



**Вищий навчальний заклад
«НАЦІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ»
Юридичний факультет
Кафедра теорії та історії держави і права**

ЗАТВЕРДЖЕНО

Декан юридичного факультету



Наталія ВЕСЕЛОВСЬКА

РОБОЧА ПРОГРАМА

ІНФОРМАЦІЙНЕ ПРАВО

(назва навчальної дисципліни)

підготовки	<u>першого (бакалаврського) рівня вищої освіти</u> (назва рівня вищої освіти)
галузі знань	<u>D «Бізнес, адміністрування та право»</u> (шифр і назва галузі знань)
спеціальності	<u>D8 «Право»</u> (код і найменування спеціальності)
освітньо-професійної програми	<u>«Право»</u> (назва освітньо-професійної програми)
тип дисципліни	<u>вибіркова навчальна дисципліна</u>

2025 рік

ПОГОДЖЕНО:

Гарант освітньої програми



Ірина КОЗАКОВА

РЕКОМЕНДОВАНО:

Кафедрою теорії та історії держави і права
протокол № 1
від «29» серпня 2025 року

Завідувач кафедри



Антон ЧУБ

Укладач: *Чернявська Богдана Вадимівна*, доктор філософії з права, доцент кафедри теорії та історії держави і права.

1. Опис навчальної дисципліни

Мова навчання: українська

Статус дисципліни: вибіркова

Передумови вивчення навчальної дисципліни: вивчення навчальної дисципліни «Інформаційне право» доцільне після оволодіння здобувачами базовими знаннями з теорії держави і права (в частині системи права, правовідносин та механізму правового регулювання); конституційного права України (щодо свободи слова, права на інформацію, приватність та правового статусу медіа); загальної частини цивільного права України (в частині особистих немайнових прав, інформації як об'єкта цивільних прав та правочинів); логіки та критичного мислення щодо здатності аналізувати інформаційні потоки, виявляти дезінформацію та будувати несуперечливу юридичну аргументацію; інформаційних технологій в юридичній діяльності (щодо практичних навичок роботи з електронними реєстрами, базами даних та хмарними сервісами); а також юридичної деонтології щодо засвоєння засад академічної доброчесності, професійної таємниці та інформаційної етики правника.

Предметом вивчення навчальної дисципліни «Інформаційне право» є суспільні відносини, що виникають у процесі виробництва, збирання, обробки, зберігання, захисту, поширення та використання інформації; правовий режим доступу до публічної інформації та захисту персональних даних; правове регулювання діяльності медіа, інтернет-платформ та електронної комерції; нормативні засади забезпечення кібербезпеки та інформаційної безпеки держави, особи і суспільства; а також юридичні інститути та режими обігу інформації з обмеженим доступом, кіберзлочинність та правові основи застосування штучного інтелекту в Україні й умовах європейської інтеграції.

Інформаційний обсяг навчальної дисципліни. На вивчення навчальної дисципліни відводиться **150** годин (5 кредитів ECTS).

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Інформаційне право» є формування у студентів цілісної системи знань про правове регулювання інформаційних відносин, засвоєння юридичних стандартів доступу до інформації та захисту персональних даних, а також оволодіння механізмами забезпечення кібербезпеки й захисту національного інформаційного простору в умовах цифрової трансформації суспільства.

Основними завданнями навчальної дисципліни «Інформаційне право» є ознайомлення здобувачів із теоретичними засадами інформаційного суспільства, еволюцією та джерелами інформаційного законодавства; аналізування правових режимів різних видів інформації (відкритої, конфіденційної, таємної, службової) та статусу суб'єктів інформаційних правовідносин; дослідження механізмів реалізації права на доступ до публічної інформації та інституту захисту персональних даних; вивчення правових стандартів функціонування цифрових медіа, електронного урядування, криптографічного захисту та нормативного забезпечення кібербезпеки; а також відпрацювання навичок складання інформаційних запитів, локальних актів підприємств щодо захисту комерційної таємниці, правової оцінки фактів кіберзлочинів та кваліфікації правопорушень в інформаційній сфері.

3. Компетентності та заплановані результати навчання

Дисципліна «Інформаційне право» забезпечує набуття таких компетентностей і програмних результатів:

Загальні компетентності (ЗК):

ЗК01	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК02	Здатність застосовувати знання у практичних ситуаціях.
ЗК03	Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК11	Здатність реалізувати свої права і обов'язки як члена суспільства; усвідомлення цінності громадянського (вільного демократичного) суспільства та необхідності його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
ЗК16	Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

Спеціальні (фахові) компетентності (СК):

СК07	Здатність застосовувати норми та інститути права, щонайменше з таких галузей, як: конституційне право, адміністративне право і адміністративне процесуальне право, цивільне і цивільне процесуальне право, трудове право, кримінальне і кримінальне процесуальне право.
СК09	Здатність використовувати бази даних органів юстиції та інформаційні технології необхідні під час здійснення юридичної діяльності.
СК10	Здатність використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин.
СК11	Здатність визначати належні та прийнятні для юридичного аналізу факти.
СК12	Здатність аналізувати правові проблеми та обґрунтовувати правові позиції.
СК14	Здатність до консультування з правових питань, зокрема, можливих способів захисту прав та інтересів клієнтів, відповідно до вимог професійної етики, належного дотримання норм щодо нерозголошення персональних даних та конфіденційної інформації.

