



**ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА**  
**ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА**

---

**ЗАТВЕРДЖЕНО**

Рішення вченої ради університету  
25 червня 2026 року,  
протокол № 13

Т.в.о. ректора, голова вченої ради  
університету, доктор юридичних наук,  
професор



Олег ОМЕЛЬЧУК

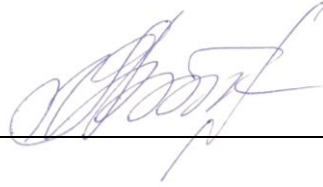
25 червня 2026 року

М.П.

**РОБОЧА ПРОГРАМА**  
**навчальної дисципліни**  
**«ІНФОРМАЦІЙНА БЕЗПЕКА»**  
**для підготовки на другому освітньому рівні**  
**здобувачів вищої освіти ступеня магістр**  
**за спеціальністю D8 Право**  
**галузі знань D Бізнес, адміністрування та право**  
**Освітня програма «Магістр права»**

**РОЗРОБНИК:**

Професор кафедри конституційного,  
адміністративного та фінансового права,  
кандидат юридичних наук, професор  
17 червня 2026 року



Ірина СТОРОЖУК

**СХВАЛЕНО**

Рішення кафедри конституційного,  
адміністративного та фінансового права  
17 червня 2026 року, протокол № 13.

Завідувач кафедри конституційного,  
адміністративного та фінансового права,  
доцент  
17 червня 2026 року



Олена ГАЛУС

**ПОГОДЖЕНО:**

Гарант освітньої програми  
18 червня 2026 року



Сергій КРУШИНСЬКИЙ

Декан юридичного факультету,  
кандидат юридичних наук, доцент  
18 червня 2026 року



Віктор ЗАХАРЧУК

Рішення методичної ради університету  
18 червня 2026 року, протокол № 8.

Голова методичної ради університету,  
кандидатка наук з державного  
управління, доцентка  
18 червня 2026 року



Ірина КОВТУН

## ЗМІСТ

|                                             | Стор. |
|---------------------------------------------|-------|
| 1. Опис навчальної дисципліни               | — 4   |
| 2. Заплановані результати навчання          | — 5   |
| 3. Програма навчальної дисципліни           | — 6   |
| 4. Структура вивчення навчальної дисципліни | — 8   |
| 4.1. Тематичний план навчальної дисципліни  | — 8   |
| 4.2. Аудиторні заняття                      | — 8   |
| 4.3. Самостійна робота студентів            | — 8   |
| 5. Методи навчання та контролю              | — 9   |
| 6. Схема нарахування балів                  | — 9   |
| 7. Рекомендована література                 | — 10  |
| 7.1. Основна література                     | — 10  |
| 7.2. Допоміжна література                   | — 10  |
| 8. Інформаційні ресурси в Інтернеті         | — 11  |

## 1. Опис навчальної дисципліни

- |                                                                |                                                                                                                                                                                                           |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Шифр і назва галузі знань                                   | – D Бізнес, адміністрування та право                                                                                                                                                                      |
| 2. Код і назва спеціальності                                   | – D8 Право                                                                                                                                                                                                |
| 3. Назва спеціалізації                                         | – спеціалізація не передбачена                                                                                                                                                                            |
| 4. Назва дисципліни                                            | – Медичне право                                                                                                                                                                                           |
| 5. Тип дисципліни                                              | – вибіркова                                                                                                                                                                                               |
| 6. Освітній рівень, на якому вивчається дисципліна             | – другий                                                                                                                                                                                                  |
| 7. Ступінь вищої освіти, що здобувається                       | – магістр                                                                                                                                                                                                 |
| 8. Загальний обсяг вивчення дисципліни (кредитів ЄКТС / годин) | – 3 / 90                                                                                                                                                                                                  |
| 9. Форма семестрового контролю                                 | – залік                                                                                                                                                                                                   |
| 10. Місце дисципліни в логічній схемі:                         | – Практика цивільного судочинства<br>Теорія і практика адміністративного судочинства<br>Застосування Конвенції про захист прав людини та основоположних свобод<br>Альтернативне вирішення правових спорів |
| 11. Мова вивчення дисципліни                                   | – українська.                                                                                                                                                                                             |

