ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ЗАТВЕРДЖЕНО
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
м.п.

НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ
з 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

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

ЗМІСТ

1. Структура вивчення навчальної дисципліни

1.1. Тематичний план навчальної дисципліни

№ теми	Назва теми	Кількість годин					
		Денна форма навчання					
		Усього	у тому числі				
			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

1.2. Лекції

№ з/п	Назва і план теми	К-сть годин
1.	**Поняття та зміст Інтернет-простору** 1.1. Визначення Інтернет-простору, архітектура мережі та базові принципи (відкритість, інтероперабельність, мережевий нейтралітет). 1.2. Юрисдикція та територіальність в онлайні: екстериторіальність норм, колізії права. 1.3. Права людини онлайн: свобода вираження, приватність, доступ до інформації. 1.4. Стандарти good governance в цифровому середовищі (прозорість, підзвітність платформ). 1.5. Цифровий контент і дані як об'єкти правовідносин. 1.6. Ключові ризики та виклики: дезінформація, кіберзагрози, порушення прав.	2
2.	**Суб'єкти та об'єкти правовідносин в мережі Інтернет** 2.1. Користувачі, провайдери доступу/хостингу, платформи, маркетплейси, агрегатори. 2.2. Об'єкти: акаунти, доменні імена, персональні дані, контент, метадані, цифрові активи. 2.3. Terms of Service/політики платформ як договори приєднання; публічна оферта онлайн. 2.4. Роль державних органів, регуляторів та DPA/Уповноваженого з прав людини/захисту даних. 2.5. Саморегулювання та coregulation (кодекси практик, галузеві стандарти). 2.6. Цифрові докази й лог-дані: збирання, збереження, допустимість.	2
3.	**Міжнародно-правове регулювання Інтернету та захисту прав** 3.1. Будапештська конвенція про кіберзлочинність та механізми співпраці (MLA, 24/7). 3.2. Конвенція 108/108+ Ради Європи та стандарти ЄСПЛ щодо приватності онлайн. 3.3. Право ЄС: GDPR, DSA, NIS2, eIDAS — сфера дії та ключові обов'язки суб'єктів. 3.4. Транснаціональна юрисдикція, виконання рішень, колізійні норми у справах онлайн. 3.5. Хмарні дані та міжнародні запити: CLOUD Act, двосторонні/багатосторонні інструменти. 3.6. Міжнародні організації (ICANN, WIPO) і політика доменних спорів (UDRP).	2
4.	**Інформаційна безпека та захист персональних даних** 4.1. Категорії персональних даних; спеціальні категорії та псевдонімізація/анонімізація. 4.2. Правові підстави обробки; згода, контракт, легітимний інтерес; принципи GDPR/ЗУ. 4.3. Права суб'єктів даних і обов'язки володільців/розпорядників; роль DPO. 4.4. DPIA, реєстри операцій, transfer impact assessment; транскордонні передачі. 4.5. Порушення безпеки даних: виявлення, 72-годинне повідомлення, повідомлення суб'єктам. 4.6. Технічні й організаційні заходи кіберзахисту (ENISA, ISO/IEC 27001).	2
5.	**Правове регулювання рекламних відносин онлайн**	2