Програмні результати навчання (ПРН):

ПРН05	Давати короткий правовий висновок щодо окремих фактичних обставин з достатньою обґрунтованістю.
ПРН06	Оцінювати недоліки і переваги певних правових аргументів, аналізуючи відому проблему.
ПРН15	Вільно використовувати для правничої діяльності доступні інформаційні технології і бази даних.
ПРН18	Застосовувати в професійній діяльності основні сучасні правові доктрини, цінності та принципи функціонування національної правової системи.
ПРН20	Виокремлювати і аналізувати юридично значущі факти і робити обґрунтовані правові висновки.
ПРН22	Надавати консультації щодо можливих способів захисту прав та інтересів клієнтів у різних правових ситуаціях.

4. Структура навчальної дисципліни

Назви тем	Обсяг у годинах											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	сем.	пз	лаб.	с. р		л	сем.	пз	лаб.	с. р
Тема 1. Теоретико-правові засади інформаційного права	12	2	4			6	15	1	2			12
Тема 2. Право на доступ до публічної інформації	14	2	4			8	15	1	2			12
Тема 3. Правовий режим інформації з обмеженим доступом	14	2	4			8	15	1	2			12
Тема 4. Правовий захист персональних даних	14	2	4			8	15	1	2			12
Тема 5. Правове регулювання діяльності медіа та Інтернету	16	4	4			8	15	1	2			12
Тема 6. Правовий режим електронного урядування та цифрових послуг	16	4	4			8	15	1	2			12
Тема 7. Кібербезпека та захист критичної інформаційної інфраструктури	14	2	4			8	14	1	1			12
Тема 8. Правові аспекти штучного інтелекту та новітніх технологій	14	2	4			8	14	1	1			12
Тема 9. Інформаційна безпека держави	18	4	6			8	16	1	1			14
Тема 10. Юридична відповідальність в інформаційній сфері	18	4	6			8	16	1	1			14
Усього годин	150	28	44	0	0	78	150	10	16	0	0	124

5. Зміст програми навчальної дисципліни

Тема 1. Теоретико-правові засади інформаційного права

Предмет, методи та система інформаційного права. Інформаційні правовідносини. Поняття та юридичні властивості інформації як об'єкта правового регулювання. Принципи інформаційного права: свобода інформації, відкритість та захищеність. Джерела інформаційного права.

Тема 2. Право на доступ до публічної інформації

Конституційне право на інформацію та механізми його реалізації. Правовий режим публічної інформації: поняття та види. Обов'язки розпорядників інформації та процедура опрацювання запитів. Обмеження доступу до інформації. Відповідальність за порушення законодавства про доступ до публічної інформації.

Тема 3. Правовий режим інформації з обмеженим доступом

Класифікація інформації з обмеженим доступом: конфіденційна, таємна, службова. Правове регулювання захисту державної таємниці. Правове регулювання комерційної таємниці. Лікарська, банківська й адвокатська таємниці як спеціальні інформаційні режими. Правові підстави та порядок відкриття інформації.

Тема 4. Правовий захист персональних даних

Поняття персональних даних та правове регулювання їх обробки. Права суб'єктів персональних даних у цифрову епоху. Вимоги до збирання, зберігання та транскордонної передачі даних. Роль Уповноваженого Верховної Ради з прав людини у сфері захисту персональних даних. Вплив Загального регламенту про захист даних (GDPR) на законодавство України.

Тема 5. Правове регулювання діяльності медіа та Інтернету

Суб'єкти медіасфери: правовий статус друкованих, онлайн-медіа та телерадіомовлення. Правові засади діяльності журналістів. Юридична відповідальність медіа за поширення недостовірної інформації. Правове регулювання українського сегмента мережі Інтернет. Соціальні мережі та платформи спільного доступу: правові виклики регулювання.

Тема 6. Правовий режим електронного урядування та цифрових послуг

Правові основи функціонування системи «Електронний уряд» та порталу «Дія». Юридичний статус електронних довірчих послуг та електронного підпису. Правовий режим державних інформаційних ресурсів та реєстрів. Надання адміністративних послуг в електронній формі. Цифрова безбар'єрність та правові гарантії доступу до цифрових технологій.

Тема 7. Кібербезпека та захист критичної інформаційної інфраструктури

Правові засади державної політики у сфері кібербезпеки. Суб'єкти забезпечення кібербезпеки. Правовий режим об'єктів критичної інформаційної інфраструктури. Юридичні механізми протидії кіберзлочинності та кібертероризму. Міжнародне співробітництво у сфері кіберзахисту.

Тема 8. Правові аспекти штучного інтелекту та новітніх технологій

Правовий статус штучного інтелекту: проблеми суб'єктності та відповідальності. Юридичні аспекти використання технології Blockchain та смарт-контрактів. Правове регулювання великих даних (Big Data) та хмарних технологій. Етичні та правові межі алгоритмічного прийняття рішень. Адаптація законодавства України до AI Act Європейського Союзу.

Тема 9. Інформаційна безпека держави

Правові засади захисту інформаційного суверенітету України. Протидія дезінформації та маніпулятивним технологіям: правові механізми. Правовий режим інформації в умовах воєнного стану. Юридичні засади діяльності Центрів протидії дезінформації. Відповідальність за злочини проти основ національної безпеки в інформаційній сфері.

