CHERNIVTSI
LAW SCHOOL

ЧЕРНІВЕЦЬКИЙ
НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Чернівецький національний університет імені Юрія Федьковича

Юридичний факультет

Кафедра міжнародного права та порівняльного правознавства

«ЗАТВЕРДЖУЮ»

Декан юридичного факультету
____проф. Віталій ГОРДЄЄВ
«28» серпня 2026 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА КОНФІДЕНЦІЙНОСТІ У МІЖНАРОДНОМУ ПРАВІ
обов'язкова навчальна дисципліна

Освітньо-професійна програма: «Міжнародне право»
Спеціальність: D9 Міжнародне право
Галузь знань: D Бізнес, адміністрування та право
Рівень вищої освіти: другий (магістерський)
Юридичний факультет
Мова навчання: українська

Чернівці, 2026 рік

Робоча програма навчальної дисципліни «Захист персональних даних та конфіденційності у міжнародному праві» складена відповідно до освітньо-професійної програми «Міжнародне право» підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю D9 Міжнародне право галузі знань D Бізнес, адміністрування та право.

Розробник:

Лабик Анастасія Русланівна, *асистент*

Викладач, що забезпечує читання даної дисципліни

Лабик Анастасія Русланівна, *асистент*

Погоджено з гарантом
ОПП Міжнародне право _____ **д.ю.н., проф. Оксана ВАЙЦЕХОВСЬКА**

Затверджено на засіданні кафедри Міжнародного права та порівняльного правознавства
Протокол № 1 від «27» серпня 2026 року

В.о. завідувача кафедри
міжнародного права
та порівняльного правознавства _____ **д.ю.н., проф. Світлана КАРВАЦЬКА**

Схвалено науково-методичною комісією юридичного факультету
Протокол № 1 від «28» серпня 2026 року

Голова науково-методичної комісії _____ **PhD. ас. Лаура БЗОВА**

Метою вивчення навчальної дисципліни **«Захист персональних даних та конфіденційності у міжнародному праві»** є формування у здобувачів вищої освіти комплексної системи теоретичних знань і практичних навичок у сфері міжнародно-правового регулювання права на конфіденційність, а також розуміння дієвих механізмів захисту персональних даних на універсальному та регіональному рівнях.

Пререквізити. Для успішного вивчення даного освітнього компонента здобувачі повинні володіти базовими теоретичними знаннями та практичними навичками, набутими під час засвоєння таких навчальних дисциплін: «Європейська конвенція про захист прав людини та основоположних свобод: методологія тлумачення та застосування», «Методологія наукових досліджень у міжнародному праві», «Актуальні проблеми приватного права».

Результати навчання. У результаті вивчення навчальної дисципліни здобувач володітиме наступними компетентностями, що закріплені в Освітньо-професійній програмі «Міжнародне право» підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю D9 Міжнародне право галузі знань D Бізнес, адміністрування та право:

Загальні компетентності:

ЗК 1. Здатність до критичного мислення, аналізу та синтезу.

ЗК 2. Здатність виявляти, ставити та вирішувати проблеми.

ЗК 9. Прагнення до утвердження академічної доброчесності.

ЗК 12. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Спеціальні (фахові) компетентності:

СК 3. Здатність інтегрувати знання та розв'язувати складні задачі міжнародного права у широких або мультидисциплінарних контекстах.

СК 4. Здатність ефективно забезпечувати адаптацію законодавства України до права ЄС у правотворчому, правоінтерпретаційному та правозастосовному контекстах, надавати правову підтримку євроінтеграційним та євроатлантичним процесам у різних сферах суспільних відносин.

СК 7. Здатність розв'язувати проблеми міжнародного права, адаптації законодавства України до права ЄС у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.

СК 11. Здатність дотримуватися професійної та академічної доброчесності, нести відповідальність за достовірність отриманих результатів наукових досліджень.

СК 12. Уміння взаємодіяти з фахівцями відповідних галузей при підборі засобів мінімізації міжнародно-правових ризиків.

СК 13. Знання і розуміння міжнародних стандартів прав людини, міжнародних універсальних і регіональних інституційних механізмів захисту прав людини; уміння застосовувати правові механізми захисту прав людини в національних і міжнародних судових органах.

Програмні результати навчання:

РН 1. Виявляти, аналізувати та пропонувати шляхи вирішення різноаспектних проблем міжнародно-правового та національно-правового змісту.

РН 2. Продукувати нові ідеї для розв'язання практичних завдань зі сфери професійної юридичної діяльності.

РН 6. Захищати інтереси держави у національних судах, міжнародних комерційних арбітражах, міжнародних судах та організаціях, зокрема інтеграційних, на міжнародних конференціях.

РН 9. Імплементувати норми міжнародних договорів, актів міжнародних міжурядових організацій, рішень міжнародних судів у національний правопорядок.

ПРН 16. Оцінювати достовірність інформації та надійність джерел, аналізувати її та використовувати для проведення наукових досліджень та професійної діяльності у сфері міжнародного права.

ПРН 17. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.

У результаті вивчення навчальної дисципліни студент повинен

а) знати:

- поняття, еволюцію та джерела міжнародно-правового регулювання права на повагу до приватного життя;
- характерні ознаки персональних даних та місце права на захист даних у системі прав людини четвертого покоління;
- універсальні стандарти та специфіку захисту персональних даних у діяльності Ради Європи і Європейського Союзу;
- прецедентну практику ЄСПЛ та Суду Справедливості ЄС у сфері захисту даних;
- принципи, підстави та процедури опрацювання загальних і окремих категорій персональних даних, у тому числі системами штучного інтелекту;
- інституційні механізми нагляду, контролю, а також засоби правового захисту та відповідальність за порушення у сфері обробки персональних даних.

б) вміти:

- тлумачити та застосовувати міжнародно-правові норми й стандарти європейських судових інституцій для вирішення практичних завдань;
- визначати обсяг прав та обов'язків суб'єктів правовідносин під час процедури опрацювання персональних даних;
- кваліфікувати правомірність обробки персональних даних, зокрема при використанні автоматизованих систем;
- обирати ефективні засоби правового захисту у випадках порушення права на конфіденційність;
- аналізувати проблеми та перспективи забезпечення права на конфіденційність в умовах європейської інтеграції України.

б) мати навички:

- здійснення системного аналізу міжнародних договорів, судових прецедентів та нормативно-правових актів ЄС у сфері управління даними;
- підготовки аргументованих юридичних позицій щодо законності опрацювання персональних даних у конкретних ситуаціях;
- оцінки правових ризиків та визначення алгоритму дій для захисту інтересів особи при витоку чи неправомірному використанні її даних.

Опис навчальної дисципліни
Загальна інформація

Форма навчання	Рік підготовки	Семестр	Кількість		Кількість годин						Вид підсумкового контролю
			кредитів	годин	лекції	практичні	семінарські	лабораторні	самостійна робота	індивідуальні завдання	
Денна	I	II	5.0	150	14	30	-	-	106	-	екзамен
Заочна	-	-	-	-	-	-	-	-	-	-	-

Структура змісту навчальної дисципліни

Назви змістових модулів і тем навчальних занять	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		лекц.	практ.	лаб.	інд.	срс		лекц.	практ.	лаб.	інд.	срс
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Теоретико-правові основи права на конфіденційність та захист даних												
Тема 1. Поняття та еволюція права на повагу до приватного життя у міжнародному праві	10	2	2	-	-	6	-	-	-	-	-	-
Тема 2. Персональні дані: поняття, характерні ознаки та джерела міжнародно-правового регулювання	10	-	2	-	-	8	-	-	-	-	-	-
Тема 3. Місце права на захист даних у системі прав людини четвертого покоління	10	-	2	-	-	8	-	-	-	-	-	-
Тема 4. Універсальні стандарти захисту конфіденційності у міжнародному праві	10	-	2	-	-	8	-	-	-	-	-	-

Тема 5. Захист персональних даних у діяльності Ради Європи та Європейського Союзу	10	2	2	-	-	6	-	-	-	-	-	-
Тема 6. Право на захист персональних даних через призму практики ЄСПЛ та Суду Справедливості ЄС	12	-	2	-	-	10	-	-	-	-	-	-
Тема 7. Проблеми та перспективи забезпечення права на конфіденційність в умовах європейської інтеграції України	10	2	2	-	-	6	-	-	-	-	-	-
Разом за ЗМ1	72	6	14	-	-	52	-	-	-	-	-	-
Змістовий модуль 2. Практичні аспекти міжнародно-правового захисту персональних даних												
Тема 1. Принципи опрацювання персональних даних	10	2	2	-	-	6	-	-	-	-	-	-
Тема 2. Підстави обробки персональних даних	12	-	2	-	-	10	-	-	-	-	-	-
Тема 3. Права та обов'язки осіб під час процедури опрацювання персональних даних	10	2	2	-	-	6	-	-	-	-	-	-
Тема 4. Актуальні питання опрацювання окремих категорій персональних даних особи	14	-	4	-	-	10	-	-	-	-	-	-
Тема 5. Особливості процедури обробки даних системами	10	2	2	-	-	6	-	-	-	-	-	-

штучного інтелекту												
Тема 6. Інституційні механізми нагляду та контролю за опрацюванням персональних даних	12	-	2	-	-	10	-	-	-	-	-	-
Тема 7. Засоби правового захисту та відповідальність за порушення у сфері обробки персональних даних	10	2	2	-	-	6	-	-	-	-	-	-
Разом за ЗМ 2	78	8	16	-	-	54	-	-	-	-	-	-
Усього годин	150	14	30	-	-	106	-	-	-	-	-	-

Тематика лекційних занять з переліком питань

№	Назва теми з основними питаннями
1	**Тема 1. Поняття та еволюція права на повагу до приватного життя у міжнародному праві.** 1. Генеза та концептуалізація права на приватність в умовах цифрової трансформації суспільства. 2. Поняття, зміст та ключові складові елементи права на повагу до приватного життя у сучасному міжнародному праві. 3. Нормативне закріплення права на конфіденційність в системі універсальних міжнародних актів. 4. Стаття 8 Конвенції про захист прав людини і основоположних свобод та еволюційне тлумачення поняття «приватне життя». 5. Міжнародно-правові критерії правомірного втручання у право на повагу до приватного життя.
2	**Тема 2. Захист персональних даних у діяльності Ради Європи та Європейського Союзу.** 1. Система стандартів Ради Європи у сфері захисту даних. 2. Взаємодія між механізмами Ради Європи та правом Європейського Союзу у сфері захисту конфіденційності. 3. Еволюція законодавства Європейського Союзу про захист даних. 4. Загальний регламент про захист даних: екстериторіальна дія, основні принципи обробки та ключові права суб'єктів даних. 5. Специфіка згоди на обробку персональних даних за стандартами GDPR. 6. Правове регулювання транскордонного передавання даних до третіх країн у праві ЄС. 7. Співвідношення вимог GDPR та положень Європейського акта про штучний інтелект у контексті управління даними.

