ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА

ЗАТВЕРДЖЕНО

Рішення вченої ради університету
29 серпня 2025 року,
Протокол № 1

Проректор з навчальної роботи

_____
(підпис) (ініціали, прізвище)

___ _____ 2025 року

м.п.

РОБОЧА ПРОГРАМА
навчальної дисципліни
«ІНФОРМАЦІЙНА БЕЗПЕКА»
для підготовки на другому освітньому рівні здобувачів вищої освіти ступеня магістр за спеціальністю 081 Право галузі знань 08 Право

м. Хмельницький
2025

Розробник робочої програми:
Викладач дисципліни:

професор кафедри конституційного, адміністративного та фінансового права, кандидат юридичних наук, професор

_____ І.П. Сторожук

25 серпня 2025 року

–

Схвалено кафедрою конституційного, адміністративного та фінансового права, протокол №1 від 26 серпня 2025 року

Завідувач кафедри _____ О.О. Галус

26 серпня 2025 року 2025 року

Декан юридичного факультету _____ В. М. Захарчук

26 серпня 2025 року

Погоджено методичною радою університету 27 серпня 2025 року, протокол № 1.

Голова методичної ради _____ І.Б. Ковтун

27 серпня 2025 року

_____

Обліковий обсяг робочої програми – 0,9 ум.др.арк.

ЗМІСТ

1. Опис навчальної дисципліни

1.	Шифр і назва галузі знань	–	08 Право
2.	Код і назва спеціальності	–	081 Право
3.	Назва спеціалізації	–	спеціалізація не передбачена
4.	Назва дисципліни	–	Інформаційна безпека
5.	Тип дисципліни	–	вибіркова
6.	Код дисципліни	–	
7.	Освітній рівень, на якому вивчається дисципліна	–	другий
8.	Ступінь вищої освіти, що здобувається	–	магістр
9.	Курс / рік навчання	–	перший
10.	Семестр	–	другий, третій
11.	Обсяг вивчення дисципліни:		
	1) загальний обсяг (кредитів ЄКТС / годин)	–	3,0 / 90
	2) денна форма навчання:		
	аудиторні заняття (годин)	–	30
	% від загального обсягу	–	33
	лекційні заняття (годин)	–	16
	% від обсягу аудиторних годин	–	53
	семінарські заняття (годин)	–	14
	% від обсягу аудиторних годин	–	47
	самостійна робота (годин)	–	60
	% від загального обсягу	–	67
	3) заочна форма навчання:		
	аудиторні заняття (годин)	–	14
	% від загального обсягу	–	16
	лекційні заняття (годин)	–	8
	% від обсягу аудиторних годин	–	57
	семінарські заняття (годин)	–	6
	% від обсягу аудиторних годин	–	43
	самостійна робота (годин)	–	76
	% від загального обсягу	–	84
12.	Форма семестрового контролю	–	Залік
13.	Мова вивчення дисципліни	–	українська.

2. Заплановані результати навчання

Навчальна дисципліна «Інформаційна безпека» забезпечує досягнення таких результатів навчання, передбачених освітньо-професійною програмою «Магістр права»:

Програмні компетентності, які здобуваються під час вивчення навчальної дисципліни

Загальні компетентності:

ЗК-1. Здатність до абстрактного мислення, аналізу та синтезу

ЗК-3 Здатність до пошуку, оброблення та аналізу інформації з різних джерел

ЗК-6 Здатність генерувати нові ідеї (креативність)

Фахові компетентності спеціальності (ФК):

СК-2 Здатність аналізувати та оцінювати вплив правової системи Європейського Союзу на правову систему України

СК-4 Здатність оцінювати взаємодію міжнародного права та міжнародних правових систем з правовою системою України

СК-6 Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію

СК-10 Здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування

Результати навчання

РН-1. Оцінювати природу та характер суспільних процесів і явищ, і виявляти розуміння меж та механізмів їх правового регулювання

РН-4. Здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки

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

РН-10. Ефективно працювати з джерелами національного та міжнародного права, виявляти колізії, прогалини, інші недоліки правового резулювання

РН-17. Інтегрувати необхідні знання та розв'язувати складні задачі правозастосування у різних сферах професійної діяльності