Тема 10. Юридична відповідальність в інформаційній сфері

Цивільно-правовий захист честі, гідності та ділової репутації. Адміністративна відповідальність за порушення в сфері зв'язку та інформації. Кримінальна відповідальність за кіберзлочини та порушення недоторканності приватного життя. Процесуальні особливості використання електронних доказів у суді. Медіація у вирішенні інформаційних спорів.

6. Теми лекцій

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Тема 1. Теоретико-правові засади інформаційного права	2	1
2	Тема 2. Право на доступ до публічної інформації	2	1
3	Тема 3. Правовий режим інформації з обмеженим доступом	2	1
4	Тема 4. Правовий захист персональних даних	2	1
5	Тема 5. Правове регулювання діяльності медіа та Інтернету	4	1
6	Тема 6. Правовий режим електронного урядування та цифрових послуг	4	1
7	Тема 7. Кібербезпека та захист критичної інформаційної інфраструктури	2	1
8	Тема 8. Правові аспекти штучного інтелекту та новітніх технологій	2	1
9	Тема 9. Інформаційна безпека держави	4	1
10	Тема 10. Юридична відповідальність в інформаційній сфері	4	1
Усього годин		28	10

7. Теми семінарських занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Тема 1. Теоретико-правові засади інформаційного права	4	2
2	Тема 2. Право на доступ до публічної інформації	4	2
3	Тема 3. Правовий режим інформації з обмеженим доступом	4	2
4	Тема 4. Правовий захист персональних даних	4	2
5	Тема 5. Правове регулювання діяльності медіа та Інтернету	4	2
6	Тема 6. Правовий режим електронного урядування та цифрових послуг	4	2
7	Тема 7. Кібербезпека та захист критичної інформаційної інфраструктури	4	1
8	Тема 8. Правові аспекти штучного інтелекту та новітніх технологій	4	1
9	Тема 9. Інформаційна безпека держави	6	1
10	Тема 10. Юридична відповідальність в інформаційній сфері	6	1
Усього годин		44	16

8. План семінарських занять

Тема 1. Теоретико-правові засади інформаційного права

Мета: системне засвоєння знань про предмет, методи та систему інформаційного права, сутність інформаційних правовідносин, а також юридичні властивості інформації як об'єкта правового регулювання.

Питання для обговорення:

1. Як визначається предмет, специфіка методів та внутрішня структура системи інформаційного права?
2. З яких елементів складаються інформаційні правовідносини та які особливості їхнього суб'єктного складу?
3. Які специфічні юридичні властивості має інформація як особливий об'єкт правового регулювання?
4. Як реалізуються та співвідносяться базові принципи права: свобода, відкритість та захищеність інформації?
5. Які особливості має система джерел вітчизняного інформаційного права та її кодифікація?

Тема 2. Право на доступ до публічної інформації

Мета: ґрунтовне вивчення конституційного права на інформацію, правового режиму публічних відомостей, обов'язків розпорядників та підстав для обмеження доступу.

Питання для обговорення:

1. Які конституційні механізми забезпечують повну реалізацію права особи на інформацію?
2. Як визначається правова сутність та які існують види публічної інформації в Україні?
3. Які імперативні обов'язки розпорядників публічної інформації та загальна процедура опрацювання запитів?
4. На основі яких законодавчих критеріїв здійснюється правомірне обмеження доступу до інформації?
5. Які види юридичної відповідальності передбачено за порушення законодавства про доступ до публічної інформації?

Тема 3. Правовий режим інформації з обмеженим доступом

Мета: комплексне опанування знань про класифікацію та специфічні правові режими конфіденційної, таємної та службової інформації, а також умов розкриття таких відомостей.

Питання для обговорення:

1. На основі яких ознак здійснюється класифікація інформації з обмеженим доступом на конфіденційну, таємну та службову?
2. Які нормативно-правові засади та інституційні механізми забезпечують охорону державної таємниці?
3. Як реалізується правове регулювання охорони комерційної таємниці підприємства?
4. У чому полягає специфіка та особливості функціонування режимів лікарської, банківської й адвокатської таємниць?
5. Які існують імперативні правові підстави та загальний процесуальний порядок законного відкриття інформації?

Тема 4. Правовий захист персональних даних

Мета: детальний аналіз правового регулювання обробки персональних даних, вимог до їх транскордонної передачі та специфіки імплементації стандартів GDPR.

Питання для обговорення:

1. Як визначається поняття персональних даних та які загальні вимоги встановлено до їхньої законної обробки?
2. Які права мають суб'єкти персональних даних у сучасну цифрову епоху?

3. Які нормативні вимоги висуваються до процесів збирання, зберігання та трансграничної передачі даних?
4. Яку роль відіграє Уповноважений Верховної Ради з прав людини у сфері нагляду та захисту персональних даних?
5. Як саме Загальний регламент про захист даних (GDPR) Європейського Союзу впливає на законодавство України?

Тема 5. Правове регулювання діяльності медіа та Інтернету

Мета: критичне переосмислення правового статусу суб'єктів медіасфери, юридичних засад діяльності журналістів та правових викликів регулювання платформ спільного доступу.

Питання для обговорення:

1. Які особливості має правовий статус друкованих, онлайн-медіа та телерадіомовлення за чинним законодавством?
2. Які нормативно-правові засади, права та професійні гарантії визначають діяльність журналістів?
3. За якими правилами настає юридична відповідальність медіа за поширення недостовірної інформації?
4. Як побудовано правове регулювання та юрисдикція в українському сегменті мережі Інтернет?
5. Які сучасні правові виклики виникають під час спроб регулювання соціальних мереж та платформ спільного доступу?