	5.1. Вимоги до онлайн-реклами: ідентифікація реклами, заборона hidden ads, шахрайських практик. 5.2. Таргетинг/профілювання, cookies та ePrivacy; згода і налаштування користувача. 5.3. Інфлюенсер-маркетинг: маркування, відповідальність блогера й рекламодавця. 5.4. Обмеження щодо дитячої, медичної, фінансової реклами; недобросовісна конкуренція. 5.5. Контент-політики платформ і DSA: transparency/адресність реклами VLOP/VLOSE. 5.6. Механізми контролю і відповідальність: регулятори, саморегулювання (ICC Code).	
6.	**Захист авторського права в мережі Інтернет** 6.1. Об'єкти авторського права онлайн, правомочності, суміжні права, техзасоби захисту (TPM). 6.2. Notice-and-takedown: DMCA; обов'язки платформ за ст. 17 DSM-Директиви. 6.3. Винятки й обмеження: цитування, пародія, освітнє використання; fair use/fair dealing (порівняльно). 6.4. Ліцензування UGC-платформ; колективне управління правами; open-licenses (Creative Commons). 6.5. Доказування порушень онлайн, збереження доказів, форензіка; відповідальність посередників. 6.6. Практика WIPO/UDRP у доменних іменах, cybersquatting.	2
7.	**Цивільно-правова відповідальність в Інтернеті** 7.1. Делікти онлайн: наклеп, посягання на приватність, хейт-спіч, неправомірний контент. 7.2. Відповідальність провайдерів/хостингів: safe harbour, notice-and-action, DSA-обов'язки. 7.3. Юрисдикція, вибір права, виконання судових рішень; geo-blocking/removal orders. 7.4. Доменні спори й UDRP; засоби захисту права на знак/фірмове найменування. 7.5. Захист ділової репутації та немайнових прав у мережі; спростування й видалення. 7.6. Відшкодування шкоди (матеріальної/моральної), припинення порушень, інші способи захисту.	2
8.	**Захист прав фізичних і юридичних осіб в мережі Інтернет** 8.1. Досудові механізми: скарги платформам, медіація, Trusted Flaggers, ODR-механізми. 8.2. Адміністративний і судовий захист: органи, підвідомчість, докази, забезпечення позову. 8.3. Баланс між свободою вираження та захистом прав: стандарти ЄСПЛ (Delfi, Benedik). 8.4. Захист персональних даних: звернення до Уповноваженого/DPA, cross-border cases. 8.5. Кібербулінг, сексторшен, stalking: профілактика, фіксація, алгоритм дій потерпілого. 8.6. Ключові кейси CJEU (Google Spain, CNIL v Google), підходи до «права на забуття».	2
9.	**Правові аспекти використання штучного інтелекту в Інтернеті** 9.1. Ризики ШІ онлайн: дискримінація, дезінформація, deepfakes; базові	2

	принципи етики ШІ. 9.2. Регуляторні підходи ЄС (AI Act), Ради Європи та України; класифікація ризиків/обов'язки. 9.3. Персональні дані та тренування моделей: правові підстави, мінімізація, DPIA для ШІ-систем. 9.4. Авторське право і генерований контент: training data, text-and-data mining, атрибуція. 9.5. Відповідальність за контент, transparency та маркування ШІ-генерацій у соцмережах (DSA). 9.6. Алгоритмічна підзвітність і нагляд: аудит, логування, доступ до даних дослідникам.	
	Усього:	**18**

1.3. Семінарські заняття

Семінарське заняття 1
Тема 1. Поняття та зміст Інтернет-простору

Питання для усного опитування та дискусії

1. Визначення та архітектура Інтернет-простору: мережеві рівні й протоколи.
2. Принципи відкритості, інтероперабельності та мережевого нейтралітету.
3. Юрисдикція в онлайні: екстериторіальність та колізії права.
4. Права людини онлайн: свобода вираження, приватність, доступ до інформації.
5. Роль платформ у формуванні цифрового середовища: підзвітність та прозорість.
6. Категорії цифрового контенту та даних як об'єктів правовідносин.
7. Кіберризики та дезінформація: правові відповіді.
8. Баланс між інноваціями та регулюванням.

Аудиторна письмова робота

Виконання тестових завдань + короткий есе-відгук (до 200 слів) про межі юрисдикції держави в Інтернеті.

Методичні вказівки

Ключові терміни: Інтернет-простір, мережевий нейтралітет, юрисдикція, права людини онлайн, контент, дані.

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

Питання для усного опитування та дискусії

1. Користувачі, провайдери доступу, хостери, платформи: правовий статус.
2. Доменні імена, акаунти, персональні дані, цифрові активи як об'єкти права.
3. Terms of Service як договір приєднання: допустимість та справедливість умов.
4. Політики модерації контенту: межі та оскарження.
5. Роль регуляторів і DPA/Уповноваженого у сфері даних.