Після завершення вивчення дисципліни здобувач повинен продемонструвати такі результати навчання:	
1. Знання *(здатність запам'ятовувати або відтворювати факти (терміни, конкретні факти, методи і процедури, основні поняття, правила і принципи, цілісні теорії тощо)*	
1.1)	визначення понятійно-термінологічного апарату з інформаційної безпеки;
1.2)	основної законодавчої, наукової та нормативно-методологічної бази у сфері забезпечення інформаційної безпеки;
1.3)	реальних та потенційних загроз у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;
1.4)	основних моделей уразливостей та джерел загроз;
1.5)	розкривати міжнародно-правові стандарти в галузі інформаційної безпеки;
1.6)	основних компонентів автоматизованих систем управління доступом та вимог до їх функціональних характеристик;
1.7)	основних методів, способів та засобів ідентифікації осіб;
1.8)	етапів побудови комплексної системи санкціонованого доступу та засобів комплексного захисту об'єктів від несанкціонованого доступу.

2. Розуміння *(здатність розуміти та інтерпретувати вивчене, уміння пояснити факти, правила, принципи; перетворювати словесний матеріал у, наприклад, математичні вирази; прогнозувати майбутні наслідки на основі отриманих знань)*	
2.1)	основних видів загроз інформаційній безпеці та технічних каналів витоку інформації, методи їх виявлення та блокування;
2.2)	основних видів та можливості технічних засобів і систем захисту інформації;
2.3)	Ррозуміти та могти пояснити механізми й процедури інформаційного захисту прав людини;
2.4)	міжнародно-правові стандарти в сфері інформаційної безпеки;
2.5)	прогнозувати тенденції нормотворення й головні напрямки здійснення інформаційної політики держави.
3. Застосування знань *(здатність використовувати вивчений матеріал у нових ситуаціях (наприклад, застосувати ідеї та концепції для розв'язання конкретних задач)*	
3.1)	застосовувати правову методологію національного законодавства забезпечення сфери інформаційної безпеки;
3.2)	пристосовувати до вітчизняного контексту позитивний досвід зарубіжних країн в сфері інформаційної безпеки;
3.3)	проектувати, ініціювати, виконувати інноваційні комплексні наукові дослідження у галузі професійної освіти на основі цілісного системного наукового світогляду;
3.4)	застосовувати право як механізм гарантування інформаційної безпеки;
3.5)	демонструвати вміння здійснювати критичний аналіз, оцінку сучасних наукових досягнень, генерування нових ідей у вирішенні дослідницьких і практичних завдань;
3.6)	застосовувати знання з інформаційної безпеки в широкому діапазоні практичної роботи та в повсякденному житті;
3.7)	з'ясовувати форми, способи і засоби захисту прав суб'єктів інформаційних правовідносин.
4. Аналіз *(здатність розбивати інформацію на компоненти, розуміти їх взаємозв'язки та організаційну структуру, бачити помилки й огріхи в логіці міркувань, різницю між фактами і наслідками, оцінювати значимість даних)*	
4.1)	дискутувати щодо місця відносин з інформаційної безпеки в системі юридичних наук;
4.2)	досліджувати тенденції нормотворення й державної політики у сфері інформаційної безпеки;
4.3)	критично оцінювати щодо створення та розвитку системи інформаційної безпеки;
4.4)	класифікувати юридичні делікти в медичних відносинах та визначати їх ознаки та юридичний склад;
4.5)	вільно і компетентно спілкуватись в діалоговому режимі з широкою науковою спільнотою та громадськістю щодо сучасних концепцій дослідження проблем медичного права;
4.6)	виділяти механізми й процедури захисту прав людини у сфері охорони здоров'я (національні й міжнародні);
4.7)	класифікувати види й підстави юридичної відповідальності у сфері охорони здоров'я.
5. Синтез *(здатність поєднувати частини разом, щоб одержати ціле з новою системною властивістю)*	
5.1)	систематизувати напрямки змін в сфері інформаційної безпеки;
5.2)	упорядковувати чинники формування прав й обов'язків суб'єктів безпекових правовідносин в інформаційній сфері;
5.3)	узагальнювати юридичну практику в галузі інформаційної безпеки;
5.4)	систематизувати правові умови провадження окремих видів інформаційної безпеки.

