ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ЗАТВЕРДЖЕНО
Рішення вченої ради університету
«29» серпня 2025 року,
протокол № *1*.

Ректор, голова вченої ради університету,
доктор юридичних наук, професор

_____ Олег ОМЕЛЬЧУК
«29» серпня 2025 року
м.п.

РОБОЧА ПРОГРАМА
навчальної дисципліни
«ЗАХИСТ ПРАВ В МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ ТА ЄС»
для підготовки на першому (освітньому) рівні
здобувачів вищої освіти освітнього ступеня бакалавра
за спеціальністю 035 Філологія
спеціалізація 035.041 Германські мови та літератури
(переклад включно), перша – англійська
галузі знань 03 Гуманітарні науки

м. Хмельницький
2025

РОЗРОБНИК:

Професорка кафедри міжнародного та європейського права, кандидатка юридичних наук, доцентка _____ Роксолана ІВАНОВА
«26» серпня 2025 року

СХВАЛЕНО

Рішення кафедри міжнародного та європейського права
«26» серпня 2025 року, протокол № 1.

Завідувачка кафедри, кандидатка юридичних наук, доцентка _____ Світлана ЛОЗІНСЬКА
«26» серпня 2025 року

Деканеса факультету управління та економіки, кандидатка економічних наук, доцентка _____ Тетяна ТЕРЕЩЕНКО
«26» серпня 2025 року

ПОГОДЖЕНО

Рішення методичної ради університету
«27» серпня 2025 року, протокол № 1.

Перша проректорка, голова методичної ради університету, кандидатка наук з державного управління, доцентка _____ Ірина КОВТУН
«27» серпня 2025 року

Обліковий обсяг 0,90 ум. др. арк.

ЗМІСТ

1. Опис навчальної дисципліни

1.	Шифр і назва галузі знань	–	03 Гуманітарні науки
2.	Код і назва спеціальності	–	035 Філологія
3.	Назва спеціалізації	–	035.041 Германські мови та літератури (переклад включно), перша – англійська
4.	Назва дисципліни	–	Захист прав в мережі Інтернет Україні та ЄС
5.	Тип дисципліни	–	Вибіркова
6.	Код дисципліни	–	ППВ 6.3.
7.	Освітній рівень, на якому вивчається дисципліна	–	Перший
8.	Ступінь вищої освіти, що здобувається	–	Бакалавр
9.	Курс / рік навчання	–	Четвертий
10.	Семестр	–	Сьомий
11.	Обсяг вивчення дисципліни:		
	загальний обсяг (кредитів ЄКТС / годин)	–	4,0 / 120
	аудиторні заняття (годин)	–	36
	% від загального обсягу	–	30
	лекційні заняття (годин)	–	18
	% від обсягу аудиторних годин	–	50
	семінарські заняття (годин)	–	18
	% від обсягу аудиторних годин	–	50
	самостійна робота (годин)	–	84
	% від загального обсягу	–	70
	тижневих годин:		8,0
	аудиторних занять	–	3,0
	самостійної роботи	–	5,0
12.	Форма семестрового контролю	–	Залік
13.	Місце дисципліни в логічній схемі:		
	1) попередні дисципліни	–	ЗПО 6. Правознавство ППВ 5.4. Міжнародне право ЗПО 4. Інформаційні системи та технології ППВ 2.1. Основи міжкультурної комунікації
	2) супутні дисципліни	–	
	3) наступні дисципліни	–	ППВ 7.3 Комунікативні стратегії
14.	Мова вивчення дисципліни	–	Українська

2. Заплановані результати навчання

Програмні компетентності, які здобуваються під час вивчення навчальної дисципліни:

Загальні компетентності

ЗК 1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини ігромадянина в Україні.

ЗК 2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

ЗК 6. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел

ЗК 7. Уміння виявляти, ставити та вирішувати проблеми.

ЗК 8. Здатність працювати в команді та автономно.

ЗК 12. Навички використання інформаційних і комунікаційних технологій

Фахові компетентності

ФК 8. Здатність вільно оперувати спеціальною термінологією

ФК 11. Здатність до надання консультацій з дотримання норм літературної мови та культури мовлення.