3	**Тема 3. Проблеми та перспективи забезпечення права на конфіденційність в умовах європейської інтеграції України.** 1. Ключові аспекти національного законодавства України у сфері захисту персональних даних. 2. Захист права на конфіденційність в умовах цифровізації державних послуг та функціонування єдиних державних реєстрів. 3. Зобов'язання України щодо адаптації законодавства про захист інформації та персональних даних відповідно до Угоди про асоціацію з ЄС. 4. Імплементація стандартів Загального регламенту про захист даних у правову систему України.
4	**Тема 4. Принципи опрацювання персональних даних.** 1. Поняття, система та юридичне значення принципів опрацювання персональних даних у міжнародному праві. 2. Принцип законності, справедливості та прозорості: критерії належного інформування суб'єкта даних. 3. Принцип обмеження мети (механізми визначення первинної мети та оцінка сумісності при подальшій обробці). 4. Принцип мінімізації даних та виклики його дотримання в епоху Big Data і функціонування предиктивних алгоритмів. 5. Принцип точності. 6. Принцип обмеження зберігання: правові та технічні критерії встановлення строків зберігання інформації. 7. Принцип цілісності та конфіденційності. 8. Принцип підзвітності.
5	**Тема 5. Права та обов'язки осіб під час процедури опрацювання персональних даних.** 1. Право на інформацію та доступ до персональних даних у міжнародно-правовому вимірі. 2. Право на виправлення та право на обмеження обробки. 3. Право бути забутим: теоретичні доктрини, критерії застосування та практичні межі реалізації в умовах розвитку цифрового середовища. 4. Право на мобільність даних та його значення для забезпечення цифрових прав людини. 5. Право на заперечення проти обробки даних, включаючи механізми захисту від прямого маркетингу. 6. Права особи щодо автоматизованого індивідуального ухвалення рішень: забезпечення алгоритмічної прозорості та захист від неправомірного профілювання системами штучного інтелекту. 7. Правовий статус, розподіл відповідальності та ключові обов'язки володільця і розпорядника інформації. 8. Статус, незалежність та функціональні обов'язки Європейського інспектора із захисту даних.
6	**Тема 6. Особливості процедури обробки даних системами штучного інтелекту.** 1. Штучний інтелект як об'єкт міжнародно-правового регулювання: етичні, технічні та правові виклики для прав людини. 2. Право на алгоритмічну прозорість та «право на пояснення»: механізми та межі реалізації при використанні складних нейромереж. 3. Проблема автоматизованого індивідуального ухвалення рішень та профілювання у контексті застосування ШІ державою та приватними корпораціями. 4. Ризик-орієнтований підхід до систем штучного інтелекту за законодавством ЄС.

	5. Правомірність автоматизованого збору великих масивів даних для тренування моделей машинного навчання. 6. Біометрична ідентифікація в режимі реального часу системами ШІ: стандарти ЄСПЛ та обмеження європейського законодавства. 7. Міжнародно-правова відповідальність та засоби захисту при порушенні прав особи внаслідок дискримінаційних чи помилкових рішень алгоритмічних систем.
7	**Тема 7. Засоби правового захисту та відповідальність за порушення у сфері обробки персональних даних.** 1. Право на ефективний засіб судового захисту у контексті опрацювання персональних даних особи. 2. Процедура та юрисдикційні аспекти подання суб'єктом даних скарги до наглядового органу. 3. Критерії та механізми відшкодування матеріальної і нематеріальної шкоди, заподіяної внаслідок порушення у сфері обробки персональних даних. 4. Специфіка притягнення до цивільно-правової відповідальності за неправомірне опрацювання даних автономними системами штучного інтелекту. 5. Адміністративна та кримінальна відповідальність за порушення у сфері обробки персональних даних: національний та зарубіжний досвід. 6. Міжнародно-правова відповідальність держави за невиконання позитивних зобов'язань щодо захисту приватності особи в цифровому середовищі.

Тематика практичних занять з переліком питань

№	Назва теми
1	**Тема 1. Поняття та еволюція права на повагу до приватного життя у міжнародному праві.** 1. Генеза та концептуалізація права на приватність в умовах цифрової трансформації суспільства. 2. Поняття, зміст та ключові складові елементи права на повагу до приватного життя у сучасному міжнародному праві. 3. Нормативне закріплення права на конфіденційність в системі універсальних міжнародних актів. 4. Стаття 8 Конвенції про захист прав людини і основоположних свобод та еволюційне тлумачення поняття «приватне життя». 5. Міжнародно-правові критерії правомірного втручання у право на повагу до приватного життя. **Завдання 1:** Здійснити порівняльно-правовий аналіз обсягу та меж захисту права на приватність відповідно до ст. 12 ЗДПЛ, ст. 17 МПГПП та ст. 8 ЄКПЛ. **Завдання 2:** На основі аналізу прецедентної практики Європейського суду з прав людини змоделювати застосування «тесту на пропорційність» для оцінки правомірності втручання держави у приватне життя особи.

2	**Тема 2. Персональні дані: поняття, характерні ознаки та джерела міжнародно-правового регулювання.** 1. Поняття та правова природа персональних даних у сучасному міжнародному праві. 2. Еволюція критеріїв та маркерів ідентифікації особи. 3. Характерні ознаки персональних даних та їх відмежування від знеособленої інформації. 4. Класифікація персональних даних: загальні та особливі (чутливі) категорії даних. 5. Анонімізація та псевдонімізація: теоретичні відмінності процедур та їх правові наслідки для статусу даних. 6. Поняття, система та види джерел правового регулювання відносин у сфері обробки персональних даних. **Завдання 1:** На основі аналізу положень GDPR та Конвенції 108+ здійснити кваліфікацію запропонованих масивів інформації з метою визначення, чи підпадають вони під категорію "персональні дані" або "чутливі дані". **Завдання 2:** Провести порівняльно-правовий аналіз термінологічного апарату Конвенції 108+ та Регламенту (ЄС) 2016/679 (GDPR), визначивши ключові відмінності у підходах до визначення суб'єкта даних, контролера та оператора.
3	**Тема 3. Місце права на захист даних у системі прав людини четвертого покоління.** 1. Поняття та теоретико-правовий вимір цифрових прав людини в умовах інформаційного суспільства. 2. Ознаки цифрових прав та їх співвідношення з класичними правами людини. 3. Система цифрових прав людини: класифікація, ключові елементи та проблема їх універсального визнання. 4. Місце права на захист персональних даних в ієрархії прав людини четвертого покоління. 5. Право на забуття як самостійне цифрове право: зміст, критерії та межі реалізації. 6. Вплив систем штучного інтелекту на трансформацію прав людини. **Завдання:** Здійснити порівняльний аналіз традиційного права на недоторканність приватного життя та цифрових прав людини, виокремивши специфічні ознаки останніх у теоретико-правовому вимірі. Обґрунтувати позицію: чи є цифрові права абсолютно новими правовими категоріями, чи це лише сучасна адаптація класичних прав до умов віртуального середовища.
4	**Тема 4. Універсальні стандарти захисту конфіденційності у міжнародному праві.** 1. Система універсальних міжнародно-правових актів та інституційних механізмів ООН у сфері захисту конфіденційності. 2. Базові стандарти захисту приватності у Загальній декларації прав людини та Міжнародному пакті про громадянські та політичні права. 3. Практика Комітету з прав людини ООН: еволюція тлумачення

	права на недоторканність приватного життя (Загальний коментар № 16). 4. Керівні принципи ООН щодо охорони комп'ютеризованих файлів персональних даних 1990 р. як перша спроба універсального регулювання обробки персональних даних. 5. Резолюції Генеральної Асамблеї та Ради з прав людини ООН щодо права на приватність у цифрову епоху: зміст та правові наслідки. 6. Мандат та напрями діяльності Спеціального доповідача ООН з права на приватність. 7. Керівні принципи Організації економічного співробітництва та розвитку щодо захисту приватності та транскордонного передавання персональних даних. 8. Проблема фрагментації міжнародного права та перспективи розробки єдиної обов'язкової універсальної конвенції про захист даних. **Завдання:** Здійснити критичний аналіз актуальної тематичної доповіді Спеціального доповідача ООН з права на приватність або Резолюції ГА ООН «Право на приватність у цифрову епоху». Сформулювати аргументовані висновки щодо міжнародно-правових критеріїв правомірності державних програм масового стеження та використання шпигунського програмного забезпечення.
5	**Тема 5. Захист персональних даних у діяльності Ради Європи та Європейського Союзу.** 1. Система стандартів Ради Європи у сфері захисту даних. 2. Взаємодія між механізмами Ради Європи та правом Європейського Союзу у сфері захисту конфіденційності. 3. Еволюція законодавства Європейського Союзу про захист даних. 4. Загальний регламент про захист даних: екстериторіальна дія, основні принципи обробки та ключові права суб'єктів даних. 5. Специфіка згоди на обробку персональних даних за стандартами GDPR. 6. Правове регулювання транскордонного передавання даних до третіх країн у праві ЄС. 7. Співвідношення вимог GDPR та положень Європейського акта про штучний інтелект у контексті управління даними. **Завдання:** Здійснити юридичний аналіз ст. 22 GDPR (право не підлягати автоматизованому індивідуальному ухваленню рішень, включаючи профілювання) у поєднанні з положеннями Регламенту (ЄС) 2024/1689. Визначити правомірність використання систем штучного інтелекту для скорингу або прийняття рішень щодо працевлаштування, змоделювавши механізм захисту особи від неправомірних наслідків алгоритмічного рішення.