## 2. Заплановані результати навчання

|                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Програмні компетентності, які здобуваються під час вивчення навчальної дисципліни</b></p> | <p><b>Загальні компетентності</b></p> <p>ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу;<br/> ЗК 3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел;<br/> ЗК 6. Здатність генерувати нові ідеї (креативність);<br/> ЗК 7. Здатність приймати обґрунтовані рішення;<br/> ЗК 8. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань);<br/> ЗК 9. Здатність працювати в міжнародному контексті.</p> <p><b>Спеціальні компетентності</b></p> <p>СК 1. Здатність застосовувати принципи верховенства права для розв'язання складних задач і проблем, у тому числі, у ситуаціях правової невизначеності;<br/> СК 6. Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію;<br/> СК 8. Здатність застосовувати медіацію та інші правові інструменти альтернативного позасудового розгляду та вирішення правових спорів;<br/> СК 9. Здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності;<br/> СК 10. Здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування;<br/> СК 13. Здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією..</p> |
| <p><b>Програмні результати навчання</b></p>                                                     | <p>РН 1. Оцінювати природу та характер суспільних процесів і явищ, і виявляти розуміння меж та механізмів їх правового регулювання;<br/> РН 2. Співвідносити сучасну систему цивілізаційних цінностей з правовими цінностями, принципами та професійними етичними стандартами;<br/> РН 3. 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;<br/> РН 6. Обґрунтовано формулювати свою правову позицію, вміти опонувати, оцінювати докази та наводити переконливі аргументи;<br/> РН 7. Дискутувати зі складних правових проблем, пропонувати і обґрунтовувати варіанти їх розв'язання;<br/> РН 10. Аналізувати взаємодію міжнародного права та міжнародно-правових систем з правовою системою України на основі усвідомлення основних сучасних правових доктрин, цінностей та принципів функціонування права;<br/> РН 13. Аналізувати та оцінювати практику застосування окремих правових інститутів;<br/> РН 14. Обґрунтовувати правову позицію на різних стадіях правозастосування;<br/> РН 17. Інтегрувати необхідні знання та розв'язувати складні задачі правозастосування у різних сферах професійної діяльності.</p>                                                                                                          |

### **3. Програма навчальної дисципліни**

#### ***Тема 1. Концептуальні засади інформаційної безпеки***

Поняття, сутність та принципи 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

Інформаційна безпека в системі національної безпеки України. Національні інтереси та загрози в інформаційній сфері. Інформаційний суверенітет держави. Державна інформаційна політика та її безпекова складова. Стратегія інформаційної безпеки України. Правові механізми забезпечення інформаційної безпеки. Формування та захист національного інформаційного простору. Інформаційна безпека в умовах цифрової трансформації. Міжнародно-правові стандарти забезпечення інформаційної безпеки.

#### ***Тема 2. Інформаційний вплив та його значення***

Поняття та сутність інформаційного впливу. Види, форми та механізми здійснення інформаційного впливу. Суб'єкти та об'єкти інформаційного впливу. Інформаційний вплив як інструмент реалізації державної інформаційної політики. Роль засобів масової інформації та цифрових платформ у формуванні суспільної свідомості. Позитивний і деструктивний інформаційний вплив. Інформаційний вплив в умовах інформаційного суспільства та цифрової трансформації. Інформаційно-психологічний вплив і його наслідки для особи, суспільства та держави. Правові механізми протидії маніпуляціям, пропаганді та дезінформації. Значення інформаційного впливу для забезпечення національної та інформаційної безпеки.

#### ***Тема 3. Загрози безпеці держави в інформаційній сфері***

Поняття та класифікація загроз безпеці держави в інформаційній сфері. Національні інтереси України в інформаційній сфері та фактори їх вразливості. Внутрішні й зовнішні загрози інформаційній безпеці держави. Дезінформація, пропаганда та інформаційно-психологічні операції як інструменти гібридного впливу. Кіберзагрози та їх вплив на функціонування державних інформаційних ресурсів і критичної інфраструктури. Загрози інформаційному суверенітету та інформаційному простору держави. Маніпулювання суспільною свідомістю та поширення фейкової інформації. Загрози у сфері захисту державної таємниці та інформації з обмеженим доступом. Державна політика щодо виявлення, попередження та нейтралізації інформаційних загроз. Правові та організаційні механізми забезпечення інформаційної безпеки держави в умовах воєнного стану та цифрової трансформації.