6. Саморегулювання та coregulation: кодекси практик.
7. Цифрові докази: лог-файли, скріншоти, ланцюг збереження.
8. Проблеми ідентифікації суб'єктів (анонімність/псевдонімність).

Аудиторна письмова робота

Кейс-аналіз: кваліфікувати ролі сторін у спорі «користувач—платформа—рекламодавець» та визначити застосовні договори/політики.

Методичні вказівки

Ключові терміни: провайдер, хостинг, платформа, домен, персональні дані, політика використання.

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

Питання для усного опитування та дискусії

1. Будапештська конвенція: сфера дії та інструменти співпраці.
2. Конвенція 108/108+: стандарти обробки персональних даних.
3. Ключові акти ЄС (огляд): GDPR, DSA, NIS2, eIDAS.
4. CLOUD Act і транскордонні запити до хмарних даних.
5. Механізми виконання іноземних рішень в «онлайн»-спорах.
6. Роль ICANN та WIPO/UDRP у доменних спорах.
7. Конфлікт законів і вибір юрисдикції.
8. Порівняння стандартів ЄСПЛ та CJEU щодо прав онлайн.

Аудиторна письмова робота

Скласти таблицю зіставлення: «Інструмент → що регулює → хто підпадає → механізми примусу/нагляду».

Методичні вказівки

Ключові терміни: MLA, 24/7 network, GDPR, DSA, NIS2, UDRP.
Порада: звертайте увагу на екстериторіальну дію деяких актів та на колізійні норми.

Семінарське заняття 4
Тема 4. Інформаційна безпека та захист персональних даних

Питання для усного опитування та дискусії

1. Правові підстави обробки даних: згода, договір, легітимний інтерес.
2. Права суб'єктів даних: доступ, виправлення, стирання, обмеження.
3. Обов'язки володільця/розпорядника: реєстри операцій, повідомлення про порушення.
4. DPO: коли потрібен та його роль.
5. DPIA та TIA: коли і як проводити.
6. Транскордонні передачі даних та гарантії.

7. Технічні й організаційні заходи безпеки: приклади.
8. Алгоритм реагування на інцидент (72 години).

Аудиторна письмова робота

Скласти «швидку інструкцію» (1 стор.) для малого сайту щодо дій у разі витоку даних.

Методичні вказівки

Ключові терміни: персональні дані, DPIA, DPO, data breach, TIA.

Семінарське заняття 5
Тема 5. Правове регулювання рекламних відносин в мережі Інтернет

Питання для усного опитування та дискусії

1. Вимоги до ідентифікації реклами онлайн.
2. Таргетована реклама: правові підстави, transparency, opt-in/opt-out.
3. Cookies/ePrivacy та зв'язок із згодою.
4. Інфлюенсер-маркетинг: маркування та відповідальність.
5. Обмеження для окремих категорій реклами (діти, медицина, фінанси).
6. Роль DSA для VLOPs: бібліотеки реклами, прозорість.
7. Недобросовісна конкуренція та агресивні практики.
8. Органи контролю та саморегулювання (ICC, IAB).

Аудиторна письмова робота

Розмітити як належить приклад рекламного поста інфлюенсера + вказати юридичні ризики.

Методичні вказівки

Ключові терміни: таргетинг, профілювання, cookies, disclosure, VLOP.

Семінарське заняття 6
Тема 6. Захист авторського права в мережі Інтернет

Питання для усного опитування та дискусії

1. Об'єкти, суб'єкти та майнові/немайнові права в онлайні.
2. Технічні засоби захисту (TPM) і їх правова охорона.
3. Notice-and-takedown (DMCA): процедура та контр-повідомлення.
4. Ст. 17 DSM: обов'язки платформ щодо UGC.
5. Винятки/обмеження: цитата, пародія, освіта; порівняння з fair use.
6. Ліцензування контенту, Creative Commons.
7. Форензіка: фіксація порушень, хеші, нотаріальне посвідчення скрінів.
8. Доменні спори та cybersquatting.

Аудиторна письмова робота

Заповнити шаблон DMCA/аналогічного запиту про видалення контенту (1 стор.) на підставі змодельованого кейсу.