6	**Тема 6. Право на захист персональних даних через призму практики ЄСПЛ та Суду Справедливості ЄС.** 1. Співвідношення юрисдикцій, мандатів та концептуальних підходів Європейського суду з прав людини і Суду Справедливості ЄС у сфері цифрової приватності. 2. Динамічне тлумачення статті 8 Конвенції про захист прав людини і основоположних свобод у контексті новітніх технологій та захисту даних. 3. Прецедентна практика ЄСПЛ щодо програм масового стеження, таємного перехоплення комунікацій та балансу з інтересами національної безпеки. 4. Захист біометричних, генетичних даних та профілювання у рішеннях ЄСПЛ (справи *S. and Marper v. the United Kingdom*, *Gaughran v. the United Kingdom*). 5. Роль Суду Справедливості у формуванні європейських стандартів захисту даних (прецеденти *Schrems I* та *Schrems II*). 6. Утвердження «права бути забутим» у практиці Суду Справедливості (справа *Google Spain*) та критерії його застосування. 7. Встановлення балансу між правом на захист персональних даних, свободою вираження поглядів та правом суспільства на інформацію у практиці європейських судів. 8. Формування судових стандартів щодо використання алгоритмічних систем, систем розпізнавання облич та предиктивної поліції. **Завдання:** Здійснити поглиблений аналіз стандартів ЄСПЛ щодо масового стеження на основі рішення Великої Палати у справі *Big Brother Watch and Others v. the United Kingdom.* Виокремити ключові критерії, які Суд застосовує для оцінки пропорційності масового перехоплення комунікацій, та змоделювати їх застосування до сучасних національних систем моніторингу.
7	**Тема 7. Проблеми та перспективи забезпечення права на конфіденційність в умовах європейської інтеграції України.** 1. Ключові аспекти національного законодавства України у сфері захисту персональних даних. 2. Захист права на конфіденційність в умовах цифровізації державних послуг та функціонування єдиних державних реєстрів. 3. Зобов'язання України щодо адаптації законодавства про захист інформації та персональних даних відповідно до Угоди про асоціацію з ЄС. 4. Імплементація стандартів Загального регламенту про захист даних у правову систему України. **Завдання 1:** Здійснити порівняльно-правовий аналіз чинного Закону України «Про захист персональних даних» та положень GDPR. Виокремити 3-5 фундаментальних розбіжностей та розробити проєкт пропозицій щодо внесення змін до національного законодавства. **Завдання 2:** Змоделювати підготовку аналітичної довідки для Міністерства цифрової трансформації щодо перспектив забезпечення цифрових прав людини при євроінтеграції. Сформулювати покрокову дорожню карту правових реформ, необхідних для повноцінної інтеграції

	України до Єдиного цифрового ринку ЄС, з особливим акцентом на захист даних при використанні систем штучного інтелекту.
8	**Тема 8. Принципи опрацювання персональних даних.** 1. Поняття, система та юридичне значення принципів опрацювання персональних даних у міжнародному праві. 2. Принцип законності, справедливості та прозорості: критерії належного інформування суб'єкта даних. 3. Принцип обмеження мети (механізми визначення первинної мети та оцінка сумісності при подальшій обробці). 4. Принцип мінімізації даних та виклики його дотримання в епоху Big Data і функціонування предиктивних алгоритмів. 5. Принцип точності. 6. Принцип обмеження зберігання: правові та технічні критерії встановлення строків зберігання інформації. 7. Принцип цілісності та конфіденційності. 8. Принцип підзвітності. **Завдання:** Здійснити аудит політики конфіденційності відомого вебсервісу чи мобільного застосунку на предмет дотримання принципу прозорості. Визначити, чи викладена інформація зрозумілою мовою, чи приховані ключові умови за складними юридичними формулюваннями, та запропонувати власну редакцію окремих пунктів для забезпечення повної відповідності стандартам GDPR.
9	**Тема 9. Підстави обробки персональних даних.** 1. Поняття та перелік законних підстав для обробки персональних даних у міжнародному праві та праві ЄС. 2. Згода суб'єкта даних: критерії дійсності, проблема "згоди за замовчуванням" та механізм відкликання. 3. Обробка, необхідна для виконання договору або для вжиття заходів до укладення договору за запитом суб'єкта даних. 4. Виконання юридичного обов'язку контролера як підстава для опрацювання даних. 5. Захист життєво важливих інтересів суб'єкта даних або іншої фізичної особи. 6. Виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера. 7. Специфіка визначення легітимних підстав для масової обробки даних з метою навчання моделей штучного інтелекту.
10	**Тема 10. Права та обов'язки осіб під час процедури опрацювання персональних даних.** 1. Право на інформацію та доступ до персональних даних у міжнародно-правовому вимірі. 2. Право на виправлення та право на обмеження обробки. 3. Право бути забутим: теоретичні доктрини, критерії застосування та практичні межі реалізації в умовах розвитку цифрового середовища. 4. Право на мобільність даних та його значення для забезпечення цифрових прав людини. 5. Право на заперечення проти обробки даних, включаючи механізми

	захисту від прямого маркетингу. 6. Права особи щодо автоматизованого індивідуального ухвалення рішень: забезпечення алгоритмічної прозорості та захист від неправомірного профілювання системами штучного інтелекту. 7. Правовий статус, розподіл відповідальності та ключові обов'язки володільця і розпорядника інформації. 8. Статус, незалежність та функціональні обов'язки Європейського інспектора із захисту даних.
11	**Тема 11. Актуальні питання опрацювання окремих категорій персональних даних особи.** 1. Поняття та види особливих (чутливих) категорій персональних даних у міжнародному праві. 2. Загальна заборона опрацювання чутливих даних та винятки з неї: аналіз правових підстав. 3. Обробка біометричних та генетичних даних: міжнародні стандарти, ризики та гарантії захисту в умовах поширення систем масової ідентифікації та відеоспостереження. 4. Правовий режим опрацювання даних про стан здоров'я. 5. Особливості захисту персональних даних дітей у цифровому середовищі. 6. Специфіка опрацювання персональних даних, пов'язаних із притягненням до кримінальної відповідальності, вироками та правопорушеннями. 7. Опрацювання особливих категорій даних в умовах збройних конфліктів та надзвичайних станів: міжнародно-правові межі відступу від зобов'язань. 8. Ризики стигматизації, дискримінації та алгоритмічного упередження при профілюванні на основі чутливих даних системами штучного інтелекту.
12	**Тема 12. Особливості процедури обробки даних системами штучного інтелекту.** 1. Штучний інтелект як об'єкт міжнародно-правового регулювання: етичні, технічні та правові виклики для прав людини. 2. Право на алгоритмічну прозорість та «право на пояснення»: механізми та межі реалізації при використанні складних нейромереж. 3. Проблема автоматизованого індивідуального ухвалення рішень та профілювання у контексті застосування ШІ державою та приватними корпораціями. 4. Ризик-орієнтований підхід до систем штучного інтелекту за законодавством ЄС. 5. Правомірність автоматизованого збору великих масивів даних для тренування моделей машинного навчання. 6. Біометрична ідентифікація в режимі реального часу системами ШІ: стандарти ЄСПЛ та обмеження європейського законодавства. 7. Міжнародно-правова відповідальність та засоби захисту при порушенні прав особи внаслідок дискримінаційних чи помилкових рішень алгоритмічних систем.

13	**Тема 13. Інституційні механізми нагляду та контролю за опрацюванням персональних даних.** 1. Система інституційних механізмів нагляду за дотриманням законодавства про захист даних: універсальний, регіональний та національний рівні. 2. Статус, мандат та повноваження Європейського інспектора з питань захисту даних. 3. Європейська рада з питань захисту даних. 4. Механізм «єдиного вікна» при транскордонній обробці даних. 5. Національні наглядові органи: критерії повної незалежності, вимоги до формування та фінансування згідно з європейськими стандартами. 6. Право суб'єкта на ефективний засіб правового захисту проти юридично значущого рішення наглядового органу.
14	**Тема 14. Засоби правового захисту та відповідальність за порушення у сфері обробки персональних даних.** 7. Право на ефективний засіб судового захисту у контексті опрацювання персональних даних особи. 8. Процедура та юрисдикційні аспекти подання суб'єктом даних скарги до наглядового органу. 9. Критерії та механізми відшкодування матеріальної і нематеріальної шкоди, заподіяної внаслідок порушення у сфері обробки персональних даних. 10. Специфіка притягнення до цивільно-правової відповідальності за неправомірне опрацювання даних автономними системами штучного інтелекту. 11. Адміністративна та кримінальна відповідальність за порушення у сфері обробки персональних даних: національний та зарубіжний досвід. 12. Міжнародно-правова відповідальність держави за невиконання позитивних зобов'язань щодо захисту приватності особи в цифровому середовищі.

Завдання для самостійної роботи студентів

Самостійна робота студента є основним засобом оволодіння навчальним матеріалом і виконується в поза аудиторний час, передбачений тематичним планом навчальної дисципліни.