#### ***Тема 4. Загрози в інформаційній безпеці суспільства***

Поняття та сутність загроз інформаційній безпеці суспільства. Інформаційна безпека суспільства як складова національної безпеки. Основні джерела та види загроз в інформаційному середовищі. Дезінформація, пропаганда, маніпулювання громадською думкою та поширення фейкової інформації. Інформаційно-психологічний вплив на суспільну свідомість. Роль соціальних мереж і цифрових платформ у поширенні інформаційних загроз. Вплив інформаційних загроз на суспільну стабільність, демократичні процеси та громадську довіру. Інформаційна культура та медіаграмотність як засоби протидії інформаційним загрозам. Діяльність державних інституцій та інститутів громадянського суспільства у сфері забезпечення інформаційної безпеки суспільства. Правові та організаційні механізми захисту суспільства від негативних інформаційних впливів в умовах цифровізації та воєнного стану.

### ***Тема 5. Загрози людині в інформаційній сфері***

Поняття та сутність загрози людині в інформаційній сфері. Інформаційні права і свободи людини як об'єкт правового захисту. Інформаційно-психологічний вплив на особу та його наслідки. Дезінформація, маніпулювання свідомістю та пропаганда як загрози інформаційній безпеці людини. Порушення права на приватність та захист персональних даних. Кібербулінг, онлайн-шахрайство та інші форми протиправної діяльності в цифровому середовищі. Загрози інформаційній безпеці дітей та вразливих категорій населення. Вплив соціальних мереж і цифрових платформ на формування світогляду та поведінки людини. Правові механізми захисту особи від негативних інформаційних впливів. Державні та міжнародні гарантії забезпечення інформаційної безпеки людини в умовах цифрового суспільства.

### ***Тема 6. Інформаційна діяльність як об'єкт небезпеки***

Поняття інформаційної діяльності та її роль у сучасному інформаційному суспільстві. Інформаційна діяльність як об'єкт правового регулювання та захисту. Ризики та загрози, пов'язані зі збиранням, зберіганням, використанням і поширенням інформації. Незаконне втручання в інформаційну діяльність та його наслідки. Порушення цілісності, достовірності, конфіденційності та доступності інформації. Кіберзагрози як фактор небезпеки для інформаційної діяльності. Зловживання інформацією, маніпуляції та дезінформація в процесі інформаційної діяльності. Загрози функціонуванню державних інформаційних ресурсів та інформаційних систем. Правові механізми забезпечення безпеки інформаційної діяльності. Державний контроль і відповідальність за порушення законодавства у сфері інформаційної діяльності.

### ***Тема 7. Захист персональних даних та цифрова безпека***

Поняття персональних даних та їх місце в системі інформаційних прав людини. Правові засади захисту персональних даних в Україні та Європейському Союзі. Принципи обробки персональних даних і гарантії дотримання права на приватність. Суб'єкти правовідносин у сфері захисту персональних даних та їх права й обов'язки. Загрози персональним даним у цифровому середовищі. Цифрова безпека як складова інформаційної безпеки особи, суспільства та держави. Кіберінциденти, витоки даних та несанкціонований доступ до інформації. Організаційно-правові та технічні заходи забезпечення цифрової безпеки. Міжнародні стандарти захисту персональних даних та кібербезпеки. Відповідальність за порушення законодавства у сфері захисту персональних даних і цифрової безпеки.

### ***Тема 8. Штучний інтелект та ризики інформаційної безпеки***

Поняття та сутність штучного інтелекту в умовах цифрового суспільства. Правові та етичні аспекти використання технологій штучного інтелекту. Штучний інтелект як фактор трансформації інформаційного простору. Ризики використання штучного інтелекту для інформаційної безпеки особи, суспільства та держави. Генерація дезінформації, дипфейки та маніпулювання суспільною свідомістю за допомогою систем штучного інтелекту. Загрози приватності та захисту персональних даних при використанні технологій штучного інтелекту. Використання штучного інтелекту у кіберпросторі та пов'язані з ним кіберзагрози. Міжнародні та європейські підходи до правового регулювання штучного інтелекту. Правові механізми мінімізації ризиків штучного інтелекту та забезпечення інформаційної безпеки.