Тема 6. Правовий режим електронного урядування та цифрових послуг

Мета: наукове дослідження основ функціонування системи «Електронний уряд», правового статусу цифрових довірчих послуг та державних інформаційних ресурсів.

Питання для обговорення:

1. Які правові основи лежать в основі функціонування системи «Електронний уряд» та вебпорталу «Дія»?
2. Який юридичний статус мають електронні довірчі послуги, кваліфікований електронний підпис та печатка?
3. Які особливості визначають правовий режим функціонування державних інформаційних ресурсів та реєстрів?
4. Як здійснюється нормативно-правове регулювання надання адміністративних послуг в електронній формі?
5. Які правові гарантії доступу до цифрових технологій містить концепція цифрової безбар'єрності?

Тема 7. Кібербезпека та захист критичної інформаційної інфраструктури

Мета: теоретичне осмислення засад державної політики у сфері кібербезпеки, правового режиму об'єктів критичної інфраструктури та механізмів протидії кіберзлочинності.

Питання для обговорення:

1. Які правові засади та стратегічні пріоритети визначають державну політику України у сфері кібербезпеки?
2. Які суб'єкти забезпечують кібербезпеку держави та як розподілена їхня компетенція?
3. Який правовий режим встановлено для об'єктів критичної інформаційної інфраструктури?
4. Які юридичні механізми застосовуються для протидії кіберзлочинності та кібертероризму?
5. Як побудовано міжнародне співробітництво та взаємодія України у сфері глобального кіберзахисту?

Тема 8. Правові аспекти штучного інтелекту та новітніх технологій

Мета: доктринальне вивчення проблем суб'єктності штучного інтелекту, правового режиму смарт-контрактів, великих даних та адаптації норм до AI Act Європейського Союзу.

Питання для обговорення:

1. Які проблеми суб'єктності та деліктоздатності штучного інтелекту виникають у сучасному правовому дискурсі?
2. За якими правилами визначається цивільно-правова відповідальність за шкоду, заподіяну системами штучного інтелекту?
3. Які юридичні аспекти супроводжують практичне використання технології Blockchain та смарт-контрактів?
4. Як будується правове регулювання обігу великих даних і використання хмарних технологій?
5. Які етичні та правові межі встановлено для алгоритмічного автоматизованого прийняття управлінських рішень?
6. Як саме відбувається адаптація законодавства України до Регламенту ЄС про штучний інтелект?
7. Які ризики для авторського права створює використання генеративного штучного інтелекту під час створення об'єктів?

Тема 9. Інформаційна безпека держави

Мета: фундаментальне осмислення правових засад захисту інформаційного суверенітету, механізмів протидії дезінформації та особливостей правового режиму в умовах воєнного стану.

Питання для обговорення:

1. Які правові засади та інструменти забезпечують захист інформаційного суверенітету України?
2. Які правові механізми застосовуються для ефективної протидії дезінформації та маніпулятивним технологіям?
3. Які особливості та обмеження прав має правовий режим інформації в умовах дії воєнного стану?
4. Які юридичні засади та повноваження визначають діяльність Центрів протидії дезінформації?
5. Яка кримінальна відповідальність передбачена за злочини проти основ національної безпеки в інформаційній сфері?

Тема 10. Юридична відповідальність в інформаційній сфері

Мета: аксіологічне розуміння цивільних, адміністративних та кримінальних деліктів в інформаційному просторі, специфіки електронних доказів та медіації в інформаційних спорах.

Питання для обговорення:

1. Як здійснюється цивільно-правовий захист честі, гідності та ділової репутації особи в цифровому середовищі?
2. За які правопорушення у сфері зв'язку та інформації передбачена адміністративна відповідальність?
3. Які діяння кваліфікуються як кримінальні кіберзлочини та порушення недоторканності приватного життя?
4. Які процесуальні особливості та правила збирання, подання й оцінки електронних доказів у суді?
5. Як інститут медіації може використовуватися під час вирішення складних інформаційних спорів?
6. Як розмежовуються поняття «оціночне судження» та «фактичне твердження» під час розгляду справ про дифамацію?
7. Які особливості має відшкодування моральної шкоди, заподіяної поширенням недостовірної інформації в мережі?

9. Теми практичних занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Не передбачено навчальним планом	-	-
Усього годин			

10. Теми лабораторних занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Не передбачено навчальним планом	-	-
Усього годин			

11. Теми самостійної роботи

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Тема 1. Теоретико-правові засади інформаційного права	6	12
2	Тема 2. Право на доступ до публічної інформації	8	12
3	Тема 3. Правовий режим інформації з обмеженим доступом	8	12
4	Тема 4. Правовий захист персональних даних	8	12
5	Тема 5. Правове регулювання діяльності медіа та Інтернету	8	12
6	Тема 6. Правовий режим електронного урядування та цифрових послуг	8	12
7	Тема 7. Кібербезпека та захист критичної інформаційної інфраструктури	8	12
8	Тема 8. Правові аспекти штучного інтелекту та новітніх технологій	8	12
9	Тема 9. Інформаційна безпека держави	8	14
10	Тема 10. Юридична відповідальність в інформаційній сфері	8	14
Усього годин		78	124