Методичні вказівки

Ключові терміни: TPM, UGC, fair use, notice-and-takedown, колективне управління. Наголос: правильно окреслюйте обсяг прав і надавайте докази правовласності.

Семінарське заняття 7
Тема 7. Цивільно-правова відповідальність в Інтернеті

Питання для усного опитування та дискусії

1. Делікти онлайн: наклеп/образа, посягання на приватність, хейт-спіч.
2. Safe harbour та notice-and-action: межі і винятки.
3. Юрисдикція і вибір права: критерії прив'язки.
4. Забезпечувальні заходи: тимчасове блокування/видалення.
5. Захист ділової репутації та немайнових прав.
6. Розмір та види відшкодування шкоди.
7. Відповідальність за посилання/вбудовування (embedding).
8. Виконання іноземних рішень онлайн.

Аудиторна письмова робота

Схема-алгоритм визначення відповідальності платформи за контент користувача (1 стор., блок-схема).

Методичні вказівки

Ключові терміни: делікт, safe harbour, embedding, забезпечення позову. Порада: чітко відрізняйте роль «видобувача», «хостера» й «видавця».

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

Питання для усного опитування та дискусії

1. Досудові механізми: скарги платформі, Trusted Flaggers, ODR.
2. Адміністративні та судові шляхи захисту в Україні та ЄС.
3. Стандарти ЄСПЛ (Delfi, Benedik) щодо модерації/відповідальності.
4. «Право на забуття»: межі й винятки (Google Spain, CNIL v Google).
5. Кібербулінг/сексторшен: алгоритм дій потерпілого.
6. Захист персональних даних: звернення до Уповноваженого/DPA.
7. Докази в онлайні: допустимість, автентичність, цілісність.
8. Медіація та restorative practices в цифрових спорах.

Аудиторна письмова робота

Підготувати проєкт скарги платформі + короткий проєкт позовної заяви (структура та ключові вимоги).

Методичні вказівки

Ключові терміни: ODR, право на забуття, модерація, кібербулінг. Рекомендація: тренувати чіткість вимог і належність доказів (дата/час/URL/скрін).

Семінарське заняття 9

Тема 9. Правові аспекти використання штучного інтелекту в Інтернеті

Питання для усного опитування та дискусії

1. Ризики ШІ онлайн: дискримінація, deepfakes, дезінформація.
2. Підходи до регулювання ШІ: ЄС (AI Act), РЄ, Україна.
3. Персональні дані та тренування моделей: правові підстави, мінімізація, DPIA.
4. Авторське право і training data; TDM-винятки.
5. Маркування ШІ-контенту, transparency обов'язки платформ (DSA).
6. Відповідальність за збитки, спричинені системами ШІ.
7. Алгоритмічна підзвітність: аудит, логування, доступ дослідникам.
8. Етичні принципи (non-maleficence, fairness, accountability).

Аудиторна письмова робота

Скласти коротку політику використання ШІ-контенту для студентського медіа (1 стор.): маркування, перевірка, апеляції.

Методичні вказівки

Ключові терміни: AI Act, DPIA для ШІ, TDM, transparency, алгоритмічна підзвітність. Фокус: поєднання приватноправових і публічно-правових вимог, пропорційність заходів.

1.5. Індивідуальні завдання

Індивідуальні завдання з навчальної дисципліни «Захист прав в мережі Інтернет» не передбачені.

1.6. Підсумковий контроль

Підсумковий семестровий контроль проводиться у формі заліку.

1.6.1. Питання для підсумкового контролю

2. Поняття та структурні рівні Інтернет-простору; особливості юрисдикції онлайн.
3. Принцип мережевого нейтралітету: сутність і правові наслідки.
4. Основні суб'єкти інтернет-правовідносин та їх правовий статус (користувачі, провайдери, платформи).
5. Об'єкти правовідносин онлайн: контент, дані, доменні імена, акаунти.
6. Публічна оферта і «Terms of Service»: правова природа та умови дійсності.
7. Політика модерації контенту: межі, підстави, оскарження.
8. Права людини в цифровому середовищі: свобода вираження vs. приватність.
9. Докази в мережі Інтернет: фіксація, автентичність, допустимість.
10. Будапештська конвенція про кіберзлочинність: ключові механізми.
11. Конвенція 108/108+: принципи обробки персональних даних.
12. GDPR: правові підстави обробки та принципи мінімізації/цільового обмеження.
13. Права суб'єктів даних за GDPR/ЗУ «Про захист персональних даних».