### ***Тема 9. Інформаційна агресія: виклики для національного та міжнародного права***

Поняття та сутність інформаційної агресії. Форми та інструменти здійснення інформаційної агресії. Інформаційна агресія як загроза національній безпеці. Конституційно-правові засади протидії інформаційній агресії в Україні. Інформаційна агресія у системі міжнародного права та міжнародної безпеки. Міжнародні стандарти та механізми реагування на інформаційні загрози. Інформаційний суверенітет держави та його захист. Баланс між свободою слова та протидією інформаційній агресії. Відповідальність держав та недержавних акторів за інформаційні злочини. Перспективи формування універсальних правових механізмів протидії інформаційній агресії.

#### 4. Структура вивчення навчальної дисципліни

##### 4.1. Тематичний план навчальної дисципліни

| №<br>те-<br>ми | Назватемі                                                             | Кількістьгодин     |            |                 |        |         |     |                     |            |                 |        |         |     |
|----------------|-----------------------------------------------------------------------|--------------------|------------|-----------------|--------|---------|-----|---------------------|------------|-----------------|--------|---------|-----|
|                |                                                                       | Деннаформанавчання |            |                 |        |         |     | Заочнаформанавчання |            |                 |        |         |     |
|                |                                                                       | Усього             | утомучислі |                 |        |         |     | Усього              | утомучислі |                 |        |         |     |
|                |                                                                       |                    | Лекції     | Сем.<br>(прак). | Лабор. | Ін.зав. | СРС |                     | Лекції     | Сем.<br>(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          | 2               | –      | –       | 6   | 10                  | 1          | –               | –      | –       | 9   |
| 2.             | Інформаційний вплив та його значення                                  | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 1          | –               | –      | –       | 9   |
| 3.             | Загрози безпеці держави в інформаційній сфері                         | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 2          | 2               | –      | –       | 6   |
| 4.             | Загрози в інформаційній безпеці суспільства                           | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 1          | 2               | –      | –       | 7   |
| 5.             | Загрози людині в інформаційній сфері                                  | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 1          | 2               | –      | –       | 7   |
| 6.             | Загрози інформаційній безпеці в інформаційно–комунікаційних мережах   | 10                 | 2          | 2               |        | –       | 6   | 10                  | 1          | –               | –      | –       | 9   |
| 7.             | Захист персональних даних та цифрова безпека                          | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 1          | –               | –      | –       | 9   |
| 8.             | Штучний інтелект та ризики інформаційної безпеки                      | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 1          | –               | –      | –       | 9   |
| 9.             | Інформаційна агресія: виклики для національного та міжнародного права | 10                 | 2          | 2               | –      | –       | 6   | 10                  | 1          | –               | –      | –       | 9   |
|                | Усьогогодин:                                                          | 90                 | 18         | 18              | –      | –       | 54  | 90                  | 10         | 6               | –      | –       | 74  |

#### 4.2. Аудиторні заняття

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

4.2.2. Плани лекцій з передбачених тематичним планом тем визначаються в силабусі навчальної дисципліни.

4.2.3. Плани семінарських (практичних) занять з передбачених тематичним планом тем, засоби поточного контролю знань визначаються в силабусі навчальної дисципліни.

#### 4.3. Самостійна робота студентів

4.3.1. Самостійна робота студентів включає опрацювання завдань до кожної теми та виконання індивідуальних завдань.

4.3.2. Завдання для самостійної роботи студентів, а також порядок здобуття балів за самостійну роботу визначаються в силабусі навчальної дисципліни.

## 5. Методи навчання та контролю

Під час лекційних занять застосовуються:

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

На семінарських (практичних) заняттях застосовуються:

- 1) дискусійне обговорення проблемних питань;
- 2) вирішення ситуаційних завдань;
- 3) складання та розгляд окремих процесуальних документів.

