

Київський університет імені Бориса Грінченка
Факультет права та міжнародних відносин
Кафедра публічного права

«ЗАТВЕРДЖУЮ»

Проректор з науково-методичної
та навчальної роботи

 Олексій ЖИЛЬЦОВ
«  » 2023 р.



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІТ-ПРАВО

для студентів

спеціальності	081 Право
рівень вищої освіти	другий (магістерський)
освітньої програми	081.00.01 Право

КИЇВ – 2023



Розробник:

Нашинець-Наумова Анфіса Юріївна, д. ю. н., професор, професор кафедри публічного права Факультету права та міжнародних відносин Київського університету імені Бориса Грінченка.

Викладач:

Нашинець-Наумова Анфіса Юріївна, д. ю. н., професор, професор кафедри публічного права Факультету права та міжнародних відносин Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри публічного права Факультету права та міжнародних відносин
Протокол від «1» вересня 2023 року № 1

Завідувач кафедри публічного права  (Ганна ВЛАСОВА)

Робочу програму погоджено з керівником проектної групи освітньої програми 081.00.01 Право
2023 р.

Гарант освітньої програми  (Петро МАТВЄЄВ)

Робочу програму перевірено
2023 р.

Заступник декана  (Анфіса НАШИНЕЦЬ-НАУМОВА)

Пролонговано:

на 20__/20__ н.р. _____ (_____). «__» _____ 20__ р., протокол №__

на 20__/20__ н.р. _____ (_____). «__» _____ 20__ р., протокол №__

на 20__/20__ н.р. _____ (_____). «__» _____ 20__ р., протокол №__

на 20__/20__ н.р. _____ (_____). «__» _____ 20__ р., протокол №__

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
ІТ-Право		
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	I	I
Семестр	2	2
Кількість змістових модулів з розподілом	1	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	32	20
Модульний контроль	8	-
Семестровий контроль		
Самостійна робота	80	100
Форма семестрового контролю	Залік	Залік

2. Мета та завдання навчальної дисципліни

Метою курсу є сприяння у підготовці фахівців-юристів, які володіють комплексом знань з ІТ-технологій в юриспруденції; надання теоретичних та практичних знань з використання, пошуку, обробки, аналізу і обміну юридичної та правової інформації в світовому інформаційному просторі.

Основним завданням курсу є формування у студентів теоретичних знань та практичних навичок у сфері інформаційних технологій в юридичній діяльності, зокрема: використання програмного забезпечення в професійній діяльності; застосування комп'ютерних і телекомунікаційних засобів; опрацювання документів в інформаційних довідково-правових системах; вміння використовувати засвоєні знання щодо захисту інформації.

3. Результати навчання за дисципліною

Студент має знати, розуміти та вміти:

– Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, цифрові, статистичні, тестові та інші, та перевіряти їх на достовірність, використовуючи сучасні методи дослідження.

– Здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.

– Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.

– Генерувати нові ідеї та використовувати сучасні технології у наданні правничих послуг.

Відповідно до освітньої програми 081.00.01 «Право» за другим (магістерським) рівнем вищої освіти зі спеціальності 081 Право, дисципліна забезпечує формування таких компетентностей:

Загальні компетентності (ЗК) –

ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК6. Здатність генерувати нові ідеї (креативність).

ЗК8. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

ЗК9. Здатність працювати в міжнародному контексті.

Спеціальні (фахові, предметні) компетентності (СК) –

СК9. Здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності.

СК10. Здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування.

СК11. Здатність критично оцінювати ефективність представництва і захисту прав, свобод та інтересів клієнтів.

СК13. Здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією.

Відповідно до освітньої програми 081.00.01 «Право» за другим (магістерським) рівнем вищої освіти зі спеціальності 081 Право, дисципліна забезпечує формування таких результатів навчання:

РН 5. Вільно спілкуватися правничою іноземною мовою (однією з офіційних мов Ради Європи) усно і письмово.

РН 8. Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.

РН 9. Генерувати нові ідеї та використовувати сучасні технології у наданні правничих послуг.

Робота студентів у Центрі практичної юриспруденції

Заняття в Центрі з дисципліни «ІТ-Право» проводяться на основі раціонального поєднання активних форм і методів навчання з урахуванням майбутньої практичної діяльності магістрів. Метою занять в Центрі практичної юриспруденції є формування у магістрів практичних навичок використання

інформаційних, телекомунікаційних технологій в професійній діяльності; вміння використовувати технології пошуку інформації; використання програмного забезпечення; знання технологій засвоєння пакетів прикладних комп'ютерних програм та довідково-правових систем тощо.