ФК 12. Здатність до організації ділової комунікації

Результати навчання:

ПР 2. Ефективно працювати з інформацією з різних джерел, критично аналізувати й інтерпретувати її

ПР 5. Співпрацювати з колегами, представниками інших культур та релігій, прибічниками різних політичних поглядів тощо.

ПР 6. Використовувати інформаційні й комунікаційні технології для вирішення професійних задач

ПР 11. Принципи, технології і прийоми створення усних і письмових текстів різних жанрів і стилів

Після завершення вивчення дисципліни здобувач повинен продемонструвати такі результати навчання:	
1. Знання *(здатність запам'ятовувати або відтворювати факти (терміни, конкретні факти, методи і процедури, основні поняття, правила і принципи, цілісні теорії тощо)*	
1.1)	Знати зміст основних термінів інтернет-права та цифрових прав (персональні дані, обробка, контролер/процесор, кукі, кібербезпека, notice-and-action, посередник, контент-модерація, доменний спір тощо).
1.2)	Відтворювати основні напрями та школи дослідження прав у цифровому середовищі (захист даних і приватності, свобода вираження, кібербезпека, інтелектуальна власність онлайн, юрисдикція та колізійне право, електронні ідентифікації та довірчі послуги).
1.3)	Відтворювати хронологію (основні етапи) еволюції регулювання Інтернету в Україні та ЄС (від Конвенції Будапешт 2001 до GDPR, eIDAS, DSM-доктрини, DSA/NIS2, оновлень українського законодавства).
1.4)	Знати базові принципи, стратегії і процедури захисту прав онлайн (законність, пропорційність, мінімізація даних, безпека обробки; механізми звернень і видалення контенту, UDRP, подання скарг до наглядових органів, досудові й судові способи захисту).
2. Розуміння *(здатність розуміти та інтерпретувати вивчене, уміння пояснити факти, правила, принципи; перетворювати*	

словесний матеріал у, наприклад, математичні вирази; прогнозувати майбутні наслідки на основі отриманих знань)	
2.1)	Пояснювати підстави впровадження онлайн-захисту прав на рівні користувача, організації, платформи та держави/ЄС.
2.2)	Розуміти роботу ключових механізмів: запити суб'єкта даних (GDPR/ЗУ), notice-and-action (DSA), інциденти за NIS2, eIDAS, UDRP.
2.3)	Обґрунтовувати вибір інструментів захисту (правові підстави, DPIA, модерація, DMCA/«право на забуття», UDRP) та наслідки рішень.
2.4)	Пояснювати значення дотримання цифрових прав для етичної комунікації, захисту авторських прав і безпечної роботи з даними.
3. Застосування знань *(здатність використовувати вивчений матеріал у нових ситуаціях (наприклад, застосувати ідеї та концепції для розв'язання конкретних задач)*	
3.1)	Обирати належний спосіб захисту в конкретній ситуації (скарга до платформи/регулятора, позов, медіація, UDRP).
3.2)	Готувати запити суб'єкта даних і вимоги про видалення/виправлення (GDPR, Закон України про ПД).
3.3)	Формувати та впроваджувати внутрішні політики: захист даних, модерація контенту, notice-and-action (DSA).
3.4)	Застосовувати процедури реагування на інциденти й повідомлення про витоки (NIS2/нац. норми).
3.5)	Коректно використовувати інструменти авторського права онлайн: DMCA-takedown, DSM-винятки, ліцензування.
3.6)	Збирати й фіксувати електронні докази (скріншоти, хеші, логи) з дотриманням процесуальних вимог.
3.7)	Проводити базову DPIA/оцінку ризиків для нових онлайн-проєктів і сервісів.
3.8)	Оскаржувати незаконну обробку даних та профілювання (скарга до ДПУ/DPAs, судовий захист).
4. Аналіз *(здатність розбивати інформацію на компоненти, розуміти їх взаємозв'язки та організаційну структуру, бачити помилки й огріхи в логіці міркувань, різницю між фактами і наслідками, оцінювати значимість даних)*	
4.1)	Порівнювати правові режими України та ЄС (GDPR/ЗУ «Про ПД», DSA/нац. норми, NIS2/кібербезпека) й виявляти колізії.
4.2)	Розкладати кейс на складові: суб'єкти/об'єкти, підстави обробки, вид контенту, юрисдикція, засоби захисту.
4.3)	Відрізняти факти (докази, логи, метадані) від оцінок і припущень; будувати доказову базу.
4.4)	Аналізувати політики платформ (moderation, notice-and-action, appeals) на відповідність DSA/GDPR.
5. Синтез *(здатність поєднувати частини разом, щоб одержати ціле з новою системною властивістю)*	
5.1)	Поєднувати норми України, ЄС (GDPR, DSA, NIS2, eIDAS) і міжнародні акти (Конвенція Будапештська, 108+) у цілісну політику захисту прав онлайн.
5.2)	Інтегрувати інтереси й механізми захисту на трьох рівнях: індивідуальному (користувач), професійному/рольовому (перекладач, модератор, адміністратор), корпоративному (організація/платформа).
5.3)	Синхронізувати внутрішні процедури (privacy, notice-and-action, апеляції, реагування на інциденти) з політиками платформ і вимогами регуляторів для узгодженої командної роботи.
5.4)	Формувати комплексну стратегію захисту прав в Інтернеті, що збалансовує свободу вираження, недоторканність приватності, безпеку даних і права інтелектуальної власності.
6. Оцінювання	