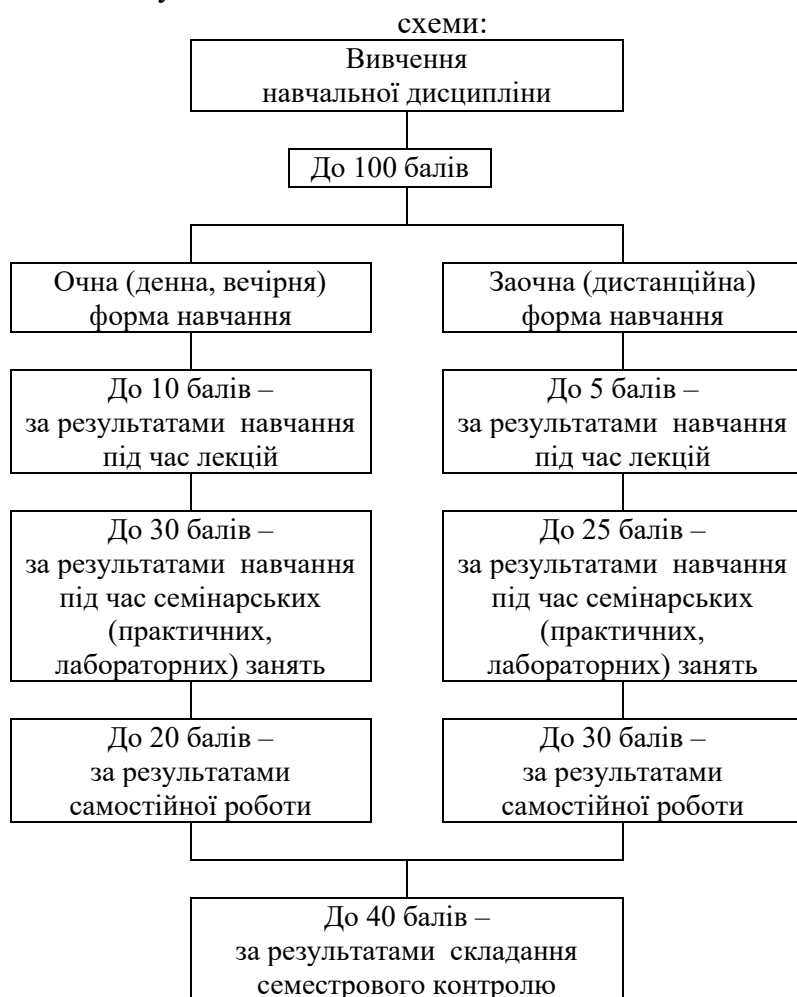
Поточний контроль знань студентів з навчальної дисципліни проводиться у таких формах:

- 1) усне або письмове опитування на семінарських заняттях;
- 2) перевірка виконання поточних контрольних робіт у формі тестування;
- 3) розв'язування творчих завдань, проведення дискусій тощо;
- 4) захист підготовленого індивідуального завдання.

Підсумковий семестровий контроль проводиться у формі заліку. Залікова оцінка виставляється на підставі результатів поточного оцінювання або складання заліку, який проводиться у формі тестування. У випадку необхідності проведення заліку онлайн, він проводиться у формі тестування із застосуванням комп'ютерних технологій в режимі реального часу.

## 6. Схема нарахування балів

6.1. Нархування балів студентам з навчальної дисципліни здійснюється відповідно до такої



6.2. Обсяг балів, здобутих студентами під час лекцій, семінарських занять, самостійної роботи студентів визначаються у силабусі з дисципліни.