Під час вивчення навчальної дисципліни студенти повинні навчитися самостійно мислити, поглиблювати засвоєні теоретичні знання, опановувати практичні навички прийняття правових рішень. Відповіді на питання повинні бути законспектовані, їхнє викладення має бути стислим і чітким, обов’язковими є посилання на використані джерела.

Форма контролю самостійної роботи – перевірка конспекту або обговорення на семінарському занятті. Питання, відведені для самостійної роботи, виносяться на поточний, модульний і підсумковий семестровий контроль.

З метою самостійного визначення рівня засвоєння теоретичного матеріалу студентам пропонуються питання для самоконтролю набутих знань.

№	Назва теми	Завдання для самостійної роботи	К-сть год.
1	Поняття та еволюція права на повагу до приватного життя у міжнародному праві	Здійснити порівняльний аналіз дефініцій приватного життя у міжнародних пактах та європейських конвенціях. Скласти глосарій базових академічних термінів (автономія особи, недоторканність житла, таємниця кореспонденції). Підготувати порівняльну таблицю еволюції інтерпретації ст. 8 ЄКПЛ у доцифрову епоху та в умовах інформаційного суспільства.	6
2	Персональні дані: поняття, характерні ознаки та джерела міжнародно-правового регулювання	Провести структурний аналіз поняття «персональні дані» за національним законодавством України та Конвенцією 108+. Класифікувати сучасні цифрові маркери (IP-адреси, файли cookie, геолокаційні дані) за критеріями ідентифікації особи. Зробити огляд системи міжнародних джерел, що регулюють обіг інформації у віртуальному середовищі.	8
3	Місце права на захист даних у системі прав людини четвертого покоління	Написати міні-есе на тему: «Концепція поколінь прав людини: чому цифрові права формують четверте покоління». Опрацювати наукові публікації українських та зарубіжних авторів щодо правової природи цифрової ідентичності. Виокремити ключові загрози для прав людини в умовах масової цифровізації публічних і приватних послуг.	8
4	Універсальні стандарти захисту конфіденційності у міжнародному праві	Проаналізувати резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» за останні роки. Зробити критичний огляд тематичної доповіді Спеціального доповідача ООН з права на приватність. Дослідити вплив Керівних принципів ОЕСР на формування глобальних стандартів транскордонного передавання даних.	8
5	Захист персональних даних у діяльності Ради Європи та Європейського Союзу	Опрацювати структуру та ключові новації модернізованої Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+). Вивчити архітектуру Загального регламенту про захист даних (GDPR - Регламент (ЄС) 2016/679). Скласти схему розмежування повноважень та відповідальності між контролером (Data Controller) і оператором (Data Processor).	6
6	Право на захист персональних даних через призму практики ЄСПЛ та Суду	Підготувати письмові анотації до двох ключових рішень ЄСПЛ щодо масового перехоплення комунікацій. Проаналізувати правові наслідки рішень Суду Справедливості ЄС у справах Schrems I та Schrems	10

	Справедливості ЄС	ІІ для транскордонних передач даних. Дослідити практику застосування «права бути забутим» за рішенням у справі Google Spain.	
7	Проблеми та перспективи забезпечення права на конфіденційність в умовах європейської інтеграції України	Здійснити аудит поточного стану гармонізації українського законодавства про захист персональних даних із вимогами GDPR та Угоди про асоціацію з ЄС. Підготувати пропозиції щодо реформування інституційної системи захисту даних в Україні (створення незалежного наглядового органу). Сформулювати аналітичну довідку щодо викликів захисту приватності в умовах електронного урядування та цифрових державних платформ.	6
8	Принципи опрацювання персональних даних	Провести практичний аудит політик конфіденційності (Privacy Policies) трьох популярних інтернет-ресурсів на предмет дотримання принципів ст. 5 GDPR (прозорість, мінімізація, обмеження мети). Розробити матрицю відповідності для гіпотетичного підприємства, що збирає персональні дані клієнтів, із зазначенням заходів дотримання принципу підзвітності.	6
9	Підстави обробки персональних даних	Створити проєкт електронної форми надання згоди, яка відповідає критеріям вільного, конкретного та поінформованого волевиявлення. Здійснити порівняльний аналіз обсягу та умов застосування такої підстави, як «виконання завдання в суспільних інтересах або здійснення офіційних повноважень» для державних органів порівняно з комерційними організаціями. Дослідити практику застосування підстави «захист життєво важливих інтересів» у контексті масштабних криз (наприклад, пандемій або умов збройних конфліктів), визначивши межі допустимого відступу від загальних правил обробки даних.	10
10	Права та обов'язки осіб під час процедури опрацювання персональних даних	Підготувати проєкт офіційного запиту суб'єкта даних до міжнародної корпорації. Проаналізувати алгоритм реалізації права на мобільність даних для банківських або телекомунікаційних послуг. Дослідити функціональні обов'язки Інспектора із захисту даних на підприємстві.	6
11	Актуальні питання опрацювання окремих категорій персональних даних особи	Дослідити правовий режим опрацювання біометричних і генетичних даних за ст. 9 GDPR та прецедентною практикою ЄСПЛ. Проаналізувати спеціальні вимоги щодо захисту персональних даних дітей у цифровому середовищі (вік цифрової згоди, батьківський контроль). Оцінити ризики обробки медичних даних у наукових дослідженнях.	10
12	Особливості	Зробити огляд ключових положень Європейського	6

	процедури обробки даних системами штучного інтелекту	акта про штучний інтелект у частині взаємодії з правилами обробки даних. Дослідити проблему забезпечення «права на пояснення» та алгоритмічної прозорості при використанні систем глибокого навчання. Оцінити правомірність автоматизованого збору масивів даних для навчання комерційних моделей ШІ.	
13	Інституційні механізми нагляду та контролю за опрацюванням персональних даних	Дослідити структуру, завдання та роль Європейської ради з питань захисту даних у забезпеченні єдиної правозастосовної практики в ЄС. Проаналізувати практику застосування механізму «єдиного вікна» при розслідуванні транскордонних порушень GDPR. Вивчити повноваження європейських національних наглядових органів щодо проведення аудитів і накладення санкцій.	10
14	Засоби правового захисту та відповідальність за порушення у сфері обробки персональних даних	Провести моніторинг та аналіз найбільших адміністративних штрафів, накладених на технологічні компанії за порушення GDPR протягом останніх років. Підготувати проєкт скарги до європейського наглядового органу у зв'язку з незаконним поширенням персональних даних. Дослідити практику відшкодування нематеріальної (моральної) шкоди особам, які постраждали внаслідок масштабних витоків даних.	6

Критерії оцінювання самостійної роботи студента

Самостійна робота оцінюється за результатами перевірки конспектів, письмових завдань (есе, рефератів), ведення термінологічного словника, виконання тестів та обговорення матеріалу відповідно до таких критеріїв:

5 балів - здобувач у повному обсязі володіє матеріалом, глибоко та всебічно розкриває зміст питань для самостійного опрацювання. Відповіді чітко та стисло законспектовані. Здобувач самостійно й аргументовано викладає матеріал під час обговорення, робить обов'язкові посилання на джерела та використовує як обов’язкову, так і додаткову літературу.

4 бали - здобувач на достатньому рівні володіє навчальним матеріалом, впевнено та обґрунтовано його викладає. У підготовленому конспекті зміст питань розкрито з використанням переважно обов'язкової літератури. Здобувач допускає лише поодинокі несуттєві неточності, які здатний виправити самостійно.

3 бали - здобувач загалом володіє матеріалом та викладає його основний зміст, проте робить це без глибокого всебічного аналізу та аргументації. Матеріал підготовлено без використання всієї необхідної літератури. Здобувач допускає окремі суттєві неточності та помилки під час відповіді.

2 бали - здобувач лише фрагментарно або частково володіє матеріалом, викладає його поверхово, неповно і без належного обґрунтування. Під час обговорення здобувач плутається в базовій термінології, не здатний до самостійної аргументації та потребує

навідних питань від викладача.

1 бал - здобувач мінімально володіє навчальним матеріалом. Він не в змозі викласти зміст питань самостійної роботи, не розуміє теоретичного матеріалу та допускає суттєві помилки.

Методи навчання

Викладання засноване на тісній взаємодії між викладачем та здобувачем із використанням інтерактивних методів з тим, щоб допомогти студентам розвивати аналітичні навички, здатність до логічно-обґрунтованої аргументації та розуміння міжнародно-правових аспектів з позицій доктрини та принципу верховенства права. Під час лекційних занять, в основному, використовуються пояснювально-ілюстративний, пізнавально-пошуковий та інтерактивний методи навчання і викладання: пояснення нового матеріалу, що має проблемний характер, у формі повідомлень, дискусій, консультацій, розв'язання ситуативних завдань, із застосуванням новітніх інформаційно- комунікаційних технологій; організація лекції у формі, коли студенти можуть аргументовано висловлювати свої погляди та аналізувати позиції різних країн, демонстрація презентацій, інтерактивних платформ, віртуальних екскурсій до європейських інституцій тощо з тематики лекційного заняття.

Поєднання компетентнісного та інтерактивного підходів становить основу організації та проведення практичних занять з дисципліни. Використовується індивідуальна або групова робота, що передбачає колоквіуми, дебати, розв'язання реальних кейсів, завдань, які вимагають збору, систематизації та аналізу інформації з національних і міжнародних джерел, її міжнародно-правової оцінки. Окрім цього, застосовується метод використання інформаційно-комунікаційних технологій, зокрема демонстрація презентацій, доповідей, рефератів, есе, колективна робота з нормативною базою.

Для забезпечення ефективного засвоєння міждисциплінарного матеріалу у процесі викладання освітнього компонента використовується комплексний підхід, що поєднує традиційні та інноваційні методи навчання.