12. Завдання для самостійної роботи

Самостійна робота – форма організації освітнього процесу, за якої здобувач вищої освіти опановує навчальну дисципліну в час, вільний від навчальних занять, під методичним керівництвом викладача, але без його безпосередньої участі. Ключовим завданням позааудиторного вивчення дисципліни «Інформаційне право» є повноцінне охоплення затвердженої програми курсу, розширення професійних компетентностей, стимулювання пізнавальної автономії та формування вміння самостійно опрацьовувати теоретичний і прикладний масив знань. Особлива увага приділяється детальному дослідженню нормативно-правової бази інформаційного суспільства, аналізу інституту захисту персональних даних та відкритих реєстрів, правовому регулюванню цифрових медіа, систем штучного інтелекту й електронного урядування. Разом із цим, діяльність спрямовується на засвоєння стратегій протидії кіберзагрозам, забезпечення державної безпеки в інформаційній сфері, а також на неухильне дотримання правил академічної доброчесності та недопущення проявів плагіату.

Самостійна робота здійснюється у формі: виконання поточних домашніх завдань; написання аналітичних звітів, есе чи рефератів із обов'язковою перевіркою на оригінальність тексту; систематичного опрацювання нормативних джерел вітчизняного та європейського законодавства, актуальної судової практики, щорічних доповідей Уповноваженого Верховної Ради України з прав людини та правових роз'яснень Центрів протидії дезінформації. Додатково передбачається поглиблення лекційного матеріалу через пошук профільної наукової літератури у глобальних мережах, електронних бібліотечних фондах, цифрових архівах та фахових періодичних виданнях. Практичний складник передбачає виконання юридичних кейсів щодо формування запитів на інформацію, розроблення внутрішньо-корпоративних положень про комерційну таємницю, підготовки згоди на обробку відомостей про особу, верифікації КЕП та процесуального оформлення електронних доказів для суду, а також впровадження комплаєнс-програм безпечного використання алгоритмічних рішень.

Всі завдання самостійної роботи поділяються на обов'язкові та вибіркові. До обов'язкових належать завдання, які студенти мають виконувати обов'язково впродовж вивчення дисципліни. Вибіркові включають альтернативні завдання, серед яких здобувач на власний розсуд обирає конкретні завдання з тим, щоб набрати необхідну кількість балів.

Нижче подано варіанти завдань для самостійної роботи здобувачів денної форми навчання, що відповідають змісту окремих тем дисципліни та поглиблюють опрацювання навчального матеріалу. Необхідно виконати один з таких варіантів:

Варіант 1.

Здійсніть детальний юридичний аналіз статті 200 Цивільного кодексу України та норм Закону України «Про інформацію» з метою виділення ключових матеріально-правових ознак інформації як об'єкта прав.

Варіант 2.

Підготуйте офіційний проєкт запиту на доступ до публічної інформації до розпорядника (органу державної влади чи місцевого самоврядування) відповідно до вимог закону.

Варіант 3.

Обґрунтуйте у формі аналітичного огляду законодавчі критерії застосування «трискладового тесту» для правомірного обмеження доступу до відомостей.

Варіант 4.

Складіть проєкт локального акта підприємства (Положення про комерційну таємницю та конфіденційну інформацію) для забезпечення правового режиму внутрішньої безпеки.

Варіант 5.

Проаналізуйте права суб'єктів персональних даних у цифрову епоху та оформіть проєкт Згоди на обробку персональних даних для користувачів вебпорталу.

Варіант 6.

Напишіть реферат про особливості правового статусу Telegram-каналів та інших онлайн-платформ спільного доступу до інформації в контексті Закону України «Про медіа».

Варіант 7.

Сформулюйте покроковий процесуальний алгоритм перевірки автентичності та юридичної сили електронного документа, підписаного за допомогою КЕП, через державні сервіси.

Варіант 8.

Дослідіть юридичні проблеми суб'єктності й деліктоздатності штучного інтелекту та розробіть рекомендації щодо адаптації законодавства України до європейського AI Act.

Варіант 9.

Висвітліть в аналітичній доповіді правові засади захисту інформаційного суверенітету України та специфіку правового режиму інформації в умовах воєнного стану.

Варіант 10.

Оформіть проєкт клопотання до суду про долучення до матеріалів справи електронного доказу (скріншоту вебсторінки чи фіксації листування в месенджері) з дотриманням процесуальних вимог.

Варіанти контрольної роботи (для заочної форми здобуття освіти)

Нижче подано варіанти завдань для контрольної роботи, що відповідають змісту окремих тем дисципліни та поглиблюють опрацювання навчального матеріалу. Необхідно обрати варіант та виконати наведені завдання. Вимоги до контрольної роботи: 8–12 сторінок тексту (*шрифт Times New Roman, 14 pt, міжрядковий інтервал – 1*). Слід опрацювати щонайменше 10–12 джерел. Використання класичних праць з інформаційного права є обов'язковим. Дотримання принципів академічної доброчесності – засадничий принцип навчання. Здійснюйте коректне цитування використаних джерел. Заборонено плагіат: текст має бути оригінальним, з власним аналітичним та методологічним осмисленням. Максимальна кількість балів за виконану контрольну роботу – 50 балів.

Варіант 1.