	6. Оцінювання *(здатність оцінювати важливість матеріалу для конкретної цілі)*
6.1)	пояснювати доцільність застосування зарубіжного досвіду в сфері інформаційної безпеки;
6.2)	оцінювати реальні та потенційні загрози у сфері інформаційної безпеки та нормативноправові шляхи їх запобігання;
6.3)	проводити аналіз ефективності законодавства України та міжнародних стандартів у сфері захисту інформації.
	7. Створення (творчість) *(здатність до створення нового культурного продукту, творчості в умовах багатовимірності та альтернативності сучасної культури)*
7.1)	визначати напрямки вдосконалення інформаційного законодавства відповідно до сучасних умов;
7.2)	готувати необхідні процесуальні документи для захисту прав людини у сфері захисту інформації
7.3)	застосовувати юридичну практику для правозахисної і правозастосовної діяльності, в т.ч. правові позиції Європейського суду з прав людини, Верховного Суду України;
7.4)	використовувати юрисдикційні й неюрисдикційні форми захисту прав людини у сфері захисту інформації;
7.5)	правильно кваліфікувати наслідки порушення в сфері інформаційної безпеки та давати їм належну юридичну оцінку.

3. Програма навчальної дисципліни

Тема 1. Концептуальні засади інформаційної безпеки

Базові поняття щодо інформації та інформаційної безпеки. Основні загальносвітові тенденції розвитку суспільства та їх вплив на напрями розвитку українського суспільства. Основні причини та механізми міждержавних, міжблокових та міжрегіональних сучасних протистоянь. Природа та визначення інформації. Носії інформації. Засоби передачі та сприйняття інформації. Властивості інформації. Сутність та визначення поняття «безпека інформації» та «безпечність інформації». Сутність та визначення поняття «інформаційна безпека». Критерії визначення об’єктів інформаційної небезпеки та їх обґрунтування. Ієрархія об’єктів інформаційної небезпеки. Інформаційна безпека як складова національної безпеки держави.

Тема 2. Інтереси держави в інформаційній сфері

Загальна характеристика інтересів держави у сфері інформаційної безпеки. Інформаційна політика держави. Політико-правові аспекти формування інформаційного суспільства держави. Стратегія формування та розвитку єдиного інформаційного простору України.

Тема 3. Загрози людині та суспільству в інформаційній сфері

Поняття і сутність маніпулювання свідомістю людини. Способи та технології маніпулювання свідомістю людини. Технології масового маніпулятивного впливу. Поняття та напрями реалізації сугестивних технологій маніпулятивного впливу. Реалізація маніпулятивних технологій в засобах масової інформації. Вплив на людину певних фізичних факторів інформаційного середовища. Вікна Овертона в аспекті інформаційної безпеки. Інформаційно-психологічна безпека особи.

Тема 4. Інтернет та інформаційна безпека

Особливості встановлення та проблеми реалізації інформаційних правовідносин в мережі Інтернет. Інтернет як арена сугестивного маніпулятивного впливу. Сутність, витоки та механізми трансформаційних процесів забезпечення національної та міжнародної безпеки. Сутність, витоки

та механізми глобалізації інформаційного простору. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення.

Тема 5. Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки

Кібернетика як джерело небезпеки. Процеси створення та впровадження інформаційно-комунікаційних технологій (ІКТ) як об'єкт і предмет нормативноправового регулювання. Безпека глобальних інформаційних систем та мереж. Соціальна інженерія в аспекті маніпулятивного впливу. Визначення поняття «кібернетична безпека» (кібербезпека). Сутність поняття «кіберсоціалізація». Соціальні мережі. Мережева мобілізація: питання демократії та безпеки. Наслідки кіберсоціалізації. Сутність поняття «кіберцивілізація». Потенційні загрози кіберцивілізації для людства. Об'єкти інформаційних загроз. Об'єкти кіберзагроз. Сутність зв'язку інформаційної безпеки та кібербезпеки.

Тема 6. Інформаційна діяльність як об'єкт небезпеки

Сутність, поняття та правове визначення поняття «інформаційна діяльність». Складові інформаційної діяльності. Засоби та їх структура здійснення інформаційної діяльності. Інформаційні ресурси: поняття, основні функції, ієрархічні рівні. Інформаційний ресурс як об'єкт інформаційної небезпеки. Взаємозв'язок інформаційної діяльності та інформаційної безпеки. Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства. Перспективи та напрями розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки.