4. Структура навчальної дисципліни

4.1. Тематичний план для денної форми навчання

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Тема 1. Поняття та сутність ІТ-Права	12	2			10
Тема 2. Правовідносини у ІТ-середовищі: суб'єкти, об'єкти та зміст	18	4	2	2	10
Тема 3. Комп'ютерна програма як об'єкт правової охорони	28	4	2	2	20
Тема 4. Електронні документи та електронний документообіг	28	4	2	2	20
Тема 5. Правові аспекти використання ІТ-технологій, питання безпеки та захисту інформації	26	2	2	2	20
Модульний контроль	8				
Разом	120	16	8	8	80
Усього годин	120	16	8	8	80

4.2. Тематичний план для заочної форми навчання

Тематичний план для заочної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Тема 1. Поняття та сутність ІТ-Права	27	2			25
Тема 2. Комп'ютерна програма як об'єкт правової охорони	31	2	2	2	25
Тема 3. Електронні документи та електронний документообіг	31	2	2	2	25
Тема 4. Правові аспекти використання ІТ-технологій, питання безпеки та захисту інформації	31	2	2	2	25
Всього	120	8	6	6	100
Усього разом	120	8	6	6	100

5. Програма навчальної дисципліни

Тема 1. Поняття та сутність ІТ-Права

Поняття та характеристика ІТ-Права. Інтернет-право. ІТ-Право як право цифрового середовища. Співвідношення «Інформаційного права» з «ІТ-Правом». ІТ-Право – це особливе право, яке регулює відносини у цифровому середовищі. Нормативно-правові акти, в тому числі і міжнародні щодо регулювання правових норм в цифровому середовищі. Засади ІТ-Права. Особливості ІТ-Права. Співвідношення понять «Цифрове середовище» і «Мережа Інтернет». Поняття електронної (цифрової) інформації. Поняття диджиталізації.

Тема 2. Правовідносини у ІТ-середовищі: суб'єкти, об'єкти та зміст

Правовідносини у сфері ІТ-технологій. Абсолютні та відносні правовідносини. Контент та інформаційна безпека власників і користувачів. Види правовідносин: між замовником веб-сайту і його розробником; між

замовником веб-сайту і його працівником; між співавторами – розробниками сайту; між власником веб-сайту і реєстратором; між реєстратором та адміністратором доменного простору; між власником веб-сайту і хостинг-провайдером; між власником веб-сайту і власниками веб-сторінок; між власником веб-сайту і авторами інформаційних матеріалів; між користувачами Інтернету і власником веб-сайту та авторами. Права та обов'язки сторін правовідносин у ІТ-середовищі.

Тема 3. Комп'ютерна програма як об'єкт правової охорони

Галузева приналежність комп'ютерних програм. Зовнішній вираз комп'ютерної програми. Комп'ютерна програма як об'єкт авторського права. Комп'ютерна програма як об'єкт винаходу. Визначення і правова регламентація інтернет-сайту. Види інтернет-сайтів. Класифікація комп'ютерних програм. Ознаки комп'ютерних програм. Системні та допоміжні (прикладні) комп'ютерні програми. Правова охорона комп'ютерних програм. Авторство/співавторство на комп'ютерну програму. Способи використання комп'ютерних програм. Реєстрація права інтелектуальної власності на комп'ютерну програму. Форми захисту інтелектуальної власності в ІТ-сфері.

Тема 4. Електронні документи та електронний документообіг

Державна політика з питань впровадження електронного документообігу. Поняття, ознаки та характеристики електронного документу. Співвідношення поняття «Документ» та «Електронний документ». Реквізити електронного документу. Електронний цифровий підпис. Особистий ключ. Відкритий ключ. Сертифікат відкритого ключа. Центр сертифікації ключів. Накладання, перевірка електронного цифрового підпису. Позначка часу на електронному документі. Електронний документообіг. Зберігання електронної документації.

Тема 5. Правові аспекти використання ІТ-технологій, питання безпеки та захисту інформації

Інформаційна безпека. Система органів влади, що відповідають за інформаційну безпеку та захист інформації. Захист інформації від вірусних атак. Ознаки зараження комп'ютера вірусом. Типи вірусів. Антивірусні програми. Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності. Засоби захисту інформації. Кіберзлочинність. Кібертероризм.