1. Розкрийте предмет, специфіку методів та внутрішню структуру системи сучасного інформаційного права України.

2. Охарактеризуйте елементи інформаційних правовідносин та особливості їхнього суб'єктного й об'єктного складу.

Варіант 2.

1. Проаналізуйте конституційні механізми реалізації права на інформацію та правовий режим публічної інформації.

2. Висвітліть підстави та процедуру притягнення до юридичної відповідальності розпорядників за порушення права на доступ до відомостей.

Варіант 3.

1. Дослідіть законодавчу класифікацію інформації з обмеженим доступом на конфіденційну, таємну та службову.

2. Окресліть правові засади та інституційні механізми забезпечення охорони державної таємниці в Україні.

Варіант 4.

1. З'ясуйте специфіку та особливості функціонування режимів лікарської, банківської й адвокатської таємниць як спеціальних систем.

2. Опишіть нормативні вимоги до збирання, зберігання, обробки та транскордонної передачі персональних даних у цифрову епоху.

Варіант 5.

1. Обґрунтуйте роль Уповноваженого Верховної Ради з прав людини у сфері нагляду за захистом персональних даних.

2. Порівняйте вимоги національного законодавства про захист персональних даних із Загальним регламентом ЄС про захист даних (GDPR).

Варіант 6.

1. Визначте особливості правового статусу друкованих, онлайн-медіа та телерадіомовлення за чинним законодавством.

2. Проілюструйте підстави та правила притягнення суб'єктів медіасфери до відповідальності за поширення недостовірної інформації.

Варіант 7.

1. Аргументуйте правові основи функціонування системи «Електронний уряд», порталу й застосунку «Дія» та публічних електронних реєстрів.

2. Поясніть юридичний статус електронних довірчих послуг, кваліфікованого електронного підпису та концепцію цифрової безбар'єрності.

Варіант 8.

1. Обговоріть проблеми цивільно-правової відповідальності за шкоду, заподіяну системами штучного інтелекту та алгоритмічними рішеннями.
2. Критикуйте використання великих даних (Big Data) та хмарних технологій з позицій забезпечення недоторканності приватного життя.

Варіант 9.

1. Сформулюйте правові засади державної політики у сфері кібербезпеки та правовий режим об'єктів критичної інформаційної інфраструктури.
2. Деталізуйте юридичні механізми протидії кіберзлочинності, кібертероризму та особливості міжнародного співробітництва у сфері кіберзахисту.

Варіант 10.

1. Оцініть процесуальні правила збирання, подання, перевірки та оцінки електронних доказів у цивільному, адміністративному та кримінальному судочинстві.
2. Класифікуйте підходи до розмежування понять «оціночне судження» та «фактичне твердження» під час розгляду інформаційних спорів про дифамацію.

13. Неформальна освіта (онлайн-курси та платформи)

У межах самостійної роботи здобувачам рекомендується проходження онлайн-курсів на міжнародних освітніх платформах з метою розширення професійних компетентностей та академічної доброчесності.

Рекомендовані платформи:

- Coursera (Legal Tech and the Digital Transformation of Law: <https://www.coursera.org/learn/legal-tech-digital-transformation-of-law>; AI for Lawyers and Other Advocates: <https://www.coursera.org/specializations/ai-for-lawyers-and-other-advocates>);
- Prometheus (Безпека в інтернеті під час війни: практичний курс: <https://prometheus.org.ua/prometheus-free/cybersecurity-during-war-practical/>; Цифрова безпека на персональному рівні: <https://prometheus.org.ua/prometheus-free/personal-digital-security/>; CS50: Вступ до кібербезпеки: <https://prometheus.org.ua/prometheus-free/cs50-cybersecurity/>);
- edX (Human-Centric Cybersecurity: Political, Legal, and Behavioural Issues: <https://www.edx.org/learn/social-sciences/universite-de-montreal-human-centric-cybersecurity-political-legal-and-behavioural-issues>).

Опрацювання зазначених онлайн-курсів не є обов'язковим і здійснюється за власною ініціативою здобувача як форма неформальної освіти. Так само не є обов'язковими саме ці курси та можуть бути пройдені інші тематичні курси, тренінги тощо.

14. Питання для підготовки до підсумкового контролю (диференційований залік)

1. Що є предметом вивчення інформаційного права?
2. З яких елементів складаються інформаційні правовідносини?
3. Які специфічні юридичні властивості має інформація як об'єкт правового регулювання?
4. Які три базові принципи покладено в основу інформаційного права?
5. Що становить систему джерел інформаційного права України?
6. Як реалізується конституційне право особи на інформацію?
7. Що таке «публічна інформація» за чинним законодавством?
8. Які імперативні обов'язки покладено на розпорядників публічної інформації?
9. У чому полягає сутність законодавчого «трискладового тесту»?
10. Яка відповідальність передбачена за неправомірну відмову в наданні публічної інформації?
11. На які три види поділяється інформація з обмеженим доступом?
12. Що становить правовий режим охорони державної таємниці?
13. Як визначається та охороняється комерційна таємниця підприємства?
14. Які суб'єкти мають право доступу до відомостей, що становлять банківську таємницю?