14. Обов’язки контролера/процесора; реєстр операцій та повідомлення про інциденти.
15. DPO: критерії обов’язковості, роль і відповідальність.
16. Транскордонні передачі даних: SCCs, BCRs, адекватність.
17. DPIA та TIA: коли потрібні, що оцінюють, результати.
18. NIS2: категорії суб’єктів, заходи кіберстійкості, інцидент-репортинг.
19. eIDAS: електронна ідентифікація та довірчі послуги (кваліфікований підпис/печатка).
20. DSA: обов’язки онлайн-платформ і VLOPs щодо прозорості та модерації.
21. Взаємодія DSA з національним правом України: виклики імплементації.
22. CLOUD Act: доступ до даних, колізії з правом ЄС/України.
23. ICANN/UDRP: процедура вирішення доменних спорів.
24. Роль WIPO у доменних спорах та авторсько-правових медіаціях.
25. Суд ЄС, справа C-131/12 Google Spain: «право на забуття» — зміст і межі.
26. Суд ЄС, справа C-507/17 Google v CNIL: територіальні межі «права на забуття».
27. Суд ЄС, справа C-18/18 Glawischnig-Piesczek: глобальне видалення контенту.
28. ЄСПЛ, справа Delfi AS v. Estonia: відповідальність порталу за коментарі.
29. ЄСПЛ, справа Benedik v. Slovenia: IP-адреса і приватність.
30. ЄСПЛ, справа Roman Zakharov v. Russia: стандарти таємного стеження.
31. ENISA Threat Landscape: типові загрози та їх правові імплікації.
32. Згода за EDPB Guidelines 05/2020: критерії дійсності та відзивності.
33. Cookies/ePrivacy: коли потрібна згода, ролі CMP.
34. Рекламні онлайн-практики: таргетинг, профілювання, прозорість.
35. Обмеження реклами для вразливих груп (діти) та чутливих сфер.
36. Інфлюенсер-маркетинг: маркування комерційних комунікацій та відповідальність.
37. Авторське право онлайн: об’єкти, суб’єкти, майнові/немайнові права.
38. DMCA notice-and-takedown: процедура, контр-повідомлення.
39. Директива DSM, ст. 17: обов’язки платформ щодо UGC.
40. Винятки/обмеження (цитата, пародія, освіта) та їх застосування онлайн.
41. Ліцензії Creative Commons: види, умови, належне атрибутування.
42. Технічні засоби захисту (TPM) та відповідальність за їх обход.
43. Кібербулінг/доксинг/сексторшен: правові інструменти захисту.
44. Захист ділової репутації онлайн: склад правопорушення та способи захисту.
45. Цивільно-правова відповідальність провайдерів/платформ: safe harbour та винятки.
46. Юрисдикція та вибір права в інтернет-спорах: критерії прив’язки.
47. Забезпечувальні заходи: блокування, видалення, збереження доказів.
48. Виконання іноземних судових рішень у спорах з онлайн-елементом.
49. Доказування шкоди від онлайн-порушень та визначення розміру відшкодування.
50. Хостинг проти видавничої діяльності: різниця для відповідальності.
51. Цифрові докази: ланцюг збереження, хешування, протоколи нотаріального огляду.
52. Політики платформи vs. імперативні норми права: пріоритети та колізії.
53. Процедури скарг і апеляцій у платформах (DSA due process).
54. Роль національних регуляторів і Уповноваженого з захисту персональних даних.
55. ODR/медіація в цифрових спорах: переваги та обмеження.
56. Правові аспекти ШІ онлайн: класифікація ризиків, підзвітність, аудит.
57. Персональні дані й тренування моделей ШІ: правові підстави, мінімізація,

DPIA.
58. Авторське право та training data/генеративний контент: TDM-винятки, атрибуція.
59. Маркування та прозорість ШІ-контенту: вимоги платформ і користувачів.
60. Етичні рамки ШІ: недискримінація, пояснюваність, справедливість.
61. Алгоритм дій організації при витоку даних/кібератаці: повідомлення, локалізація, взаємодія з DPA/Кіберполіцією.