(здатність оцінювати важливість матеріалу для конкретної цілі)	
6.1)	Визначати й тлумачити KPI дотримання прав онлайн: відповідність GDPR/DSA/NIS2, частка обґрунтованих скарг, час реакції на запити суб'єктів даних/правовласників.
6.2)	Оцінювати ефективність процедур «notice-and-action» та комунікацій із користувачами/регуляторами (повнота повідомлень, прозорість, своєчасність, доступність мовою користувача).
6.3)	Моніторити виконання строків і результативність проєктів комплаєнсу: видалення незаконного контенту, повідомлення про витоки даних, виконання рішень судів/органів нагляду.
7. Створення (творчість) *(здатність до створення нового культурного продукту, творчості в умовах багатовимірності та альтернативності сучасної культури)*	
7.1)	Розробляти тренінгові програми з цифрових прав (GDPR/DSA, кібергігієна, авторське право онлайн) з кейсами та чек-листами дій.
7.2)	Оптимізувати процедури реагування (наради/воркфлоу) на інциденти: notice-and-action, витоки даних, DMCA/UDRP, з чіткими ролями й таймлайнами.
7.3)	Організовувати делегування в комплаєнсі: модерація контенту, обробка запитів суб'єктів даних, взаємодія з регуляторами/правовласниками (SLA, шаблони відповідей).
7.4)	Формувати кросфункційні команди (юристи, IT-безпека, перекладачі) з урахуванням часових поясів, ескалацій і резервування критичних функцій.

3. Програма навчальної дисципліни

Тема 1. Поняття та зміст Інтернет-простору

Визначення Інтернет-простору як сукупності технічної інфраструктури, протоколів і соціально-правових відносин, що виникають у мережі. Архітектура мережі: DNS, IP-адресація, хостинг, CDN, платформи та посередники (access, caching, hosting, online platforms). Види цифрового контенту та даних: персональні, технічні, поведінкові, контент-дані та метадані. Екстериторіальність Інтернету та проблема юрисдикції: критерії зв'язку з правопорядком, місце заподіяння шкоди, місце надання послуги. Електронна ідентифікація і автентифікація, електронні докази: лог-файли, заголовки HTTP, фіксація веб-сторінок, збереження цифрового сліду. Ризики цифрового середовища: деанонімізація, порушення приватності, маніпуляції контентом, дезінформація, кіберінциденти. Базові підходи до правового врегулювання: саморегулювання платформ, державне регулювання, міжнародні стандарти, співрегулювання.