15. У чому полягає специфіка правового режиму адвокатської таємниці?
16. Що таке «персональні дані» у розумінні інформаційного права?
17. Які ключові права має суб'єкт персональних даних?
18. Які вимоги встановлено до транскордонної передачі персональних даних?
19. Які повноваження має Уповноважений ВРУ з прав людини у сфері захисту даних?
20. Який вплив на правову систему України справляє Регламент ЄС GDPR?
21. Як Закон України «Про медіа» визначає статус онлайн-медіа?
22. Які професійні права та правові гарантії встановлено для журналістів?
23. Як визначається відповідальність медіа за поширення недостовірної інформації?
24. Як розмежовуються «оціночні судження» та «фактичні твердження»?
25. Які правові виклики виникають під час регулювання платформ спільного доступу?
26. Що становить правову основу системи «Електронний уряд» в Україні?
27. Який юридичний статус має кваліфікований електронний підпис (КЕП)?
28. Які вимоги висуваються до функціонування публічних електронних реєстрів?
29. Що таке «цифрова безбар'єрність» у контексті надання електронних послуг?
30. Які нормативні акти становлять основу державної політики у сфері кібербезпеки?
31. Яка компетенція Кіберполіції та Держспецзв'язку у сфері кіберзахисту?
32. Що таке «критична інформаційна інфраструктура» та який її правовий режим?
33. Які діяння кваліфікуються кримінальним законом як кіберзлочини?
34. Які проблеми суб'єктності штучного інтелекту існують у юридичній доктрині?
35. Як визначається цивільно-правова відповідальність за шкоду, заподіяну ШІ?
36. Що таке «смарт-контракт» та чи визнається він електронним правочином в Україні?
37. Що становить правовий зміст інформаційного суверенітету держави?
38. Які правові механізми застосовуються для протидії дезінформації?
39. Як змінюється правовий режим інформації в умовах воєнного стану?
40. Що таке «електронний доказ» та які правила його подання до суду?

15. Методи навчання

Методи навчання на лекціях: вербальний метод (лекція, дискусія, консультація, обговорення тощо); методи візуалізації (презентація, метод ілюстрації, метод демонстрацій: та інші); робота з навчально-методичною літературою (конспектування, тезування, анотування тощо); інші методи у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо).

Методи навчання на семінарських заняттях: вербальний метод (дискусія, співбесіда тощо); метод візуалізації (презентація, метод ілюстрації (графічний, табличний, тощо), метод демонстрацій та інші); робота з навчально-методичною літературою (рецензування, підготовка реферату, есе, доповіді тощо); інші методи у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо); кейс-метод (вирішення ситуацій тощо); практичний, пошуковий метод.

16. Методи оцінювання

У процесі вивчення дисципліни «Інформаційне право» використовуються такі методи оцінювання:

для поточного контролю – у вигляді усного та письмового опитування, фронтального опитування, тестування, написання есе (рефератів), вирішення кросвордів, контрольна робота (для заочної форми здобуття освіти); самостійна робота, неформальна освіта (онлайн-курси та платформи) тощо.

для підсумкового контролю – проведення підсумкового контролю (усна та/або письмова відповідь, тестування тощо).

17. Засоби діагностики результатів навчання

Робоча програма передбачає застосування засобів діагностики результатів навчання за формами контролю знань:

- *поточний контроль* може передбачати застосування широкого спектру форм та методів оцінювання знань, що проводиться за кожною темою.

- *підсумковий контроль* передбачає проведення диференційованого заліку.

Завершальним етапом досягнення запланованих програмних результатів навчання з навчальної дисципліни «Інформаційне право» є підсумковий контроль – диференційований залік.

18. Критерії та порядок оцінювання результатів навчання

Для оцінювання знань здобувачів вищої освіти застосовуються контрольні заходи у формі поточного та підсумкового контролю знань відповідно до Положення про оцінювання знань здобувачів вищої освіти.

Поточний контроль

Види навчальної діяльності здобувачів вищої освіти обираються та оцінюються викладачем за рекомендованою шкалою в залежності від особливостей навчальної дисципліни. Оцінювання окремих видів навчальної діяльності здобувача вищої освіти для дисципліни «Інформаційне право» відбувається за такими рекомендованими балами:

Види навчальної діяльності здобувачів вищої освіти	Кількість балів (від – до)
Аудиторна робота	
Відповідь на практичному, семінарському, лабораторному занятті	1-5
Вирішення ситуаційних завдань, розв'язання задач тощо	1-5
Тестування	1-5
Ділова гра, практичний кейс тощо	1-10
Інші види аудиторної роботи*	
Самостійна робота	
Реферат, есе тощо	1-10
Інші види навчальної діяльності здобувачів вищої освіти (участь у публічних заходах (конференція, олімпіада тощо); написання наукової статті, участь у конкурсах студентських робіт тощо)	1-10
Інші види самостійної роботи*	
Контрольна робота (для заочної форми здобуття освіти)	1-50

*види навчальної діяльності здобувачів освіти обираються та оцінюються викладачем за рекомендованою шкалою в залежності від особливостей навчальної дисципліни.

Для визначення ступеня засвоєння навчального матеріалу та поточного оцінювання знань здобувачів вищої освіти застосовуються критерії відповідно до Положення про оцінювання знань здобувачів вищої освіти ([https://nam.kyiv.ua/files/pdf/polozhennia-pro-otsiniuvannia-znan-zdobuvachiv-\(red-2021\).pdf](https://nam.kyiv.ua/files/pdf/polozhennia-pro-otsiniuvannia-znan-zdobuvachiv-(red-2021).pdf)).