Тема 7. Інформаційна агресія: виклики для національного та міжнародного права

Сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя». Маніпулювання свідомістю, сутність та види маніпуляції. Роль та місце маніпулювання в національних системах державного управління та політичних системах, а також у формуванні та здійсненні міжнародних стосунків. Сутність та прояви інформаційного насильства. Проблемні питання правового запобігання здійсненню інформаційного насильства.

Тема 8. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки

Поняття кіберзлочинності. Конвенція Ради Європи «Про кіберзлочинність» від 23.11.01 р. № 994-575. Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Європейському Союзі.

4. Структура вивчення навчальної дисципліни

4.1. Тематичний план навчальної дисципліни

№ теми	Назва теми	Кількість годин											
		Денна форма навчання						Заочна форма навчання					
		Усього	у тому числі					Усього	у тому числі				
			Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС		Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	Концептуальні засади інформаційної безпеки	10	2	1	–	–	7	10	1	–	–	–	9
2.	Інтереси держави в інформаційній сфері	10	2	1	–	–	7	10	1	–	–	–	9
3.	Загрози людині та суспільству в інформаційній сфері	11	2	2	–	–	7	13	2	2	–	–	9
4.	Інтернет та інформаційна безпека	11	2	2	–	–	7	13	2	2	–	–	9
5.	Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки	12	2	2	–	–	8	10	–	–	–	–	10
6.	Інформаційна діяльність як об'єкт небезпеки	12	2	2	–	–	8	10	–	–	–	–	10
7.	Інформаційна агресія: виклики для національного та міжнародного права.	12	2	2	–	–	8	14	2	2	–	–	10
8.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки	12	2	2	–	–	8	10	–	–	–	–	10
	Усього годин:	90	16	14	–	–	60	90	8	6	–	–	76

4.2. Аудиторні заняття

4.2.1. Аудиторні заняття (лекції, семінарські заняття) проводяться згідно з темами та обсягом годин, передбачених тематичним планом.

4.2.2. Плани лекцій з передбачених тематичним планом тем визначаються в підрозділі 1.2 навчально-методичних матеріалів з дисципліни.

4.2.3. Плани семінарських (практичних, лабораторних) занять з передбачених тематичним планом тем, засоби поточного контролю знань та методичні рекомендації для підготовки до занять визначаються в підрозділі 1.3 навчально-методичних матеріалів з дисципліни.

4.3. Самостійна робота студентів

4.3.1. Самостійна робота студентів денної форми навчання включає завдання до кожної теми та індивідуальні завдання.

4.3.2. Завдання для самостійної роботи студентів та методичні рекомендації до їх виконання визначаються в підрозділі 1.4 навчально-методичних матеріалів з дисципліни.

4.3.3. Студенти денної форми навчання виконують індивідуальні завдання у формі реферату.

4.3.4. Тематика індивідуальних завдань та методичні рекомендації до їх виконання визначаються в підрозділі 1.5 навчально-методичних матеріалів з дисципліни.

4.3.5. Індивідуальні завдання виконуються в межах часу, визначеного для самостійної роботи студентів, та оцінюються частиною визначених в розділі 6 цієї програми кількості балів, виділених для самостійної роботи.

5. Методи навчання та контролю

Під час лекційних занять застосовуються:

1) традиційний усний виклад змісту теми;
2) слайдова презентація.

На семінарських та практичних заняттях застосовуються:

- дискусійне обговорення проблемних питань;
- вирішення тестових завдань;
- повідомлення про виконання індивідуальних завдань;
- розв'язування творчих завдань, проведення аналітичних досліджень, складання графічних схем, таблиць, діаграм, тощо.