1.6.2. Приклад залікового білета

1. 1. Підходи до визначення правового режиму Інтернет-простору та цифрових прав (публічно-правовий, приватно-правовий, змішаний; екстериторіальність і юрисдикція).
2. Оцінка впливу на захист даних (DPIA): поняття, мета, ключові етапи та результати.
3. Тести. Оберіть одну правильну відповідь:
3.1. Який міжнародний інструмент є базовим для протидії кіберзлочинності?
а) Конвенція Ради Європи 108+;
б) Будапештська конвенція ETS №185;
в) Директива (ЄС) 2019/790 (DSM);
г) Регламент (ЄС) № 910/2014 (eIDAS).
3.2. Яка справа Суду ЄС закріпила «право на забуття» в пошукових системах?
а) C-18/18 Glawischnig-Piesczek;
б) C-507/17 Google v CNIL;
в) C-131/12 Google Spain;
г) C-362/14 Schrems I.
3.3. Хто є «контролером» персональних даних у розумінні GDPR?
а) Будь-який суб’єкт, що обробляє дані за дорученням;
б) Суб’єкт, який визначає цілі та засоби обробки;
в) Фізична особа — власник акаунта;
г) Будь-яка державна установа.
3.4. Транскордонна передача даних з ЄС до третьої країни можлива без додаткових гарантій, якщо:
а) Дані були анонімізовані;
б) Є рішення про належний рівень захисту (adequacy);
в) Є усна згода суб’єкта;
г) Передача здійснюється через e-mail.
3.5. NIS2 насамперед встановлює:
а) Авторсько-правові винятки для інтернет-платформ;
б) Вимоги кіберстійкості та інцидент-репортингу для секторів/суб’єктів;
в) Процедуру notice-and-takedown;
г) Правила кваліфікованого е-підпису.

2. Схема нарахування балів

2.1. Нарахування балів студентам з навчальної дисципліни здійснюється відповідно до схеми, зображеної на рис. 2.1.

