливає на інформаційну безпеку? 20. Які приклади гібридних загроз у сфері інформаційної безпеки можна навести? 21. Які основні методи захисту інформації в ІТ-системах? 22. Що таке криптографія та яку роль вона відіграє у цифровій безпеці? 23. Які види кіберзлочинів найчастіше зустрічаються в Україні? 24. Що таке соціальна інженерія та як їй протидіяти? 25. Які основні принципи кібергігієни для користувачів? 26. Як працює двофакторна автентифікація? 27. Які основні стандарти інформаційної безпеки застосовуються в Україні?

	28. Що таке DDoS-атака та як її можна запобігти? 29. Які організаційні заходи забезпечують цифрову безпеку на підприємстві? 30. Як здійснюється аудит інформаційної безпеки? 31. Як міжнародне право регулює питання інформаційної агресії? 32. Чи може інформаційна агресія бути кваліфікована як акт війни? 33. Які механізми міжнародної відповідальності існують за інформаційні злочини? 34. Як узгодити українське законодавство із вимогами GDPR? 35. Які етичні проблеми виникають при використанні персональних даних? 36. Чи допустиме використання даних для комерційних цілей без згоди особи? 37. Як забезпечити баланс між свободою слова та протидією дезінформації? 38. Які виклики створює глобалізація для інформаційної безпеки? 39. Як міжнародні організації (ООН, ЄС, НАТО) реагують на інформаційні загрози? 40. Які перспективи розвитку правового регулювання інформаційної безпеки в Україні?
Критерії оцінювання	Оцінювання здійснюється відповідно до Положенням про організацію освітнього процесу у ХУУП імені Леоніда Юзькова (https://cutt.ly/FtC24tq0). Нарахування балів студентам з навчальної дисципліни здійснюється відповідно до такої схеми: <pre> graph TD A[Вивчення навчальної дисципліни] --> B[100 балів] B --> C[Очна денна, вечірня форма навчання] B --> D[Заочна дистанційна форма навчання] C --> E[до 10 балів – за результатами навчання під час лекцій] E --> F[до 30 балів – за результатами навчання під час семінарських практичних, лабораторних занять] F --> G[до 20 балів – за результатами самостійної роботи] D --> H[до 5 балів – за результатами навчання під час лекцій] H --> I[до 25 балів – за результатами навчання під час семінарських практичних, лабораторних занять] I --> J[до 30 балів – за результатами самостійної роботи] G --> K[до 40 балів – за результатами складання семестрового контролю] J --> K </pre>

	Підсумковий семестровий контроль з дисципліни проводиться у формі заліку. У випадку необхідності проведення заліку онлайн, він проводиться у формі тестування із застосуванням комп'ютерних технологій в режимі реального часу. Підсумовування балів за результатами вивчення навчальної дисципліни здійснюється, як правило, на підставі результатів поточного контролю. Семестрова оцінка із залікової навчальної дисципліни (за умови, що здобувачем за поточний контроль накопичено 36 і більше балів) обчислюється за формулою: $\sum c = \text{Бпк} * 100 / 60, \text{ де:}$ $\sum c$ – загальна кількість балів; Бпк – кількість балів, отриманих за поточний контроль. Здобувач освіти, який бажає отримати підсумковий бал вищий за розрахунковий (відповідно до зазначеної формули) із залікової навчальної дисципліни, має право скласти семестровий залік. У такому разі семестрова оцінка із залікової навчальної дисципліни обчислюється шляхом додавання накопичених здобувачем освіти балів з поточного та семестрового контролю. У разі отримання здобувачем вищої освіти на заліку підсумкової оцінки, що є нижчою ніж розрахункова, йому виставляється розрахункова оцінка. Якщо здобувач вищої освіти до дати завершення теоретичного навчання у відповідному семестрі накопичив за поточний контроль менше 20 балів, йому у відомості виставляється підсумкова оцінка «F» і такий здобувач має право на повторне вивчення відповідної навчальної дисципліни.
Можливість визнання результатів неформальної освіти	Результати неформальної освіти здобувача (участь у вебінарах, курсах, круглих столах, інших заходах за тематикою пов'язаною із вивченням навчальної дисципліни) можуть бути визнані у порядку, визначеному Положенням про порядок визнання результатів навчання у Хмельницькому університеті управління та права імені Леоніда Юзькова, здобутих шляхом неформальної та/або інформальної освіти (https://cutt.ly/Ee8mmyUb). Результати неформальної освіти здобувача можуть бути визнані шляхом повного або часткового зарахування балів за самостійну роботу.
Політика академічної доброчесності	Розділ «Академічна доброчесність» на сайті Університету (https://surl.li/eqbtoy) Кодекс академічної доброчесності Хмельницького університету управління та права імені Леоніда Юзькова (https://cutt.ly/5rMH6Rjj). Положення про систему запобігання академічному плагиату в академічних та наукових текстах у Хмельницькому університеті управління та права імені Леоніда Юзькова (https://cutt.ly/8rMH7UJZ)
Політика врегулювання конфліктів	Етичний кодекс Хмельницького університету управління та права імені Леоніда Юзькова (https://surl.li/xdccxm). Процедура звернення з апеляцією на результати підсумкового контролю передбачена п. 3.8.8 Положення про організацію освітнього процесу у ХУУП імені Леоніда Юзькова (https://cutt.ly/FtC24tq0).
Зворотній зв'язок	1. Під час аудиторних занять, консультацій. 2. За допомогою анкетування після завершення вивчення навчальної дисципліни, регулярних анкетувань студентів, що проводяться в університеті.

	3. На корпоративну електронну пошту i_storozhuk@univer.km.ua
--	--

РОЗРОБНИК професор кафедри конституційного, адміністративного та фінансового права, кандидат юридичних наук, професор **Ірина Сторожук**

СХВАЛЕНО рішення кафедри конституційного, адміністративного та фінансового права від 17 червня 2026 року, протокол № 13.

**Завідувач кафедри
конституційного, адміністративного
та фінансового права**


Олена ГАЛУС

**Погоджено
Гарант освітньої програми**


Сергій КРУШИНСЬКИЙ

Обліковий обсяг – 0,75 ум.др.арк.