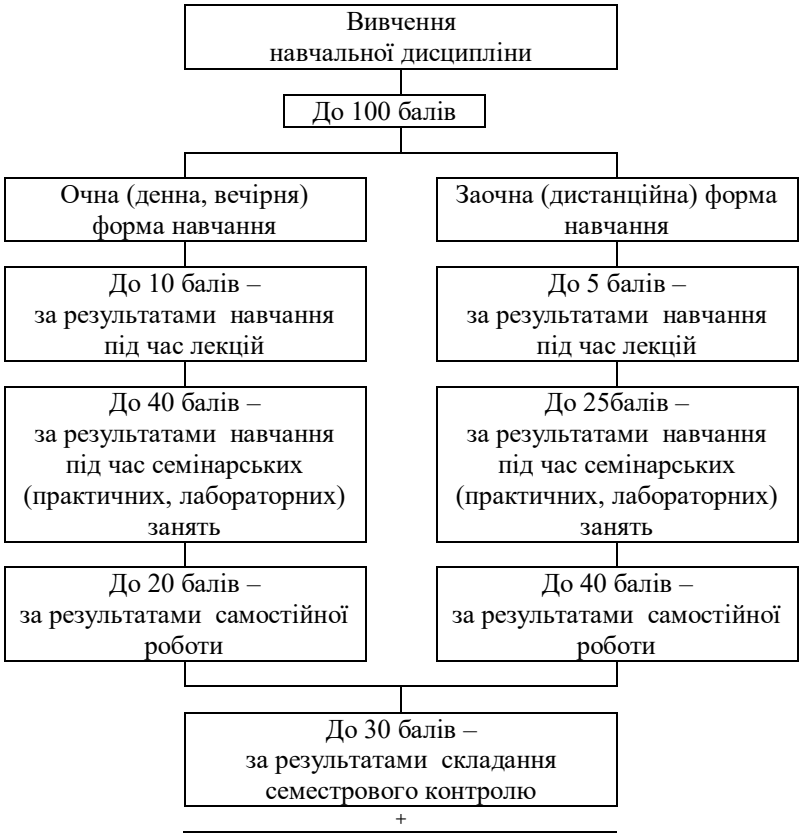
Поточний контроль знань студентів з навчальної дисципліни проводиться у формах:

1) усне або письмове (у тому числі тестове) бліц-опитування студентів щодо засвоєння матеріалу попередньої лекції, експрес-опитування на лекціях;
2) усне або письмове (у тому числі тестове) опитування на семінарських заняттях;
3) виконання поточних контрольних робіт у формі тестування.

Підсумковий семестровий контроль проводиться у формі письмового тестування.

6. Схема нарахування балів

6.1. Нарахування студентам балів за результатами навчання здійснюється за схемою, наведеною на рис.



6.2. Обсяг балів, здобутих здобувачем вищої освіти під час лекцій з навчальної дисципліни, визначається у пропорційному співвідношенні до кількості відвіданих лекцій. Загальна кількість балів визначається за формулою:

$$\sum л = Фл / Пл \times Max,$$

де: ∑л – загальна сума балів;

Фл – кількість фактично відвіданих лекцій;

Пл – планова кількість лекцій, визначена робочою програмою;

Мах – максимальна кількість балів, яку здобувач вищої освіти може отримати за роботу на лекціях.

З цієї навчальної дисципліни передбачено проведення 8 лекційних занять за денною формою навчання, 4 – за заочною формою навчання.

6.3. З цієї навчальної дисципліни передбачено проведення 7 семінарських занять за денною формою навчання, 3 – за заочною формою навчання.

№ з/п	Форма навчання	Кількість лекцій за планом	Кількість відвіданих лекцій							
			1	2	3	4	5	6	7	8
1.	Денна	8	1	2	3,5	5	6,5	7	8,5	10
2.	Заочна	4	2,5	5,0	7,5	10				

Обсяг балів, здобутих здобувачем вищої освіти під час семінарських (практичних, лабораторних) занять з навчальної дисципліни, визначається за формулою:

$$\sum c = (Б1+Б2+\ldots+Бn) / n \times К,$$

де: ∑с – загальна сума балів;

Б – кількість балів, отриманих на одному занятті;

n – кількість семінарських (практичних, лабораторних) занять, визначених робочою програмою;

К – коефіцієнт, який, як правило, дорівнює 9.

Коефіцієнт К може бути іншим з урахуванням специфіки навчальної дисципліни.

За результатами семінарського (практичного, лабораторного) заняття кожному здобувачеві вищої освіти до відповідного документа обліку успішності виставляється кількість балів від 0 до 5 числом, кратним 0,5, яку він отримав протягом заняття.

Бали заносяться до документів обліку успішності здобувачів вищої освіти науково-педагогічним працівником, який провів заняття, одразу після його завершення.