6. Контроль навчальних досягнень

6.1. Система оцінювання навчальних досягнень студентів для денної форми навчання

№ з/п	Вид діяльності студента	Макс. кількість балів за одиницю		
			Кільк. одиниць	Макс. кількість балів за вид
1	Відвідування лекцій	1	8	8
2	Відвідування практичних занять	1	4	4
3	Виконання завдань на практичному занятті	10	4	40
4	Відвідування лабораторних занять	1	4	4
5	Виконання завдань на лабораторному занятті	10	4	40
6	Виконання завдань для самостійної роботи	5	1	5
7	Виконання модульної роботи	25	4	100
	Разом	-	-	201
	Максимальна кількість балів:		201	
	Розрахунок коефіцієнта:		0,497	
	Підсумковий бал		100	

для заочної форми навчання

№ з/п	Вид діяльності студента	Макс. кількість балів за одиницю		
			Кільк. одиниць	Макс. кількість балів за вид
1	Відвідування лекцій	1	4	4
2	Відвідування практичних занять	1	3	3
3	Відвідування лабораторних занять	1	3	3
4	Виконання завдань на практичному занятті	10	3	30
5	Виконання завдань на лабораторному занятті	10	3	30
6	Виконання завдань для самостійної роботи	5	1	5
	Разом	-	-	75
	Максимальна кількість балів:		75	
	Розрахунок коефіцієнта:		1,333	
	Підсумковий бал		100	

Критерії оцінювання навчальних досягнень студентів при виконанні практичних (лабораторних) занять

Бал	Критерій
9-10	Магістр володіє системними знаннями навчального матеріалу та ефективно їх застосовує для виконання практичних (лабораторних) завдань, передбачених навчальною програмою. Відповідь магістра повна, правильна, логічна, містить аналіз, систематизацію, узагальнення. Вміє самостійно знаходити і користуватися джерелами інформації, оцінювати отриману інформацію. Правильно і усвідомлено використовує всі види нормативно-правової документації в межах навчальної дисципліни.
7-8	Магістр володіє основним матеріалом та застосовує його при виконанні практичних (лабораторних) завдань як у типових, так і дещо ускладнених умовах. Для визначення основних понять, аналізує, порівнює і систематизує інформацію. Його відповідь в цілому правильна, логічна і достатньо обґрунтована. Виконує практичні (лабораторні) завдання за типовим алгоритмом з консультацією викладача. Усвідомлено користується довідковою інформацією. При виконанні практичних (лабораторних) завдань припускається несуттєвих помилок, які може виправити.
5-6	Магістр без достатнього розуміння відтворює основний навчальний матеріал та виконує практичні (лабораторні) завдання з епізодичною допомогою викладача і з окремими помилками визначення основних понять. Може частково аналізувати навчальний матеріал, порівнювати і робити висновки. Користується окремими видами нормативної документації. При відповіді та виконанні практичних (лабораторних) завдань припускається помилок, може частково виправляти.
3-4	Магістр частково володіє навчальним матеріалом, не в змозі виконати практичні (лабораторні) завдання, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
1-2	Магістр за допомогою викладача відтворює на рівні розпізнавання окремі елементи (фрагменти) навчального матеріалу та виконує зі значними труднощами окремі елементи практичних (лабораторних) завдань. Припускається суттєвих помилок.

6.2 Завдання для самостійної роботи та критерії оцінювання

Питання, що виносяться на самостійне опрацювання

1. Законодавче визначення домену чи доменного імені.
2. Адміністрування адресного простору мережі Інтернет в Україні і світі.

3. Діяльність світової Інтернет-корпорації з призначення доменних імен і номерів – (ICANN).
4. Поняття і правове регулювання електронної комерції.
5. Виникнення електронних грошей.
6. Емітенти, користувачі і власники електронних грошей.
7. Види електронних грошей.
8. Електронні платіжні системи.
9. Відмінність електронних грошей від криптовалют.
10. Договори, що використовуються в ІТ-сфері.
11. Види порушень авторських і суміжних прав в Інтернеті
12. Особливості та види реклами в інтернеті (медійна, банерна, контекстна, вірусна реклама).
13. Просування, інтернет-розсилки, спам ті інші види інтернет-реклами.
14. Право Європейського Союзу в ІТ-сфері