Методи формування професійної компетентності (набуття теоретичних знань):

- проблемна лекція (розкриття теоретичного матеріалу через призму актуальних правових колізій (наприклад, конфлікт між стрімким розвитком систем штучного інтелекту та фундаментальним правом особи на приватність);
- лекція-візуалізація (використання мультимедійних презентацій, інфографік, блок-схем та таблиць для наочного пояснення складної архітектури європейського законодавства та алгоритмів опрацювання даних);
- дискусія (залучення здобувачів до аргументованого обговорення проблемних питань під час практичних занять, стимулювання критичного мислення щодо доктринальних концепцій цифрових прав людини).

Методи формування практичних умінь та навичок:

- Case study (системний аналіз та розв'язання реальних правових ситуацій на основі прецедентної практики Європейського суду з прав людини та Суду Справедливості ЄС);

- юридичне моделювання та Moot court (симуляція процедури судових засідань або оскарження рішень наглядових органів);
- метод аналізу та розробки юридичних документів (практична робота зі складання політики конфіденційності, форми надання згоди, звітів з оцінки впливу на захист даних та аналізу міжнародних нормативних документів);
- робота з правовими першоджерелами (самостійний пошук та опрацювання студентами рішень міжнародних судів і рекомендацій європейських інституцій у цифрових архівах та бібліотечних базах).

Методи стимулювання пізнавальної активності та самостійної роботи:
- проєктний метод (робота в малих групах над розробкою комплексних стратегій захисту даних для гіпотетичних клієнтів)
- метод наукового пошуку (підготовка індивідуальних науково-аналітичних есе, тез для студентських науково-практичних конференцій та розробка мультимедійних презентацій для публічного захисту);
- взаємооцінювання (критичний аналіз студентами юридичних документів чи презентацій, підготовлених колегами).

Система контролю та оцінювання

Методи поточного контролю:
- індивідуальне і фронтальне усне опитування;
- бліц-опитування;
- письмові самостійні роботи (реферати, есе);
- ведення термінологічного словника;
- виконання практичних, індивідуальних та самостійних завдань;
- розв’язання проблемних ситуацій та правових задач;
- тестування (стандартизовані тести);
- презентації результатів досліджень.

Форми контролю:
- **поточний контроль** (здійснюється на практичних заняттях та за результатами виконання завдань самостійної роботи);
- **підсумковий контроль** (комбінований екзамен, який поєднує дві форми контролю: відповідь на теоретичні питання, передбачені робочою програмою навчальної дисципліни та розв’язання тестових завдань).

Критерії оцінювання поточного та підсумкового контролю

Поточний контроль проводиться на кожному практичному занятті та за результатами виконання завдань самостійної роботи. Він передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначеної теми (у тому числі, самостійно опрацьованого матеріалу) під час роботи на практичних заняттях та самостійного виконання завдань, передбачених робочою програмою навчальної дсципліни.

Критерії поточного оцінювання знань здобувачів за темами

№	Тема	Критерії оцінювання
1.	Поняття та еволюція права на повагу до приватного життя у міжнародному праві	**3 бали** — студент демонструє системне розуміння поняття та змісту права на приватне життя, правильно співвідносить положення ст. 12 ЗДПЛ, ст. 17 МПГПП та ст. 8 ЄКПЛ, аргументовано визначає критерії правомірності втручання та застосовує тест пропорційності до запропонованої ситуації; використовує належні міжнародно-правові джерела та судову практику. **2 бали** — студент загалом правильно характеризує право на приватне життя та відповідні міжнародно-правові стандарти, визначає основні критерії правомірності втручання, однак допускає окремі неточності або недостатньо обґрунтовує застосування тесту пропорційності. **1 бал** — студент відтворює окремі положення теми, але має труднощі з їх систематизацією та практичним застосуванням; аргументація неповна, наявні суттєві неточності. **0 балів** — студент не демонструє розуміння змісту права на приватність та не може застосувати міжнародно-правові критерії до практичної ситуації.
2.	Персональні дані: поняття, характерні ознаки та джерела міжнародно-правового регулювання	**3 бали** — студент правильно кваліфікує запропоновану інформацію як персональні, чутливі або знеособлені дані, розмежовує анонімізацію і псевдонімізацію, коректно використовує поняття суб’єкта даних, контролера та оператора, проводить порівняння підходів GDPR і Конвенції 108+. **2 бали** — правильно визначає основні ознаки персональних даних та їх категорії, однак допускає незначні помилки при кваліфікації окремих видів інформації або порівнянні правових термінів. **1 бал** — має загальне уявлення про персональні дані, проте не може належним чином провести їх правову кваліфікацію або розмежувати основні категорії. **0 балів** — не розуміє правової природи персональних даних та не може виконати завдання щодо їх класифікації.
3.	Місце права на захист даних у системі прав людини четвертого покоління	**3 бали** — студент аргументовано розкриває поняття цифрових прав людини, визначає їх співвідношення з класичними правами, обґрунтовує місце права на захист персональних даних у системі прав людини четвертого покоління та формує самостійну юридично аргументовану позицію щодо правової природи цифрових прав. **2 бали** — студент правильно характеризує основні ознаки цифрових прав та їх зв’язок із традиційними правами людини, однак аргументація щодо їх самостійності або місця в системі прав людини є недостатньо розгорнутою.

		1 бал — студент відтворює окремі теоретичні положення, але не забезпечує належного порівняльного та критичного аналізу. **0 балів** — не розуміє основних теоретичних категорій теми.
4.	Універсальні стандарти захисту конфіденційності у міжнародному праві	**4 бали** — студент системно характеризує універсальні міжнародно-правові стандарти захисту приватності, визначає роль ООН, Комітету з прав людини, Спеціального доповідача ООН та ОЕСР, критично оцінює відповідну резолюцію або доповідь і аргументовано визначає критерії правомірності масового стеження та використання шпигунського програмного забезпечення. **3 бали** — студент належно характеризує основні універсальні стандарти та інституційні механізми, правильно визначає ключові критерії правомірності втручання, але допускає окремі неточності або недостатню глибину аналізу. **2 бали** — студент знає основні міжнародні акти та механізми, але переважно відтворює матеріал без достатньої критичної оцінки та аргументації. **1 бал** — має фрагментарні знання та не може повноцінно застосувати міжнародні стандарти до проблеми масового стеження. **0 балів** — не демонструє знань щодо універсальних стандартів захисту приватності.
5.	Захист персональних даних у діяльності Ради Європи та Європейського Союзу	**4 бали** — студент правильно визначає співвідношення стандартів Ради Європи та права ЄС, застосовує положення GDPR, Конвенції 108+ та Регламенту (ЄС) 2024/1689, аргументовано визначає правомірність використання систем ШІ для скорингу або прийняття кадрових рішень і пропонує належний механізм захисту особи. **3 бали** — студент правильно застосовує основні положення GDPR та законодавства ЄС, розуміє особливості автоматизованого ухвалення рішень, але допускає окремі неточності у співвідношенні відповідних актів. **2 бали** — знає основні положення GDPR та загальні принципи регулювання ШІ, проте їх практичне застосування є поверховим. **1 бал** — має фрагментарні знання та не може належним чином визначити правомірність обробки даних або алгоритмічного рішення. **0 балів** — не володіє основними правовими положеннями теми.
6.	Право на захист персональних даних через призму практики ЄСПЛ та Суду Справедливості ЄС	**4 бали** — студент здійснює комплексний аналіз відповідної практики ЄСПЛ і Суду Справедливості ЄС, правильно визначає правові позиції у справах щодо масового стеження, біометричних даних, транскордонної передачі та «права бути забутим», аргументовано

		застосовує сформульовані судами критерії до запропонованої ситуації. **3 бали** — правильно визначає правові позиції основних рішень та може застосувати їх до практичної ситуації, однак аналіз окремих критеріїв або співвідношення юрисдикцій є недостатньо глибоким. **2 бали** — знає основний зміст відповідної судової практики, але переважно переказує рішення без належного виокремлення правових позицій та їх практичного застосування. **1 бал** — знає окремі справи, але не може сформулювати їхнє правове значення. **0 балів** — не володіє практикою європейських судових інституцій у сфері захисту даних.
7.	Проблеми та перспективи забезпечення права на конфіденційність в умовах європейської інтеграції України	**4 бали** — студент здійснює комплексне порівняння українського законодавства та GDPR, правильно визначає основні розбіжності, обґрунтовує напрями адаптації законодавства України та формулює послідовні й юридично обґрунтовані пропозиції щодо реформування національної системи захисту даних. **3 бали** — студент правильно визначає основні напрями гармонізації українського законодавства з правом ЄС та аргументує відповідні пропозиції, але окремі положення потребують конкретизації. **2 бали** — студент характеризує загальні проблеми адаптації законодавства України, але не демонструє достатньої здатності до порівняльного аналізу та вироблення конкретних пропозицій. **1 бал** — має загальне уявлення про євроінтеграційні процеси у сфері захисту даних, але не може визначити практичні напрями правової адаптації. **0 балів** — не розуміє основних проблем гармонізації українського законодавства з правом ЄС.
8.	Принципи опрацювання персональних даних	**3 бали** — студент правильно визначає зміст і юридичне значення принципів обробки даних, може застосувати їх до аналізу реальної політики конфіденційності, виявляє порушення принципів прозорості, мінімізації та обмеження мети і пропонує юридично обґрунтовані зміни. **2 бали** — правильно характеризує основні принципи та виявляє більшість недоліків політики конфіденційності, однак окремі висновки або запропоновані зміни недостатньо обґрунтовані. **1 бал** — знає окремі принципи, але має труднощі з їх практичним застосуванням до конкретного документа. **0 балів** — не може визначити зміст основних принципів опрацювання персональних даних.
9.	Підстави обробки персональних даних	**3 бали** — студент правильно визначає належну правову підставу обробки у конкретній ситуації, розмежовує згоду, виконання договору, юридичного обов’язку, завдання в суспільних інтересах та захист життєво