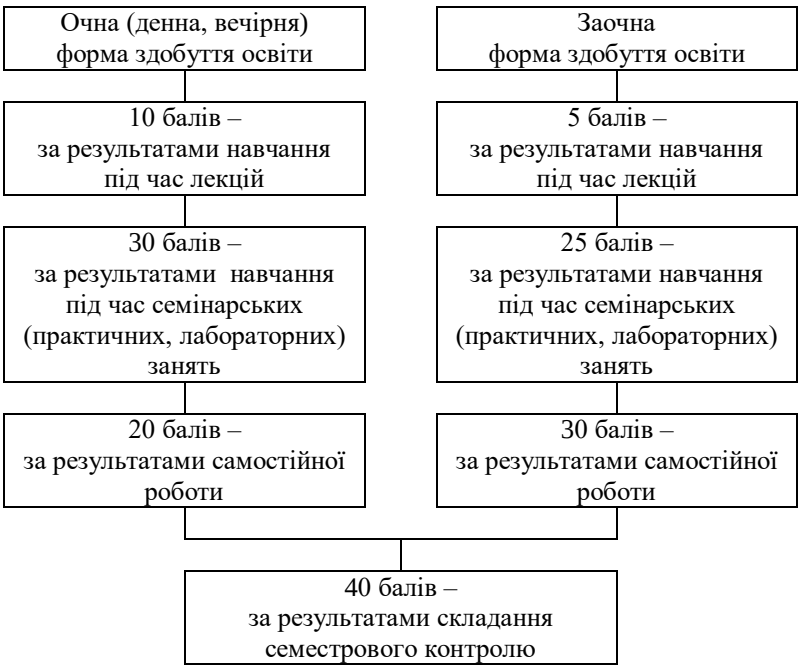

Рис. 2.1. Схема нарахування балів студентам за результатами навчання

2.2. Обсяг балів, здобутих студентом під час лекцій з навчальної дисципліни «*Захист прав в мережі Інтернет в Україні та ЄС*», обчислюється у пропорційному співвідношенні кількості відвіданих лекцій і кількості лекцій, передбачених навчальним планом, і визначається згідно з Положенням про організацію освітнього процесу в Хмельницькому університеті управління та права імені Леоніда Юзькова.

З навчальної дисципліни «*Захист прав в мережі Інтернет в Україні та ЄС*» передбачено проведення 9 лекційних занять за денною формою здобуття освіти. Отже, студент може набрати під час лекцій таку кількість балів:

№ з/п	Форма здобуття освіти	Кількість лекцій за планом	Кількість відвіданих лекцій							
			1	2	3	4	5	6	7	9
1.	Денна	8	1,25	2,50	3,75	5,00	6,25	7,50	8,75	10,00

2.3. З навчальної дисципліни «*Захист прав в мережі Інтернет в Україні та ЄС*» передбачено проведення 9 семінарських занять за денною формою здобуття освіти. За результатами семінарського (практичного) заняття кожному студенту до відповідного документа обліку успішності виставляється кількість балів від 0 до 5 числом, кратним 0,5, яку він отримав протягом заняття. Критерії поточного оцінювання знань студентів наведені у Положенні про організацію освітнього процесу в Хмельницькому університеті управління та права імені Леоніда Юзькова.

2.4. Перерозподіл кількості балів в межах максимально можливої кількості балів за самостійну роботу студентів наведено в таблиці:

№ з/п	8 тем	Номер теми								Усього балів
		1.	2.	3.	4.	5.	6.	7.	8.	
1.	Максимальна кількість балів за самостійну роботу	2	3	3	3	3	2	2	2	20

	Усього балів		20

2.5. Підсумовування балів за результатами вивчення навчальної дисципліни здійснюється на підставі результатів поточного контролю.

Семестрова оцінка із залікової навчальної дисципліни (за умови, що здобувачем за поточний контроль накопичено 36 і більше балів) обчислюється за формулою:

$$\sum C = Б_{пк} \cdot 100 \div 60,$$

де $\sum C$ – загальна кількість балів;

$Б_{пк}$ – кількість балів, отриманих за поточний контроль.

Студент, який бажає отримати підсумковий бал вищий за розрахунковий (відповідно до зазначеної формули) із залікової навчальної дисципліни, має право скласти семестровий залік. У такому разі семестрова оцінка із залікової навчальної дисципліни обчислюється шляхом додавання накопичених здобувачем освіти балів з поточного та семестрового контролю. У разі отримання здобувачем вищої освіти на заліку підсумкової оцінки, що є нижчою ніж розрахункова, йому виставляється розрахункова оцінка.

За семестровий контроль, що проводиться у формі заліку з навчальної дисципліни «*Захист прав в мережі Інтернет в Україні та ЄС*», студент може максимально одержати 40 балів. Шкала визначення кількості балів та критерії оцінювання знань студентів за результатами семестрового контролю, подана у Положенні про організацію освітнього процесу в Хмельницькому університеті управління та права імені Леоніда Юзькова.

Перерозподіл балів, в межах максимально можливого одержання їх кількості за надані студентами відповіді, наведений в таблиці:

№ з/п	Алгоритм нарахування балів	Номер питань (завдання) залікового білета			Разом балів
		1	2	3 (тести)	
1.	Максимальна кількість балів відповідь на кожне питання залікового білета	10	10	20	40

3. Рекомендовані джерела

3.1. 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.
12. ICANN. Uniform Domain-Name Dispute-Resolution Policy (UDRP): ICANN, 1999. URL: https://www.icann.org/resources/pages/policy-2012-02-25-en.

3.2. 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.

4. 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