Критерії оцінювання

Бал	Критерій
5	Магістр засвоїв теоретичний матеріал, який винесений на самостійну роботу, застосування для оформлення результатів самостійної роботи не тільки рекомендованої, а й додаткової літератури та творчого підходу; чітке володіння понятійним апаратом, теорією; вміння використовувати їх для виконання конкретних практичних завдань, розв'язання ситуацій. Оформлення результатів самостійної роботи повинно бути логічним та послідовним.
3-4	Магістр засвоїв теоретичний матеріал з відповідної теми, який винесений на самостійну роботу та наявне вміння орієнтуватися в ньому, усвідомлене застосування знань для розв'язання практичних задач. Оформлення виконаного завдання з самостійної роботи має бути послідовним.
1-2	Магістр не повністю засвоїв тему для самостійного опрацювання, не досконало володіє основними поняттями та положеннями навчальної дисципліни, невпевнено орієнтується в першоджерелах та в рекомендованій літературі, непереконливо відповідає, додаткові питання викликають невпевненість або відсутність знань.
0	Магістр не опанував навчальний матеріал з відповідної теми для самостійного опрацювання, не знає основних понять і термінів навчальної дисципліни, не орієнтується в першоджерелах та в рекомендованій літературі, відсутнє наукове або логічне мислення.

6.3. Форми проведення модульного контролю та критерії оцінювання

Виконання модульних контрольних робіт здійснюється в письмовому вигляді з використанням роздрукованих завдань або на платформі Moodle. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

Критерії оцінювання

Бал	Критерії
24-25	Магістр вирішив всі завдання абсолютно вірно і повно дав відповіді на питання як теоретичного, так і практичного характеру. Логічно і послідовно аргументував і виклав свою точку зору.
20-23	Магістр вирішив завдання з 1 помилкою, відповідь на питання містить повне розгорнуте, правильне та обґрунтоване викладення матеріалу, допущено 2-3 помилки при вирішенні практичних завдань.
15-19	Магістр правильно і повно вирішив більшість, але не всі завдання, відповідь на запитання є не повністю аргументованою; допускає незначні неточності
10-14	Магістр правильно вирішив половину завдань; думка викладена з порушенням логіки подання матеріалу. Магістр правильно вирішив ситуацію, проте не зовсім слушно аргументує її, або враховує не всі, а деякі умови ситуації. Вирішує декілька завдань поверхнево.
5-9	Магістр вирішив трохи менше половини завдань; може дати визначення юридичного поняття. Відповідь на запитання дає неповно і поверхнево.
0-4	Магістр не вирішив більшість завдань або вирішив неправильно; відповіді на питання є неповними; неправильно обґрунтовує своє рішення.

6.4. Форми проведення семестрового контролю та критерії оцінювання

Навчальні досягнення студентів з дисципліни «ІТ-Право» оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поетапної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок на практичних та лабораторних заняттях та під час виконання самостійної роботи, розширення кількості підсумкових балів до 100.

Семестровий контроль знань студентів з навчальної дисципліни здійснюється у формі заліку.

6.5. Шкала відповідності оцінок

Рейтингова оцінка	Оцінка за стобальною шкалою	Значення оцінки
A	90-100 балів	Відмінно – відмінний рівень знань (умінь) в межах обов'язкового матеріалу з можливими незначними недоліками
B	82-89 балів	Дуже добре – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81 балів	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74 балів	Задовільно – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68 балів	Достатньо – мінімально можливий допустимий рівень знань (умінь)
FX	35-59 балів	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34 балів	Незадовільно з обов'язковим повторним вивченням курсу – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична карта дисципліни

для денної форми навчання

Разом: 120 год., із них: лекції – 16 год., практичні заняття – 8 год.,

лабораторні заняття – 8 год.

Модульний контроль – 8 год.

Самостійна робота – 80 год.