		важливих інтересів, оцінює легітимність масової обробки даних для навчання систем ШІ. **2 бали** — правильно характеризує більшість законних підстав і може застосувати їх до практичної ситуації, але допускає окремі неточності щодо умов їх використання. **1 бал** — знає основні підстави обробки, але не може належним чином визначити, яка саме підстава застосовується у конкретному випадку. **0 балів** — не розуміє системи правових підстав обробки персональних даних.
10.	Права та обов'язки осіб під час процедури опрацювання персональних даних	**4 бали** — студент правильно визначає зміст і межі прав суб'єкта даних, порядок їх реалізації та обов'язки контролера і розпорядника, здатний підготувати юридично обґрунтований запит щодо доступу до даних, визначити алгоритм реалізації права на мобільність та розмежувати повноваження відповідальних осіб. **3 бали** — правильно характеризує основні права суб'єкта даних та обов'язки контролера, може застосувати їх у практичній ситуації, але допускає окремі неточності щодо процедури реалізації. **2 бали** — знає основні права та обов'язки, однак практична частина виконана неповно або без достатнього правового обґрунтування. **1 бал** — має фрагментарне уявлення про права суб'єкта даних та обов'язки контролера. **0 балів** — не може визначити основні права та обов'язки учасників правовідносин.
11.	Актуальні питання опрацювання окремих категорій персональних даних особи	**4 бали** — студент правильно кваліфікує особливі категорії даних, визначає умови допустимості їх обробки, застосовує міжнародні та європейські стандарти до біометричних, генетичних, медичних даних і даних дітей, оцінює ризики дискримінації та алгоритмічного упередження. **3 бали** — правильно характеризує правовий режим чутливих даних і основні гарантії їх захисту, але недостатньо глибоко аналізує окремі спеціальні випадки. **2 бали** — знає основні категорії чутливих даних та загальну заборону їх обробки, однак не завжди правильно визначає винятки та умови правомірності. **1 бал** — має фрагментарні знання щодо спеціальних категорій даних. **0 балів** — не розуміє особливостей правового режиму чутливих персональних даних.
12.	Особливості процедури обробки даних системами штучного інтелекту	**4 бали** — студент комплексно оцінює правомірність обробки даних системами ШІ, розмежовує алгоритмічну прозорість і «право на пояснення», застосовує ризик-орієнтований підхід, оцінює законність автоматизованого збору даних, біометричної ідентифікації та визначає можливі засоби захисту у разі дискримінаційного або помилкового рішення. **3 бали** — правильно характеризує основні правові ризики обробки даних системами ШІ та може застосувати

		відповідні правові стандарти, але окремі висновки недостатньо аргументовані. **2 бали** — знає ключові проблеми використання ШІ у сфері персональних даних, проте практичне застосування норм є неповним. **1 бал** — має загальне уявлення про взаємозв'язок ШІ та захисту персональних даних, але не здатний належно кваліфікувати конкретну ситуацію. **0 балів** — не демонструє розуміння основних правових проблем обробки даних системами ШІ.
13.	Інституційні механізми нагляду та контролю за опрацюванням персональних даних	**3 бали** — студент правильно визначає систему наглядових механізмів на універсальному, європейському та національному рівнях, розмежовує повноваження Європейського інспектора із захисту даних, Європейської ради з питань захисту даних і національних органів, пояснює механізм «єдиного вікна» та засоби оскарження рішень наглядових органів. **2 бали** — правильно характеризує основні інституційні механізми та їх повноваження, але допускає окремі неточності щодо розмежування компетенції. **1 бал** — знає окремі наглядові органи та їх функції, але не може системно пояснити механізм їх взаємодії. **0 балів** — не розуміє інституційної системи нагляду за захистом персональних даних.
14.	Засоби правового захисту та відповідальність за порушення у сфері обробки персональних даних	**4 бали** — студент правильно визначає ефективний засіб правового захисту залежно від характеру порушення, визначає порядок звернення до наглядового або судового органу, обґрунтовує можливість відшкодування матеріальної та нематеріальної шкоди, розмежовує цивільну, адміністративну, кримінальну та міжнародно-правову відповідальність і враховує специфіку порушень, пов'язаних із системами ШІ. **3 бали** — правильно визначає основні засоби правового захисту та види відповідальності, може застосувати їх до конкретної ситуації, але допускає окремі неточності щодо процедури або правових наслідків. **2 бали** — знає основні способи захисту та види відповідальності, однак не завжди правильно визначає належний механізм реагування на конкретне порушення. **1 бал** — має фрагментарні знання щодо засобів захисту та відповідальності. **0 балів** — не може визначити належний спосіб захисту порушеного права та відповідний вид юридичної відповідальності.

Критерії підсумкового оцінювання знань здобувачів

Підсумковий семестровий контроль оцінюється **від 0 до 100** балів і переводиться у національну шкалу та шкалу ЄКТС:

- здобувачам вищої освіти, які повністю оволоділи програмою навчальної дисципліни на творчому рівні, можуть дати відповіді на всі питання курсу, опанували

рекомендовану літературу, виставляють оцінку **A**. При цьому оцінку - 100 балів, як виняток, можуть отримати тільки здобувачі вищої освіти, які, крім відмінних знань за програмою дисципліни, виявили активність в науково-дослідній роботі за тематикою курсу, стали призерами студентських олімпіад, виступали на конференціях тощо;

- здобувачам вищої освіти, які оволоділи програмою навчальної дисципліни на творчому рівні, проте у відповідях допустили незначні неточності, ставлять оцінку **B**;
- здобувачам вищої освіти, які в основному оволоділи програмою навчальної дисципліни на продуктивному рівні, проте у відповідях допускають несуттєві помилки, ставлять оцінку **C**;
- здобувачам вищої освіти, які показали задовільні результати оволодіння Робочою програмою навчальної дисципліни на репродуктивному рівні й при відповідях допускають помилки, ставлять оцінку **D**;
- здобувачам вищої освіти, які виявили мінімально достатній рівень знань з дисципліни, необхідний для продовження навчання, вивчили основні терміни курсу та орієнтуються в матеріалі базового підручника, ставлять оцінку **E**.
- здобувачі вищої освіти, які за результатами вивчення дисципліни отримали незадовільні оцінки **FX** або **F**, повинні додатково виконати індивідуальні завдання для підвищення рівня своїх знань і при оцінці FX повторно перескласти підсумковий контроль, а при оцінці F пройти повторний курс вивчення дисципліни зі складанням підсумкового контролю.

Підсумковий контроль проводиться у формі комбінованого екзамену, який передбачає відповідь на теоретичні питання, передбачені робочою програмою навчальної дисципліни, та виконання 25 тестових завдань. Максимальна кількість балів за екзамен становить **50 балів**, з них **25 балів – за усну відповідь на теоретичні питання та 25 балів – за виконання тестових завдань.**

Критерії оцінювання усної відповіді під час екзамену:

23–25 балів — студент демонструє системні, глибокі та ґрунтовні знання з відповідних тем навчальної дисципліни; повно, логічно та послідовно розкриває зміст теоретичних питань; правильно застосовує міжнародно-правові норми, стандарти захисту персональних даних та конфіденційності, положення права Європейського Союзу, практику ЄСПЛ і Суду Справедливості ЄС; здійснює належний правовий аналіз, використовує відповідну юридичну термінологію, формулює аргументовані висновки та демонструє здатність застосовувати набуті знання до практичних правових ситуацій.

19–22 бали — студент демонструє достатньо повні та системні знання, розкриває основний зміст теоретичних питань, правильно характеризує відповідні міжнародно-правові та європейські стандарти, може застосовувати їх до правових ситуацій. Відповідь є загалом обґрунтованою, однак допускаються окремі неточності, недостатня глибина розкриття окремих положень або незначні помилки в аргументації.

15–18 балів — студент володіє основним обсягом навчального матеріалу, проте відповідь характеризується неповнотою, недостатньою системністю або поверховістю окремих положень. Правильно відтворює основні поняття, принципи та нормативні положення, однак має труднощі з їх комплексним аналізом, порівнянням та практичним застосуванням. Допускає окремі суттєві неточності.

10–14 балів — студент демонструє фрагментарні знання з основних питань

дисципліни, розкриває лише окремі положення теоретичного матеріалу, допускає суттєві помилки у визначенні понять, характеристиці міжнародно-правових норм та судової практики. Практичне застосування знань є обмеженим, аргументація недостатня.

5–9 балів — студент володіє лише окремими елементами навчального матеріалу, не може послідовно розкрити зміст більшості поставлених питань, допускає численні помилки та неточності, не демонструє належного розуміння взаємозв'язків між міжнародними та європейськими стандартами захисту персональних даних.

1–4 бали — студент демонструє мінімальні та несистемні знання, не може належним чином розкрити зміст теоретичних питань, допускає істотні помилки, не здатний застосувати положення навчальної дисципліни до практичних ситуацій.

0 балів — студент не надав змістовної відповіді на теоретичні питання або не продемонстрував знань навчального матеріалу.

Тестова частина складається з **25 тестових завдань**, кожне з яких оцінюється в **1 бал** за умови вибору правильної відповіді.

Підсумкова оцінка за екзамен визначається як сума балів, отриманих за усну відповідь на теоретичні питання та виконання тестових завдань. Максимальна оцінка за підсумковий контроль становить **50 балів**.

Розподіл балів, які отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)														Кількість балів (екзаменаційна робота)	Сумарна к-ть балів
Змістовий модуль №1							Змістовий модуль № 2								
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т 10	Т 11	Т 12	Т 13	Т 14	50	100
3	3	3	4	4	4	4	3	3	4	4	4	3	4		

Т1, Т2 ... Т14 – теми змістових модулів.