Порядок зарахування результатів неформальної освіти

Результати проходження онлайн-курсів можуть бути зараховані як складова самостійної роботи за заявою здобувача в порядку, визначеному Положенням про порядок визнання результатів навчання набутих у неформальній/інформальній освіті (<https://nam.kyiv.ua/files/pdf/polozhennia-pro-neformalnu-ta-informalnu-osvitu.pdf>).

Максимальна кількість балів – до **10 балів** у межах самостійної роботи.

Підсумковий контроль

Максимальна кількість балів за диференційований залік з навчальної дисципліни «Інформаційне право» складає **40 балів**.

Для визначення ступеня засвоєння навчальної дисципліни та контрольного оцінювання знань здобувачів вищої освіти за підсумковим контролем застосовуються критерії відповідно до Положення про оцінювання знань здобувачів вищої освіти.

Підсумкова оцінка переводиться у національну систему оцінювання і шкалу ECTS згідно з таблицею:

Порядок переведення оцінок у систему ECTS

Сума балів за всі види навчальної діяльності	ОЦІНКА ECTS	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		для екзамену курсової роботи (проекту), практики	для заліку (диференційованого заліку)
90-100	A	Відмінно	зараховано
82-89	B	Добре	
75-81	C		
64-74	D	Задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

19. Розподіл балів, які отримують здобувачі вищої освіти

Для денної форми здобуття освіти

Поточний контроль та самостійна робота – 60											Підсумковий контроль	Сума
T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	Самостійна робота		
5 балів	5 балів	5 балів	5 балів	5 балів	5 балів	5 балів	5 балів	5 балів	5 балів	10 балів	40 балів	100 балів

Для заочної форми здобуття освіти

Поточний контроль та самостійна робота – 60		Підсумковий контроль	Сума
Контрольна робота	Самостійна робота		
50 балів	10 балів	40 балів	100 балів

20. Методичне забезпечення

Методичне забезпечення дисципліни «Інформаційне право» узагальнено в комплексі навчально-методичного забезпечення, який включає:

- силабус;
- робочу програму навчальної дисципліни;
- варіанти завдань для самостійної роботи здобувачів;
- варіанти завдань для підсумкового контролю;
- інші матеріали.

21. Рекомендована література

1. Довгань О.Д., Ткачук Т.Ю. Кіберризика критичної інфраструктури: від аналізу загроз до впровадження рішень: наук.-практ. посіб. Київ; Одеса: Фенікс, 2024. 77 с.

2. Енциклопедія соціогуманітарної інформології / за заг. ред. К.І. Белякова. Т. 1. Київ: ВД «Гельветика», 2020. 472 с. URL: https://ippi.org.ua/sites/default/files/enciklopediya_sociogumanitarnoy_informologii.pdf

3. Ковалів М.В., Єсімов С.С., Ярема О.Г. Інформаційне право України: навч. посіб. Львів: ЛьвДУВС, 2022. 416 с. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/4844/1/InformPravoUKR.pdf>

4. Ковальчук А.Ю., Чернявська Б.В. Європейський досвід протидії дезінформаційним впливам. *ScienceRise. Juridical Science*. 2024. № 2(28). С. 50–54. DOI: <https://doi.org/10.15587/2523-4153.2024.309074>

5. Ковальчук А.Ю., Чернявська Б.В., Ковальчук М.С. Організація обміну податковою інформацією між країнами як захід запобігання легалізації коштів, одержаних злочинним шляхом. *Часопис Київського університету права*. 2023. № 3. С. 75–78. DOI: <https://doi.org/10.36695/2219-5521.3.2023.14>
6. Нашинець-Наумова А.Ю. Інформаційне право: навч. посіб. К.: Київ. ун-т ім. Б. Грінченка, 2020. 136 с. URL: https://elibrary.kubg.edu.ua/id/eprint/30656/3/A_Nashynets_Naumova_IP_FPMV.pdf
7. Уткіна М.С. Інформаційне право (у схемах і таблицях): навч. посіб. Суми: СумДУ, 2022. 221 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi81/0061654.pdf>
8. Фурашев В., Радзієвська О. Правове забезпечення інформаційної безпеки: курс лекцій. Київ; Одеса: Фенікс, 2022. 158 с.
9. Чернявська Б.В., Ковальчук А.Ю. Міжнародно-правовий аспект протидії доксингу в цифрову епоху. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2024. Вип. 85(4). С. 257–267. DOI: <https://doi.org/10.24144/2307-3322.2024.85.4.37>
10. Dutchak S., Opolska N., Shchokin R. et al. International aspects of legal regulation of information relations in the global internet network. *Journal of Legal, Ethical and Regulatory Issues*. 2021. Vol. 23(3). pp. 1-7. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/3645/1/шевців%20стаття.pdf>
11. Kulchytskyi T., Rezvorovych K., Dutchak S. et al. Legal regulation of cybersecurity in the context of the digital transformation of Ukrainian society. *Lex Humana*. 2024. Vol. 16(1). pp. 443–460. URL: <https://seer.ucp.br/seer/index.php/LexHumana/article/view/2933>
12. Veselovska N., Krushynskyi S., Kravchuk O. et al. Combating cybercrime and criminal legal measures under the conditions of the state of martial. *AD ALTA – Journal of Interdisciplinary Research*. 2022. Vol. 12(2), XXXI. pp. 233–236.