Тиждень	I	II	III	IV	V	VI	VII	VIII
Лекції (бали)	<i>Л1 (1б) Л2 (1б)</i>	<i>Л3 (1б)</i>	<i>Л4 (1б)</i>	<i>Л5 (1б)</i>	<i>Л6 (1б)</i>	<i>Л7 (1б)</i>	<i>Л8 (1б)</i>	
Практичні заняття (теми, бали)		<i>Тема 2 1-11 б</i>		<i>Тема 3 1-11 б</i>		<i>Тема 4 1-11 б</i>		<i>Тема 5 1-11 б</i>
Лабораторні заняття (теми, бали)			<i>Тема 2 1-11 б</i>		<i>Тема 3 1-11 б</i>		<i>Тема 4 1-11 б</i>	<i>Тема 5 1-11 б</i>
Самостійна робота	(5 балів)							
Поточний контроль (вид, бали)				МКР 0–25	МКР 0–25		МКР 0–25	МКР 0–25
Підсумковий контроль (вид, бали)	Залік (100 балів)							

для заочної форми навчання

Разом: 120 год., із них: лекції – 8 год., практичні заняття – 6 год.,

лабораторні заняття – 6 год.

Самостійна робота – 100 год.

Тиждень	I	II	III	IV				
Лекції (бали)	<i>Л1 (1 б)</i>	<i>Л2 (1 б)</i>	<i>Л3 (1 б)</i>	<i>Л4 (1 б)</i>				
Практичні заняття (бали)		<i>ПР 1 1-11 б</i>	<i>ПР 2 1-11 б</i>	<i>ПР 3 1-11 б</i>				
Лабораторні заняття (бали)		<i>Лаб 1 1-11 б</i>	<i>Лаб 2 1-11 б</i>	<i>Лаб 3 1-11 б</i>				
Самостійна робота	(5 балів)							
Підсумковий контроль (вид, бали)	Залік (100 балів)							

8. Рекомендовані джерела

1. Загальна декларація прав людини 1948 року // *Голос України*, 2008. 10 груд.
2. Конвенція про захист прав людини і основоположних свобод 1950 року // *Голос України*. 2001. 10 січ.
3. Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року. [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_326.
4. Конвенція про оцінку впливу на навколишнє середовище у транскордонному контексті від 25 лютого 1991 року. [Електронний ресурс]. Режим доступу: http://zakon1.rada.gov.ua/laws/show/995_272.
5. Угода про співробітництво в галузі інформації від 09.10.1992 р. // *Офіційний вісник України*. 2004. № 40. Ст. 2700.
6. Директива 95/46/ЄС Європейського Парламенту і Ради Європи «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 р. // *Офіційний журнал L 281*, 23/11/1995. С. 0031-0050.
7. Директива 97/66/ЄС Європейського Парламенту і Ради Європи «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» // *Офіційний журнал L 024*, 30/01/1998 С. 0001-0008.
8. Окінавська Хартія глобального інформаційного суспільства від 22.07.2000 р. // *Дипломатический вестник*. 2000. № 8. С. 51-56.
9. Конвенція про кіберзлочинність від 23 листопада 2001 року // *Офіційний вісник України*. 2007. № 65.
10. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» від 12.12.2003 р. [Електронний ресурс]. Режим доступу: http://zakon1.rada.gov.ua/laws/show/995_c57.
11. Резолюція 60/45, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй, «Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки» від 08.12.2005 р. [Електронний ресурс]. Режим доступу: http://zakon1.rada.gov.ua/laws/show/995_e45.
12. Конституція України: Прийнята Верховною Радою України 28.06.1996 року // *Відомості Верховної Ради України*. 1996. № 30. Ст.141.
13. Кодекс України про адміністративні правопорушення від 27.12.1984 року // *Відомості Верховної Ради Української РСР*. 1984. Додаток до № 51. Ст.1122.
14. Кримінальний кодекс України від 05.04.2001 року // *Відомості Верховної Ради України*. 2001. № 25–26. Ст.131.
15. Цивільний кодекс України від 16.01.2003 року // *Відомості Верховної Ради України*. 2003. № 40. Ст. 356.

16. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. 1992. № 48. Ст. 650.
17. Закон України «Про друковані засоби масової інформації (пресу) в Україні» від 16.11.1992 року // Відомості Верховної Ради України. 1993. № 1. Ст.1.
18. Закон України «Про науково-технічну інформацію» від 25 червня 1993 року // Відомості Верховної Ради України. 1993. № 33. Ст. 345.
19. Закон України «Про Національний архівний фонд та архівні установи» від 24.12.1993 року // Відомості Верховної Ради України. 1994. № 15. Ст. 86.
20. Закон України «Про державну таємницю» від 21.01.1994 року // Відомості Верховної Ради України. 1994. № 16. С.93.
21. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 року // Відомості Верховної Рпди України. 1994. № 31. Ст. 286.
22. Закон України «Про бібліотеки і бібліотечну справу» від 27.01.1995 року // Відомості Верховної Ради України. 1995. № 7. Ст. 45.
23. Закон України «Про інформаційні агентства» від 28.02.1995 року // Відомості Верховної Ради України. 1995. № 13. Ст. 83.
24. Закон України «Про звернення громадян» від 02.10.1996 року // Відомості Верховної Ради України. 1996. № 47. Ст. 256.
25. Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» від 23.09.1997 року // Відомості Верховної Ради України. 1997. № 50. Ст. 302.
26. Закон України «Про національну програму інформатизації» від 04.02.1998 року // Відомості Верховної Ради України. 1998. № 27–28. Ст. 181.
27. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 року // Відомості Верховної Ради України. 2003. № 36. Ст. 275.
28. Закон України «Про телекомунікації» від 18.11.2003 року // Відомості Верховної Ради України. 2004. № 12. Ст. 155.
29. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 року // Відомості Верховної Ради України. 2007. № 12. Ст. 102.
30. Закон України «Про доступ до публічної інформації» від 13.01.2011 року // Відомості Верховної Ради України. 2011. № 32. Ст. 314.
31. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України // Урядовий кур'єр від 28.08.2021.
32. Про рішення Ради національної безпеки і оборони України від 7 грудня 2019 року «Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки»: Указ Президента України від 20.12.2019. № 923/2019.
33. Розпорядження Кабінету Міністрів України від 15.05.2013 року № 386-

р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» // Урядовий кур'єр. 2013. № 105.

34. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. № 2163-VIII.

35. Щодо окремих заходів із забезпечення інформаційної безпеки РНБО: Рішення РНБО від 14.05.2021.

36. Порядок отримання автоматизованою системою обробки даних Міністерства внутрішніх справ України інформаційних файлів або метаданих від автоматичної системи виявлення та фіксації шляхом фотозйомки або відеозапису подій, що містять ознаки адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху, за допомогою технічних засобів (приладів контролю) МВС України: Наказ від 06.04.2020. № 326. Зареєстровано: Мін'юст України від 08.05.2020. № 422/34705.

37. Про схвалення Концепції впровадження технологій будівельного інформаційного моделювання (BIM-технологій) в Україні та затвердження плану заходів з її реалізації: Розпорядження Кабінету Міністрів України від 17.02.2021. № 152-р.

38. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Щодо окремих заходів із забезпечення інформаційної безпеки»: Указ Президента України від 18.05.2021 № 198/2021.

39. Постанова Кабінету Міністрів України від 09.08.1993 року № 611 «Про перелік відомостей, що не становлять комерційної таємниці». [Електронний ресурс]. Режим доступу: <http://zakon4.rada.gov.ua/laws/show/611-93-%D0%BF>.

40. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12.08.2005 року № 440 // Офіційний вісник України, 2005. № 34. С. 172. стаття 2089.

41. Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг: Указ Президента України // Урядовий кур'єр. 2019. № 144.

42. Про деякі заходи з покращення доступу до мобільного Інтернету: Указ Президента України // Урядовий кур'єр. 2019. № 128.

43. Про внесення змін до Правил надання та отримання телекомунікаційних послуг: Постанова Кабінету Міністрів України // Урядовий кур'єр. 2019. № 547.

44. Про затвердження Положення про інтегровану систему електронної ідентифікації: Постанова Кабінету Міністрів України // Урядовий кур'єр. 2019. № 211.

45. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури Постанова Кабінету Міністрів України // Урядовий кур'єр. 2019. № 118.

46. Про внесення змін до Положення про формування та виконання Національної програми інформатизації: Постанова Кабінету Міністрів України

// Урядовий кур'єр. 2019. № 103.

47. Рекомендації для Інтернет-провайдерів, контент-провайдерів та користувачів файлообмінних мереж та інших веб-сервісів щодо правомірного використання об'єктів авторського права і суміжних прав у мережі Інтернет, затв. Державною службою інтелектуальної власності України. URL-адреса. Електронний ресурс. Режим доступу: <http://sips.gov.ua/ua/ip.html?s=print>.

48. Брижко В.М. Інформаційне право та інформаційне законодавство. НДІП НАПрН України. 2-ге вид., допов. Харків : Право, 2021. 288 с.

49. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. Київ, ДУТ. 2019. 288 с.

50. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності / І. О. Валюшко. // Вісник НТУУ "КПІ". Політологія. Соціологія. Право. 2018. №3. С. 117–124.