Шкала оцінювання: національна та ЄКТС

Оцінка за національною шкалою	**Оцінка за шкалою ЄКТС**	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Відмінно	A (90-100)	відмінно
Добре	B (80-89)	дуже добре
	C (70-79)	добре
Задовільно	D (60-69)	задовільно
	E (50-59)	достатньо
Незадовільно	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно) з обов'язковим самостійним опрацюванням освітнього компоненту до перескладання

Перелік питань для самоконтролю та підсумкового контролю навчальних досягнень студентів

1. Дайте визначення права на повагу до приватного життя та охарактеризуйте його генезу в умовах цифрової трансформації суспільства.
2. Проаналізуйте нормативне закріплення права на конфіденційність в системі універсальних міжнародних актів.
3. Розкрийте міжнародно-правові критерії правомірного втручання у приватне життя особи.
4. Охарактеризуйте еволюційне тлумачення поняття «приватне життя» крізь призму статті 8 Конвенції про захист прав людини і основоположних свобод.
5. Дайте визначення персональних даних, охарактеризуйте їх правову природу та ключові маркери, що дозволяють відмежувати їх від знеособленої інформації.
6. Здійсніть порівняльний аналіз процедур анонімізації та псевдонімізації, розкривши їх теоретичні відмінності та правові наслідки для статусу даних.
7. Охарактеризуйте систему та види джерел правового регулювання відносин у сфері обробки персональних даних, виокремивши загальні та особливі (чутливі) категорії даних.
8. Дайте визначення цифрових прав людини, розкрийте їх специфічні ознаки та проаналізуйте їх співвідношення з класичними правами людини.
9. Охарактеризуйте місце права на захист персональних даних в ієрархії прав людини четвертого покоління та проаналізуйте вплив штучного інтелекту на їх трансформацію.
10. Проаналізуйте право на забуття як самостійне цифрове право, розкривши його зміст, критерії та межі реалізації в інформаційному суспільстві.
11. Проаналізуйте базові стандарти захисту приватності в системі універсальних міжнародно-правових актів.
12. Охарактеризуйте роль Керівних принципів ООН (1990 р.) та ОЕСР у формуванні універсального регулювання обробки персональних даних.
13. Проаналізуйте правові наслідки резолюцій Генеральної Асамблеї ООН щодо права на приватність у цифрову епоху.
14. Охарактеризуйте систему стандартів Ради Європи у сфері захисту даних та проаналізуйте її взаємодію з правом Європейського Союзу.
15. Проаналізуйте основні принципи обробки, ключові права суб'єктів даних та екстериторіальну дію Загального регламенту про захист даних ЄС.
16. Здійсніть аналіз співвідношення вимог GDPR та положень Європейського акта про штучний інтелект у контексті управління даними.
17. Проаналізуйте прецедентну практику ЄСПЛ щодо програм масового стеження та таємного перехоплення комунікацій, розкривши критерії балансу з інтересами національної безпеки.
18. Охарактеризуйте підходи ЄСПЛ до захисту біометричних і генетичних даних та профілювання на основі ключових рішень Суду.
19. Проаналізуйте роль Суду Справедливості ЄС у формуванні стандартів захисту даних, утвердженні «права бути забутим» та регулюванні транскордонного передавання даних.

20. Охарактеризуйте стан національного законодавства України у сфері захисту персональних даних та виокремте ризики в умовах цифровізації державних послуг.

21. Проаналізуйте зобов'язання України щодо імплементації стандартів GDPR відповідно до Угоди про асоціацію з ЄС та розкрийте перспективи повноцінної інтеграції до Єдиного цифрового ринку.

22. Дайте визначення та розкрийте юридичне значення принципів законності, справедливості та прозорості опрацювання персональних даних.

23. Проаналізуйте зміст принципів мінімізації даних та обмеження зберігання, охарактеризувавши виклики щодо їх дотримання в епоху Big Data.

24. Охарактеризуйте принципи обмеження мети, точності, цілісності, конфіденційності та підзвітності у контексті міжнародних стандартів обробки даних.

25. Дайте визначення та перелік законних підстав для обробки персональних даних за міжнародним правом та правом ЄС.

26. Проаналізуйте критерії дійсності згоди суб'єкта даних, механізм її відкликання та розкрийте правову проблему «згоди за замовчуванням».

27. Охарактеризуйте специфіку застосування таких підстав обробки, як виконання юридичного обов'язку, захист життєво важливих інтересів та суспільний інтерес, у тому числі для навчання ШІ.

28. Проаналізуйте зміст права на інформацію, доступ, виправлення та обмеження обробки персональних даних у міжнародно-правовому вимірі.

29. Охарактеризуйте права особи щодо захисту від автоматизованого індивідуального ухвалення рішень, профілювання та прямого маркетингу.

30. Розкрийте правовий статус, ключові обов'язки та межі відповідальності володільця (контролера) і розпорядника (оператора) персональних даних.

31. Дайте визначення особливих (чутливих) категорій персональних даних та проаналізуйте правові підстави, що становлять виняток із загальної заборони на їх обробку.

32. Охарактеризуйте ризики та міжнародні гарантії захисту при обробці біометричних даних, генетичних даних та інформації про стан здоров'я.

33. Проаналізуйте правовий режим опрацювання персональних даних дітей.

34. Охарактеризуйте специфіку захисту чутливих даних в умовах збройних конфліктів та ризику алгоритмічного упередження.

35. Охарактеризуйте штучний інтелект як об'єкт міжнародно-правового регулювання та проаналізуйте ризик-орієнтований підхід до алгоритмічних систем за законодавством ЄС.

36. Проаналізуйте зміст «права на пояснення» та розкрийте механізми забезпечення алгоритмічної прозорості при автоматизованому зборі масивів даних.

37. Охарактеризуйте міжнародно-правові межі застосування систем біометричної ідентифікації в режимі реального часу та специфіку відповідальності за помилкові рішення ШІ.

38. Проаналізуйте систему інституційних механізмів нагляду за дотриманням законодавства про захист даних на універсальному та регіональному рівнях.

39. Охарактеризуйте статус, мандат та повноваження Європейського інспектора з питань захисту даних та Європейської ради з питань захисту даних.

40. Розкрийте критерії незалежності та вимоги до функціонування національних наглядових органів, а також проаналізуйте ефективність механізму «єдиного вікна».

41. Проаналізуйте механізми реалізації права на ефективний засіб судового та адміністративного захисту у сфері опрацювання персональних даних.

42. Охарактеризуйте підстави та критерії відшкодування матеріальної і нематеріальної шкоди, заподіяної внаслідок порушення законодавства про захист даних.

43. Проаналізуйте специфіку притягнення до відповідальності за неправомірне опрацювання даних автономними системами ШІ.

44. Розкрийте підстави міжнародно-правової відповідальності держави у цифровій сфері.

Зарахування результатів неформальної освіти

Індивідуальна траєкторія здобувача вищої освіти у процесі вивченні навчальної дисципліни також реалізується через участь у неформальній/інформальній освіті.

Зарахування результатів неформальної освіти здійснюється на основі Порядку визнання у Чернівецькому національному університеті імені Юрія Федьковича результатів навчання, здобутих шляхом неформальної та/або інформальної освіти (URL: https://media.chnu.edu.ua/media/4g5fzssb/poriadok-vyznannia-rezultativ-navchannia-zdobutykh-shliakhom-neformalnoi-ta-abo-informalnoi-osvity.pdf).

За наявності належного сертифіката здобувачу освіти нараховується **3 бали** за відповідну тему, що прирівнюється до оцінювання виконання завдань практичного заняття. До зарахування приймаються результати проходження окремих тем дисципліни на авторитетних онлайн-платформах, наприклад, Coursera, Prometheus, навчальних курсів HELP, зокрема, але не виключно, наступних:

- *Artificial Intelligence and Human Rights* (освітня платформа Council of Europe HELP Programme): https://help.elearning.ext.coe.int/enrol/index.php?id=7331
- *Access to Justice in the Digital Environment* (освітня платформа Council of Europe HELP Programme): https://help.elearning.ext.coe.int/enrol/index.php?id=8402
- *Інтернет та цифрові права людини* (освітня платформа ВУМ online): https://vumonline.ua/course/internet-and-digital-rights/
- *Data Protection and Privacy Rights* (освітня платформа Council of Europe HELP Programme): https://help.elearning.ext.coe.int/enrol/index.php?id=1658

Рекомендована література

Основна

1. Charter of Fundamental Rights of European Union. Official journal of European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT.
2. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828

(Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
3. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Judgment of the Court (Grand Chamber), 13 May 2014. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62012CJ0131.
4. Верховна Рада України. (1992). Про інформацію (Закон № 2657-XII). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
5. Верховна Рада України. (2010). Про захист персональних даних (Закон № 2297-VI). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Генеральна Асамблея ООН. (1990). Керівні принципи щодо регламентації комп'ютеризованих картотек персональних даних (Резолюція 45/95). URL: https://digitallibrary.un.org/record/105299?v=pdf.
7. Генеральна Асамблея ООН. (2013). Право на недоторканність приватного життя в цифрову епоху (Резолюція 68/167). URL: https://digitallibrary.un.org/record/764407/files/A_RES_68_167-EN.pdf.
8. Європейська соціальна хартія (переглянута): міжнародний документ. Страсбург, 3 травня 1996 р. Відомості Верховної Ради України, 2006, № 43, ст. 418. URL: https://zakon.rada.gov.ua/laws/show/994_062#Text.
9. Європейський Союз, Європейське співтовариство з атомної енергії та Україна. (2014). Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.
10. Європейський суд з прав людини. (2008, 4 грудня). Справа «S. and Marper v. the United Kingdom» (Заяви № 30562/04 та 30566/04). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}.
11. Європейський суд з прав людини. (2020, 13 лютого). Справа «Gaughran v. the United Kingdom» (Заява № 45245/15). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]}.
12. Європейський суд з прав людини. (2021, 25 травня). Справа «Big Brother Watch and Others v. the United Kingdom» (Заяви № 58170/13, 62322/14 та 24960/15). URL: https://hudoc.echr.coe.int/ukr#{%22itemid%22:[%22001-210077%22]}.
13. Загальна декларація прав людини: міжнародний документ. ООН, 10.12.1948. URL: https://zakon.rada.gov.ua/go/995_015.
14. Комітет з прав людини ООН. (1988). Загальний коментар № 16: Стаття 17 (Право на недоторканність приватного життя). Управління Верховного комісара ООН з прав людини. URL: https://www.refworld.org/legal/general/hrc/1988/27539.
15. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. № 994_326. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.
16. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 4 листопада 1950 р. № 995_004. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
17. Міжнародний пакт про громадянські і політичні права (Міжнародний пакт ратифіковано Указом Президії Верховної Ради Української РСР № 2148 VIII (2148-08) від 19.10.1973 року). URL: https://zakon.rada.gov.ua/laws/show/995_043#.