Тема 2. Суб'єкти та об'єкти правовідносин в мережі Інтернет

Суб'єкти: фізичні особи (користувачі, споживачі, правовласники), юридичні особи (платформи, хостинг-провайдери, ЗМІ, роботодавці), державні органи та регулятори, міжнародні організації і механізми врегулювання доменних спорів. Правовий статус посередників і межі їх відповідальності; умови «безпечної гавані» (notice-and-takedown, належна обачність). Об'єкти: персональні дані, облікові записи, доменні імена, торговельні марки, авторські та суміжні права, бази даних, контент, зображення та біометричні дані. Умови користування (ToS), політики платформ (Privacy, Cookies, Content, Ads) як джерела договірного регулювання. Виникнення, зміна і припинення онлайн-правовідносин; презумпції поведінки користувача; правосуб'єктність ботів та облікових записів, делегування доступів і відповідальності.

Тема 3. Міжнародно-правове регулювання Інтернету та захисту прав у цифровому середовищі

Мультиакторна модель управління Інтернетом: роль міжнародних організацій (Рада Європи, ЄС, ICANN, WIPO), галузевих конвенцій і регламентів. Колізійні питання і вибір права: юрисдикція за місцем заподіяння шкоди, місцем проживання відповідача/споживача, «спрямованість діяльності» в конкретну державу. Транскордонне виконання рішень і міжнародна правова допомога; приватне міжнародне право в доменних спорах і в онлайн-дифамації. Співвідношення міжнародних стандартів свободи вираження, приватності та безпеки; тест пропорційності обмежень у цифровому середовищі. Державні наглядові органи та коди співрегулювання; механізми оскарження дій платформ (внутрішні апеляції, медіація, арбітраж). Алгоритм транскордонного захисту прав: від фіксації доказів до звернення в іноземний регулятор/суд.

Тема 4. Інформаційна безпека та захист персональних даних

Категорії даних, їх чутливість і правові підстави обробки; інформована згода, легітимні інтереси, договірні зобов'язання, публічний інтерес. Права суб'єкта даних: доступ, виправлення, видалення, обмеження, заперечення, перенесення; реалізація прав у взаємодії з контролерами і процесорами. Політики приватності, cookie-банери, DPIA/оцінка впливу на захист даних. Управління інцидентами: виявлення, документування, повідомлення

регуляторів і суб'єктів; принципи «privacy by design/default». Технічні та організаційні заходи безпеки: шифрування, контроль доступу, журналювання, сегментація, мінімізація даних, псевдонімізація. Балансування прав: приватність vs. свобода вираження, доступ до публічної інформації, інтереси розслідувань і журналістики. Специфіка трансферів даних за кордон та вимоги до угод обробки.

Тема 5. Правове регулювання рекламних відносин в мережі Інтернет

Поняття онлайн-реклами та вимоги до маркування (ідентифікація реклами, комерційна комунікація, спонсорство, інфлюенсер-контент). Персоналізована реклама, профілювання і таргетинг; обмеження щодо чутливих категорій та неповнолітніх. Заборонені практики: недобросовісна, агресивна, оманлива реклама, прихована реклама і «нативка» без маркування. Обов'язки рекламодавця, виробника, розповсюджувача й платформи; due diligence і збереження доказів замовлення. Співвідношення з захистом даних: cookie-ідентифікатори, mobile-ID, ретаргетинг, відмови (opt-out) і згоди (opt-in). Порядок реагування на порушення: претензії, скарги до регуляторів/саморегулівних органів, видалення оголошень, блокування акаунтів; межі відповідальності платформи.