51. Головка О. М. Медіабезпека людини: засади інформаційно-правової політики: монографія. Київ: Видавничий дім «АртЕк». 2019. 168 с.

52. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.

53. Інтернет речей: теоретико-методологічні основи правового регулювання. Т.1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія / О.А. Баранов; НДІП НАПрН України. К.: Видавничий дім «АртЕк». 2018. 344 с.

54. ІТ ПРАВО / Яворська Л.С., Тарасенко Л.Л., Мартин В.М., Самагальська Ю.Я. та ін. / За заг. ред. Яворської О.С. Львів: Видавництво «Левада», 2017. 470 с.

55. Кормич Б.А. Інформаційне право [Текст]: підручник. Х. : БУРУН і К., 2011. 334 с.

56. Кевін Митник Мистецтво залишатись непоміченим. Хто ще читає ваші імейли? Київ: Наш формат, 2019. 280 с.

57. Когут Ю.І. Цифрова трансформація економіки та проблеми кібербезпеки. Київ: SIDCON, 2021. 368 с.

58. Марущак А.І. Інформаційне право України. К.: ЦУЛ, 2011. 456 с.

59. Науково-практичний коментар до Закону України «Про доступ до публічної інформації». [Електронний ресурс]. Верховна Рада України: Режим доступу: http://www.president.gov.ua/docs/comment_api_final.pdf.

60. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с.

61. Нашинець-Наумова А.Ю. Практикум з інформаційного права: навчально-методичний посібник. К.: Типографія «Планета», 2014. 128 с.

62. Нашинець-Наумова А.Ю. Основи інформаційного права: навчальний посібник. К.: Вив-во «Сталь», 2015. 198 с.

63. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. К.: Видавничий дім «Гельветика», 2017. 169 с.
64. Нашинець-Наумова А.Ю. Інформаційна безпека суб'єктів господарювання: проблеми теорії та практики правозастосування: монографія / під заг. ред. д.ю.н. В.І. Курила. Херсон: Видавничий дім «Гельветика», 2017. 386 с.
65. Нашинець-Наумова А.Ю. Правове забезпечення інформаційної безпеки: міжнародний досвід і можливість використання // Право і суспільство. Дніпро, 2018. № 6. С. 159–164.
66. Нашинець-Наумова А.Ю. Принципи забезпечення системи національної безпеки: конституційно-правовий аспект // Науковий вісник міжнародного гуманітарного університету. Збірник наукових праць. Серія: Юриспруденція. Одеса, 2018. № 35. Т.1. С. 50–56.
67. Нашинець-Наумова А.Ю. До питання щодо боротьби з кібершпіонажем: вивчення та осмислення // Актуальні проблеми правознавства. Зб. наук. праць. Тернопіль, 2019. Вип. 1 (17). С. 126-132.
68. Нашинець-Наумова А.Ю. Світовий досвід законодавчої регламентації режимів конфіденційної інформації // Підприємництво, господарство і право. Київ, 2019. №4. С. 166-171.
69. Нашинець-Наумова А.Ю. Протидія комп'ютерній злочинності в кібернетичному просторі // Вісник кримінологічної асоціації України. Зб. наук. праць. Харків, 2019. № 1(20). С. 108-117.
70. Основи ІТ-права: навч. посіб. / Т. В. Бачинський, Р. І. Радейко О. І. Харитоновна. К.: Юрінком Інтер. 2017. 208 с.
71. Пилипчук В.Г. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.
72. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків: 2018. 289 с.
73. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних. Збірник документів; [неофіційний пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука]. (Науково-дослідний інститут інформатики і права Національної академії правових наук України). К. : ТОВ «Видавничий дім» АртЕк», 2018. 180 с.
74. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи: монографія / А. В. Тарасюк. Київ; Одеса : Фенікс, 2020. 404 с.
75. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : Монографія. К. : ТОВ «Видавничий дім «АртЕк», 2018. 411 с.
76. Харитоновна О.І. Проблемні питання визначення системи (структури)

ІТ-ПРАВА // ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. Львів: НУ «Львівська політехніка», 2016. С. 280.

77. Харитонова О.І., Бачинський Т.В., Радейко Р.І. ІТ-ПРАВО. Київ: ЮРІНКОН-ІНТЕР, 2020. 244 с.

78. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Белякова. Київ: КВІЦ, 2019. 344 с.