18. Міжнародний пакт про економічні, соціальні і культурні права: Міжнародний документ. Організація Об'єднаних Націй, 19.10.1973. URL: https://zakon.rada.gov.ua/laws/show/995_042#Text.
19. Організація економічного співробітництва та розвитку (ОЕСР). (2013). Керівні принципи ОЕСР щодо захисту приватності та транскордонного передавання персональних даних. URL: https://www.oecd.org/en/topics/privacy-principles.html.
20. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. № 984_008-16. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Додаткова

1. Alwirfili, N. Z. A. (2024). The right to privacy in the digital age. Al-Haq Journal for Sharia and Legal Sciences, 139-157. URL: https://www.al-haqjournal.ly/index.php/alhaq/article/view/242.
2. Ienca, M., & Malgieri, G. (2022). Mental data protection and the GDPR. Journal of Law and the Biosciences, 9(1), lsac006. URL: https://academic.oup.com/jlb/article-pdf/doi/10.1093/jlb/lsac006/43965523/lsac006.pdf.
3. Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. Management Science, 69(8), 4389-4412. URL: https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2022.4614.
4. Labyk A., Toronchuk I. Problems and Prospects for Ensuring Digital Human Rights in Terms of Ukraine's European Integration. International Conference on EU Prospectives (29-30 May, 2026, Batumi, Georgia). Batumi: Batumi Shota Rustaveli State University, 2026. P. 191-200. URL: https://dspace.chnu.edu.ua/handle/123456789/14741.
5. Labyk A. Algorithmic Discrimination as a Threat to Digital Human Rights: a Theoretical and Legal Dimension. Journal of International and European Law. 2026. Issue 1. P. 53-64. DOI: https://doi.org/10.31861/jiel.2026.1.53-64.
6. Бліхар, М. (2023). Організаційно-правовий механізм захисту персональних даних. Науковий вісник Ужгородського національного університету. Серія: Право, 2(77), 31-36. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/283773.
7. Ванкевич, О. (2024). Право на приватність у практиці ЄСПЛ. Наукові заходи Юридичного факультету Західноукраїнського національного університету, 131-135. URL: http://confuf.wunu.edu.ua/index.php/confuf/article/download/1456/1435.
8. Волкова, Ю. Ф. (2023). Право на приватність в умовах глобалізації. Аналітично-порівняльне правознавство, (5), 113-118. URL: http://journal-app.uzhnu.edu.ua/article/view/290532.
9. Гаращенко, В. В. (2025). Захист персональних даних: західна доктрина та судова практика. Науковий вісник Ужгородського національного університету. Серія: Право, 1(92), 45-52. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/350039.
10. Головацький, Н. Т. (2024). Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України. Науковий вісник Ужгородського національного університету. Серія: Право, 2(85), 288-292. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/315396.
11. Гудзь, Л. В. (2024). Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання. Науковий вісник

Ужгородського національного університету. Серія: Право, 1(86), 175-180. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/320125.
12. Дяковський, О. С. Характерні риси прояву захисту персональних даних. Юридичний науковий електронний журнал. 2024. № 10. С. 230-232. URL: https://ela.kpi.ua/items/84af850a-160f-4f3b-8c5a-629001ba8541.
13. Кожухар О. Правове регулювання систем штучного інтелекту та захист персональних даних: лінії взаємозв'язків. Наукові записки НаУКМА. Юридичні науки. 2025. Т. 16. С. 80-87. URL: https://ekmair.ukma.edu.ua/items/d1c771c5-f999-46b2-9bba-dff1c9dfe27d.
14. Лабик А. Право на пояснення алгоритмічних рішень у системі цифрових прав людини. Науковий вісник Ужгородського Національного Університету. Серія Право. 2025. Вип. 92. Ч. 5. С. 209-214. URL: https://archer.chnu.edu.ua/xmlui/handle/123456789/13728.
15. Пальчик, М. Л., Шкрібляк, К. П., & Березделцький, Ю. М. (2025). Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки україни в умовах війни. Аналітично-порівняльне правознавство, 2(6), 425-434. URL: http://journal-app.uzhnu.edu.ua/article/view/346536.
16. Попович, Т. П., Маслюк, О. В., & Мацола, А. А. (2025). Штучний інтелект та право на приватність: актуальні виклики цифрової епохи. Науковий вісник Ужгородського національного університету. Серія: Право, 5(90), 465-470. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/341218.
17. Телешев С. П. Особливості реалізації права фізичної особи на знищення інформації стосовно себе (право на забуття). Правова держава. 2023. № 51. С. 93-106.
18. Федорова, Т. С., & Дронов, В. Ю. (2023). Право на доступ до інформації та захист персональних даних у міжнародному праві та міжнародних відносинах. Нове українське право, (3), 41-46. URL: https://newukrainianlaw.in.ua/index.php/journal/article/view/480.
19. Чістякова, І. М., & Кудлай, І. В. (2026). Право на приватність як ключовий елемент формування глобального регулювання штучного інтелекту. Актуальні проблеми сталого розвитку, 3(5), 548-558. URL: https://journals.csr.com.ua/index.php/sustainability/article/view/596.
20. Щербак, О. В. (2025). Особливості інформаційно-правового забезпечення захисту персональних даних неповнолітніх. Сучасна доктрина права, (7 (89)), 45-51. URL: https://humanitarian.com.ua/index.php/juridical/article/download/190/209.

Інформаційні ресурси

1. https://www.rada.gov.ua/ - Офіційний портал Верховної Ради України.
2. https://www.kmu.gov.ua/ - Урядовий портал.
3. https://minjust.gov.ua/ua - Міністерство юстиції України.
4. http://www.un.org/ru/index.html - офіційний сайт Організації Об'єднаних Націй.
5. http://www.icj-cij.org/homepage/index.php?p1=0&lang=en – офіційний сайт Міжнародного Суду ООН.
6. https://www.coe.int/en/web/portal - вебсайт Ради Європи.
7. https://www.coe.int/uk/web/kyiv - Офіс Ради Європи в Україні.
8. https://www.osce.org/ - Організація з безпеки і співробітництва в Європі.

9. https://european-union.europa.eu – вебсайт Європейського Союзу.
10. https://eur-lex.europa.eu/homepage.html - законодавство Європейського Союзу.
11. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en - Court of Justice of the European Union (CJEU).
12. https://ukraine-eu.mfa.gov.ua/ - Представництво України при Європейському Союзі.
13. http://en.euabc.com/ - Інтернет-глосарій термінів ЄС.
14. https://www.oecd.org/ - Організація економічного співробітництва та розвитку.
15. https://www.echr.coe.int - вебсайт ЄСПЛ.
16. https://hudoc.echr.coe.int – документи Європейського суду з прав людини.
17. https://www.edpb.europa.eu/home_en - Європейська рада з питань захисту даних.
18. https://www.edps.europa.eu/_en - Європейський інспектор з питань захисту даних.
19. https://www.coe.int/en/web/data-protection - Портал Ради Європи із захисту даних.
20. https://fra.europa.eu/en - Агентство Європейського Союзу з основних прав.
21. https://digital-strategy.ec.europa.eu/en/policies/ai-office - Європейський офіс зі штучного інтелекту.
22. https://curia.europa.eu/ - База даних Суду Справедливості ЄС.
23. https://thedigital.gov.ua/ - Міністерство цифрової трансформації України.

Політика академічної доброчесності

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні освітнього компонента регламентовано чинними документами ЧНУ:

- «Етичний кодекс Чернівецького національного університету імені Юрія Федьковича»: https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/etychnyi-kodeks-chernivetskoho-natsionalnoho-universytetu-imeni-yuriia-fedkovycha/;
- «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університету імені Юрія Федьковича»: https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polozhennia-pro-vyiavlennia-ta-zapobihannia-akademichnomu-plahiatu-u-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/;
- «Політикою використання штучного інтелекту в Чернівецькому національному університету імені Юрія Федьковича»: https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polityka-vykorystannia-shtuchnoho-intelektu-v-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/.

Використання здобувачами освіти інструментів штучного інтелекту (ШІ) під час виконання навчальних завдань:

- допускається за умови дотримання принципів академічної доброчесності (здобувач освіти несе відповідальність за зміст, достовірність і результати поданої

роботи, а у разі використання ШІ зобов’язаний зазначити факт і спосіб його застосування);

- не допускається використання ШІ як заміни самостійного виконання завдань або з метою порушення вимог академічної доброчесності;
- додаткові обмеження чи вимоги щодо використання ШІ можуть визначатися викладачем в освітньому процесі для конкретних видів навчальної діяльності відповідно до особливостей дисципліни.