Критерії поточного оцінювання знань студентів наведені у п. 4.3. Положення про організацію освітнього процесу в Хмельницькому університеті управління та права імені Леоніда Юзькова (в редакції, затвердженій рішення вченої ради ХУУП імені Леоніда Юзькова від 28 серпня 2020 року, протокол № 1).

7. Рекомендовані джерела

7.1. Основні джерела

1. Інформаційна безпека та кібербезпека держави: навчальний посібник/ Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська.- Київ: Ліра-К, 2025. - 224 с.
2. Правове забезпечення інформаційної безпеки : курс лекцій / В. Фурашев, О. Радзієвська ; ДНУ «Ін-т інформ., безпеки і права Нац. акад. прав. наук України». – Київ; Одеса : Фенікс, 2022. 158 с. URL: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoibezpeki
3. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації: навчальний посібник / О. Довгань , Н. Ткачук , Т. Ткачук , В. Петров. – К., Артек. 2022. 171 с. URL: https://ippi.org.ua/pravovi-zasadi-zabezpechennya-kiberbezpeki-v-umovakh-tsifrovoitransformatsii
4. 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. URL: https://ippi.org.ua/zakhist-

pravprivatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu
5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. URL: https://ippi.org.ua/kiberbezpeka-vinformatsiinomu-suspilstvi
6. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

7.2. Допоміжні джерела

1. Права людини: інформаційний вимір: монографія / О.О. Тихомиров. – Одеса: Видавництво «Юридика», 2023. 304 с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf
2. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О. П. Дзьобаня. – Харків: Право, 2021. – 776 с. URL: http://ippi.org.ua/natsionalna- bezpeka-svitoglyadni-ta-teoretiko-metodologichni-zasadi
3. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології. / Арістова І.В., Баранов О.А., Дзьобань О.П. та ін.; за заг. ред. проф. К.І. Бєлякова: монографія. – Київ: КВІЦ, 2019. 344 с. (Розділ 4. Характеристика галузевих видів юридичної відповідальності за інформаційні делікти.) URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf
4. Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони/ збірник документів і матеріалів / Упорядники: Беланюк М.В., Доронін І.М., Лебединська О.В., Радзієвська О.Г., Пилипчук В.Г., Шамара О.В., Фурашев В.М. – К.: Видавничий дім «АртЕк». 2020. 756 с. URL: http://ippi.org.ua/sites/default/files/verstka_zbirnuk_zakoniv.pdf
5. Інформаційне та соціально-правове моделювання: посібник / Д. В. Ланде, В. М. Фурашев; за заг. ред. Д. В. Ланде. – Київ-Одеса : Фенікс, 2021. – 276 с. - URL: http://ippi.org.ua/sites/default/files/posibnik.pdf
6. Кібербезпека «суспільства знань»: монографія/ Довгань О., Тарасюк А., Ткачук Т. : монографія. – Київ-Одеса : Фенікс, 2021. – 176 с. URL: http://ippi.org.ua/kiberbezpeka- %C2%ABsuspilstva-znan%C2%BB
7. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія / Н. Уханова; за заг. ред. В. Пилипчука. – Київ- Одеса: Фенікс, 2022. 140 с. URL: http://ippi.org.ua/problemi-protidiinegativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus
8. Соціальні та цифрові трансформації: нова парадигма кібербезпеки. Монографія. / О. А. Баранов. – Київ: 2021. 86 с. URL: https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsiinova-paradigma-kiberbezpeki
9. Трансформація: соціальна & цифрова & правова: монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату / О. А. Баранов. – Одеса:

Видавничий дім «Гельветика», 2022. 272 с. URL: https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova

Для пошуку іншої необхідної літератури та нормативно-правових актів

8. Інформаційні ресурси в Інтернеті

1. http://www.rada.gov.ua - Веб-портал Верховної Ради України
2. http://www.president.gov.ua - Веб-портал Адміністрації Президента України
3. http://www.kmu.gov.ua - Веб-портал Кабінету Міністрів України
4. http://mon.gov.ua - Веб-сайт Міністерства освіти і науки України
5. http://nbuv.gov.ua/ - Веб-сайт Національної бібліотеки України імені В.І. Вернадського
6. http://gntb.gov.ua/ua/ - Веб-сайт державної науково-технічної бібліотеки України
7. http://www.ounb.km.ua/ - Веб-сайт Хмельницької обласної універсальної наукової бібліотеки