Тема 6. Захист авторського права в мережі Інтернет

Об'єкти авторського права та суміжних прав у цифровому середовищі: тексти, зображення, відео, музика, комп'ютерні програми, бази даних, контент, створений ШІ. Види онлайн-порушень: нелегальний хостинг/стрімінг, повторні заливки, обходи технічних засобів захисту, «запозичення» з соцмереж. Процедури notice-and-takedown/stay-down, контрсповіщення, повторні порушники; роль контент-ідентифікації. Винятки і обмеження: цитування, новинні цілі, пародія/карикатура/пастиш, освіта і наукові цілі; межі «fair use/деяких винятків» у крос-правопорядках. Розмір відповідальності та способи захисту: припинення порушення, відшкодування, компенсація, спростування; превентивні стратегії правовласників (водяні знаки, метадані, ліцензування). Співвідношення договірних умов платформи з імперативними нормами авторського права.

Тема 7. Цивільно-правова відповідальність в Інтернеті

Дифамація (наклеп, образа) та захист честі, гідності й ділової репутації онлайн; межі критики і допустимих оціночних суджень; тягар доказування і спростування. Порушення приватності: розголошення персональних даних, доксинг, незаконне використання зображення/імені, втручання у приватне життя. Шкода від інформації та сервісів: причинний зв'язок, передбачуваність шкоди, мінімізація збитків; немайнова шкода та критерії її оцінки. Способи захисту: вимога про видалення/спростування, блокування доступу, забезпечення доказів, судова заборона, відшкодування збитків/компенсація; альтернативні способи врегулювання спорів. Відповідальність користувача, автора, адміністратора ресурсу та платформи; умови звільнення посередника від відповідальності. Особливості доказування в цифрових спорах: електронні докази, експертиза, ланцюжок збереження.

Тема 8. Захист прав фізичних і юридичних осіб в мережі Інтернет

Алгоритм реагування на порушення: ідентифікація порушення → фіксація і консервація доказів (скрінінг, веб-архіви, хеш-суми) → звернення до платформи/хостера (формальні вимоги до notice) → регулятор/омбудсман → досудова претензія → суд/арбітраж. Репутаційні інструменти: «право на забуття/видалення», верифікація акаунтів, робота з

пошуковими індексами, запити суб'єкта даних. Доменні спори: підстави, елементи «конфузійної подібності», відсутність прав і добросовісних інтересів, недобросовісна реєстрація/використання; підготовка UDRP-скарги та захист від неї. Взаємодія з правоохоронними органами у випадку шахрайства, вимагання, порушень та кіберінцидентів; міжнародна допомога. Вибір процесуальної стратегії з урахуванням юрисдикції, швидкості, витрат і ефективності виконання; медіація та переговори з платформами.

Тема 9. Правові аспекти використання штучного інтелекту в Інтернеті

Класи ризику систем ШІ та їх правові наслідки; вимоги прозорості, верифікації і маркування ШІ-контенту (включно з deepfake). Авторське право і тренування моделей: дані для навчання, текст-і-дані майнінг, ліцензування датасетів, відтворення стилю; статус творів, створених ШІ, і розподіл прав. Відповідальність за ШІ-контент: дифамація, порушення приватності, маніпуляції і дезінформація; due diligence провайдерів і користувачів, оцінка ризиків, журналювання. Автоматизовані рішення: інформаційні обов'язки, право на пояснення/людське втручання, недискримінація та етичні вимоги. Комплаєнс-практики для організацій: політика використання ШІ, аудит моделей, управління даними і доступами, документування процесів, реагування на інциденти. Взаємодія з платформами і регуляторами щодо видалення ШІ-порушень, перевірки автентичності та відстежуваності контенту.

4. Структура вивчення навчальної дисципліни

4.1. Тематичний план навчальної дисципліни

№ теми	Назва теми	Кількість годин											
		Денна форма навчання						Заочна форма навчання					
		Усього	у тому числі					Усього	у тому числі				
			Лекції	Сем. (прак).	Лабор.	Ін. зав.	СРС		Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС
1.	Поняття та зміст Інтернет-простору	13	2	2	-	-	9	-	-	-	-	-	-
2.	Суб'єкти та об'єкти правовідносин в мережі Інтернет	13	2	2	-	-	9	-	-	-	-	-	-
3.	Міжнародно-правове регулювання Інтернету та захисту прав у цифровому середовищі	13	2	2	-	-	9	-	-	-	-	-	-
4.	Інформаційна безпека та захист персональних даних	13	2	2	-	-	9	-	-	-	-	-	-
5.	Правове регулювання рекламних відносин в мережі Інтернет	13	2	2	-	-	9	-	-	-	-	-	-
6.	Захист авторського права в мережі Інтернет	13	2	2	-	-	9	-	-	-	-	-	-