## **7. Рекомендовані джерела**

### **7.1. Основні джерела**

1. Титова Н. М., Рідей Н. М., Настрадін В. П., Присяжнюк М. М., Мамченко С. М., Артюх С. В., Яворська Р. О. Інформаційна безпека та кібербезпека держави : навч. посіб. Київ : Ліра-К, 2025. 224 с.
2. Фурашев В., Радзієвська О. Правове забезпечення інформаційної безпеки : курс лекцій / 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-informatsiinoi-bezpeki>
3. Довгань О., Ткачук Н., Ткачук Т., Петров В. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації : навч. посіб. Київ : Арттек, 2022. 171 с. URL: <https://ippi.org.ua/pravovi-zasadi-zabezpechennya-kiberbezpeki-v-umovakh-tsifrovoi-transformatsii>
4. Пилипчук В. Г., Брижко В. М., Доронін І. М. та ін. 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. URL: <https://ippi.org.ua/zakhist-prav-privatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu>
5. Довгань О., Литвинова Л., Дорогих С. Кібербезпека в інформаційному суспільстві : інформ.-аналіт. дайджест / відп. ред. О. Довгань ; Держ. наук. установа «Ін-т інформ., безпеки і права НАПрН України» ; Нац. б-ка України ім. В. І. Вернадського. URL: <https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi>
6. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. та ін. Інформаційна безпека : підручник / під ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.

### **7.2. Допоміжні джерела**

1. Тихомиров О. О. Права людини: інформаційний вимір : монографія. Одеса : Юридика, 2023. 304 с. URL: [http://ippi.org.ua/sites/default/files/tihomirov\\_o.o.\\_prava\\_lyudini\\_monografiya.pdf](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. Арістова І. В., Баранов О. А., Дзьобань О. П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія / за заг. ред. проф. К. І. Белякова. Київ : КВІЦ, 2019. 344 с. URL: [http://ippi.org.ua/sites/default/files/monografiya\\_ok\\_0.pdf](http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf)
4. Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони : зб. док. і матеріалів / упоряд. М. В. Беланюк, І. М. Доронін, О. В. Лебединська, О. Г. Радзієвська, В. Г. Пилипчук, О. В. Шамара, В. М. Фурашев. Київ : АртЕк, 2020. 756 с. URL: [http://ippi.org.ua/sites/default/files/verstka\\_zbirnuk\\_zakoniv.pdf](http://ippi.org.ua/sites/default/files/verstka_zbirnuk_zakoniv.pdf)
5. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання : посіб. / за заг. ред. Д. В. Ланде. Київ ; Одеса : Фенікс, 2021. 276 с. URL: <http://ippi.org.ua/sites/default/files/posibnik.pdf>
6. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань» : монографія. Київ ; Одеса : Фенікс, 2021. 176 с. URL: <http://ippi.org.ua/kiberbezpeka-%C2%ABsuspilstva-znan%C2%BB>
7. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства : монографія / за заг. ред. В. Пилипчука. Київ ; Одеса : Фенікс, 2022. 140 с. URL: <http://ippi.org.ua/problemsi-protidii-negativnim-informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus>

8. Баранов О. А. Соціальні та цифрові трансформації: нова парадигма кібербезпеки : монографія. Київ, 2021. 86 с. URL: <https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsii-nova-paradigma-kiberbezpeki>
9. Баранов О. А. Трансформація: соціальна & цифрова & правова : монографія у 3 т. Т. 1 : Порятунк цивілізації: економіка результату. Одеса : Гельветика, 2022. 272 с. URL: <https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova>

#### **8. Інформаційні ресурси в Інтернеті**

- |    |                                                                         |                                                                                                                               |
|----|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1. | <a href="http://www.rada.gov.ua">http://www.rada.gov.ua</a>             | Веб-портал Верховної Ради України                                                                                             |
| 2. | <a href="https://www.president.gov.ua">https://www.president.gov.ua</a> | Офіційне інтернет-представництво Президента України                                                                           |
| 3. | <a href="https://dsszzi.gov.ua">https://dsszzi.gov.ua</a>               | Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України                                            |
| 4. | <a href="https://cert.gov.ua">https://cert.gov.ua</a>                   | Офіційний сайт Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA)                                 |
| 5. | <a href="https://ippi.org.ua">https://ippi.org.ua</a>                   | Офіційний сайт Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» |
| 6. | <a href="https://nrada.gov.ua">https://nrada.gov.ua</a>                 | Офіційний сайт Національної ради України з питань телебачення і радіомовлення                                                 |
| 7. | <a href="https://www.president.gov.ua">https://www.president.gov.ua</a> | Офіційне інтернет-представництво Президента України                                                                           |