7.	Цивільно-правова відповідальність в Інтернеті	13	2	2	-	-	9	-	-	-	-	-	-
8.	Захист прав фізичних і юридичних осіб в мережі Інтернет	13	2	2	-	-	9	-	-	-	-	-	-
	Правові аспекти використання штучного інтелекту в Інтернеті	16	2	2	-		12						
Всього годин:		120	18	18	-	-	84		-	-	-	-	-

4.2. Аудиторні заняття

4.2.1. Аудиторні заняття (лекції, семінарські заняття) проводяться згідно з темами та обсягом годин, передбачених тематичним планом.
4.2.2. Плани лекцій з передбачених тематичним планом тем визначаються в підрозділі 1.2 навчально-методичних матеріалів з дисципліни.
4.2.3. Плани семінарських занять з передбачених тематичним планом тем, засоби поточного контролю знань та методичні рекомендації для підготовки до занять визначаються в підрозділі 1.3 навчально-методичних матеріалів з дисципліни.

4.3. Самостійна робота студентів

4.3.1. Самостійна робота студентів денної форми здобуття освіти включає завдання до окремих тем.
4.3.2. Завдання для самостійної роботи студентів та методичні рекомендації до їх виконання визначаються в підрозділі 1.4 навчально-методичних матеріалів з дисципліни.
4.3.3. Виконання індивідуальних завдань (у разі їх наявності) є обов'язковим для усіх студентів.
4.3.4. Тематика індивідуальних завдань та методичні рекомендації до їх виконання визначаються в підрозділі 1.5 навчально-методичних матеріалів з дисципліни.
4.3.5. Індивідуальні завдання виконуються в межах часу, визначеного для самостійної роботи студентів, та оцінюються частиною визначених в розділі 6 цієї програми кількості балів, виділених для самостійної роботи.

5. Методи навчання та контролю

Під час лекційних занять застосовуються:
1) традиційний усний виклад змісту теми;
2) створення проблемних ситуацій;
3) видача випереджальних завдань до лекції;
4) слайдова презентація;
5) експрес-опитування, діалог, дискусія;
6) методи активного слухання та методи зворотного зв'язку.
На семінарських та практичних заняттях застосовуються:
1) дискусійне обговорення проблемних питань;
2) вирішення ситуаційних завдань та кейсів із застосуванням сучасних інформаційних технологій;
3) методи активного слухання, диференціації та методи рефлексії.
Поточний контроль знань студентів з навчальної дисципліни проводиться у формах:
1) усне або письмове (у тому числі тестове) бліц-опитування студентів щодо засвоєння матеріалу попередньої лекції;
2) усне або письмове (у тому числі тестове) опитування на семінарських заняттях;

3) виконання практичних завдань із застосуванням сучасних інформаційних технологій;
4) захист підготовленої презентації.

Підсумковий семестровий контроль проводиться у формі заліку.

Структура залікового білета містить два теоретичних питання і 10 тестових завдань.

6. Схема нарахування балів

6.1. Нарахування балів студентам з навчальної дисципліни здійснюється відповідно до схеми, наведеної на рисунку 6.1.

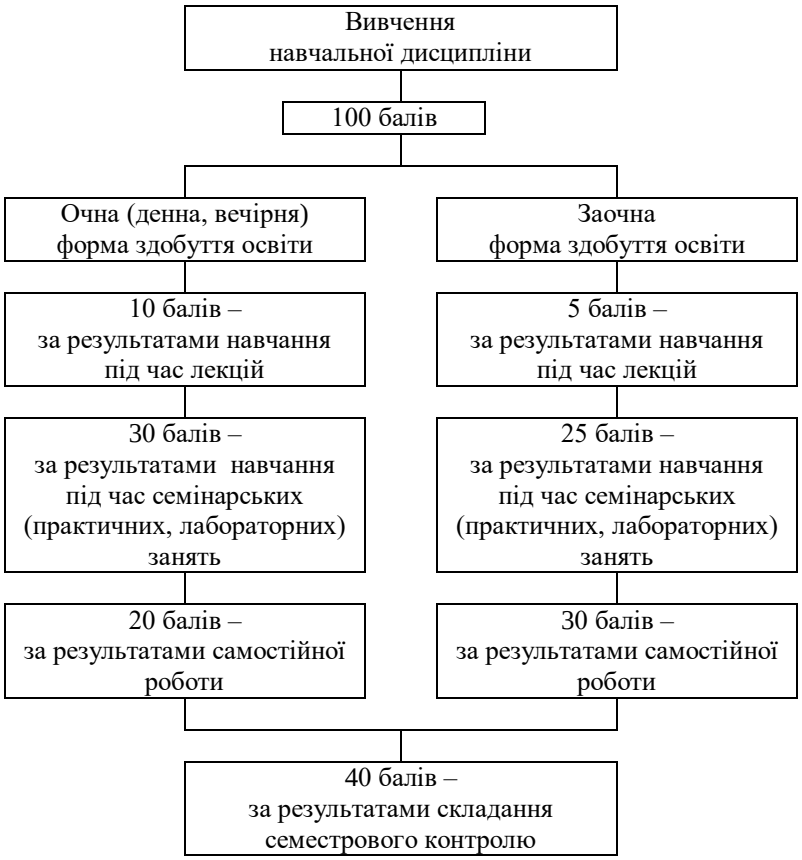

Рис. 6.1. Схема нарахування балів студентам за результатами навчання

6.2. Обсяг балів, здобутих студентом під час лекцій, семінарських занять, самостійної роботи студентів та виконання індивідуальних завдань, визначається в навчально-методичних матеріалах з цієї дисципліни.

7. Рекомендовані джерела

7.1. Основні джерела

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII (зі змін.). Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI (зі змін.). Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
4. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. Законодавство України.

URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.
5. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV (розд. III; ст. 277, 280–299). Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.
6. Convention on Cybercrime (Budapest Convention): ETS No.185, Council of Europe, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
7. Convention 108/108+ on data protection (CETS No.223 — amending protocol): Council of Europe. URL: https://www.coe.int/en/web/data-protection/convention108-and-protocol.
8. Regulation (EU) 2016/679 (General Data Protection Regulation — GDPR): EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
9. Regulation (EU) 2022/2065 (Digital Services Act — DSA): EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
10.Directive (EU) 2022/2555 (NIS2 Directive): EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
11.Regulation (EU) No 910/2014 (eIDAS): EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

7.2. Допоміжні джерела

1. EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR (актуальна версія). URL: https://edpb.europa.eu
2. EDPB–EDPS Joint Opinion on the Data Act (орієнтири щодо доступу/обміну даними). URL: https://edpb.europa.eu
3. EDPB. Guidelines 01/2022 on data subject rights – Right of access. URL: https://edpb.europa.eu
4. EDPB. Guidelines 9/2022 on personal data breach notification. URL: https://edpb.europa.eu
5. ENISA Threat Landscape (щорічний звіт, останні випуски). URL: https://www.enisa.europa.eu/topics/threats-and-trends/threat-landscape
6. ENISA. Handbook on Security of Personal Data Processing. URL: https://www.enisa.europa.eu
7. ENISA. Guidelines on Incident Reporting for DSPs & OES (NIS/NIS2). URL: https://www.enisa.europa.eu
8. OECD Privacy Guidelines (revised). URL: https://www.oecd.org/sti/privacy-consumer-policy/oecd-privacy-framework.htm
9. NIST Privacy Framework 1.0. URL: https://www.nist.gov/privacy-framework
10. NIST AI Risk Management Framework 1.0 (AI RMF). URL: https://www.nist.gov/itl/ai-risk-management-framework
11. Council of Europe. Guide on human rights for Internet users (CoE, 2014, оновл. матеріали). URL: https://www.coe.int
12. Council of Europe. Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries. URL: https://www.coe.int
13. OSCE. Freedom of Expression on the Internet: Guidebook (Representative on Freedom of the Media). URL: https://www.osce.org
14. WIPO. Copyright and the Internet: Selected Issues & Case Law Overviews. URL: https://www.wipo.int
15. WIPO Arbitration and Mediation Center. Domain Name Dispute Resources (UDRP case summaries). URL: https://www.wipo.int/amc/en/domains/
16. ICANN. UDRP Resources & Practice. URL: https://www.icann.org
17. European Commission. DSA Guidance & Q&A (впровадження, VLOPs/VLOSEs). URL: https://digital-strategy.ec.europa.eu
18. European Commission. eIDAS Toolbox & guidance (включно з eIDAS 2 оновленнями). URL: https://digital-strategy.ec.europa.eu
19. European Commission. Copyright in the Digital Single Market – implementation resources. URL: https://commission.europa.eu
20. European Union Agency for Fundamental Rights (FRA). Handbook on European Data Protection

Law (остання редакція). URL: https://fra.europa.eu
21. CJEU Case-law Digest on Data Protection & Digital Rights (офіц. огляди). URL: https://curia.europa.eu
22. UK ICO. Guidance on cookies, online tracking & children's code (Age Appropriate Design Code). URL: https://ico.org.uk
23. NOYB – European Center for Digital Rights (аналітика кейсів GDPR/DSA). URL: https://noyb.eu
24. IAPP (International Association of Privacy Professionals). DPO, DPIA, transfers toolkits. URL: https://iapp.org
25. EDRi (European Digital Rights). Analysis on platform regulation & fundamental rights online. URL: https://edri.org
26. CDT (Center for Democracy & Technology). Content moderation, transparency, due process online. URL: https://cdt.org
27. Access Now. Digital rights & platform accountability reports. URL: https://www.accessnow.org
28. Мінцифри України. Роз'яснення щодо персональних даних, кібергігієни, цифрових сервісів. URL: https://thedigital.gov.ua
29. Уповноважений ВРУ з прав людини. Рекомендації з питань захисту персональних даних. URL: https://ombudsman.gov.ua
30. Держспецзв'язку / CERT-UA. Попередження та поради з кібербезпеки. URL: https://cert.gov.ua / https://cip.gov.ua
31. Kuner C., Bygrave L.A., Docksey C. (eds.). The GDPR: A Commentary (OUP, 2020) – розширені тлумачення (як довідник до основних джерел).
32. Lynskey O. The Foundations of EU Data Protection Law (OUP).
33. Bygrave L.A. Data Privacy Law: An International Perspective (OUP).
34. Greenleaf G. Global Data Privacy Laws (щорічні огляди, SSRN).
35. Svantesson D. Private International Law and the Internet (Kluwer, 2021) – юрисдикція й колізії у мережі.

8. Інформаційні ресурси в мережі Інтернет

https://zakon.rada.gov.ua/	Інформаційно-пошукова система «Законодавство України»
http://mon.gov.ua	Веб-сайт Міністерства освіти і науки України
http://www.irbis-nbuv.gov.ua/	База даних Національної бібліотеки України імені В.І. Вернадського
http://gntb.gov.ua/ua/	Веб-сайт державної науково-технічної бібліотеки України
http://www.ounb.km.ua/	Веб-сайт Хмельницької обласної універсальної наукової бібліотеки
https://nrfu.org.ua/	Веб-сайт Національного фонду досліджень України
https://www.scopus.com	Наукометрична база даних Scopus
https://www.webofscience.com	Наукометрична база даних Web of Science
http://www.freefullpdf.com/	База даних наукових публікацій
https://www.base-search.net/	Bielefeld Academic Search Engine пошукова система академічних веб-ресурсів
https://doaj.org/	Онлайн-каталог журналів з відкритим доступом
www/ukrstat.gov.ua	Вебсайт Державної служби статистики України