



Вищий навчальний заклад  
«НАЦІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ»  
Юридичний факультет  
Кафедра публічного та приватного права

**ЗАТВЕРДЖЕНО**

Декан юридичного факультету



Наталія ВЕСЕЛОВСЬКА

**РОБОЧА ПРОГРАМА**

**ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ  
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ**

(назва навчальної дисципліни)

підготовки другого (магістерського) рівня вищої освіти  
(назва рівня вищої освіти)

галузі знань D «Бізнес, адміністрування та право»  
(шифр і назва галузі знань)

спеціальності D8 «Право»  
(код і найменування спеціальності)

освітньої програми «Право»  
(назва освітньо-професійної програми)

тип дисципліни вибіркова

**2025 рік**

**ПОГОДЖЕНО:**

Гарант освітньої програми



(підпис)

Наталія ВЕСЕЛОВСЬКА  
(прізвище, ініціали)

**РЕКОМЕНДОВАНО:**

Кафедрою публічного та приватного права  
протокол № 1  
від «28» серпня 2025 року

Завідувач кафедри



(підпис)

Ірина КОЗАКОВА  
(прізвище, ініціали)

**Укладач:** *Чернявська Богдана Вадимівна*, доктор філософії у галузі права.

## 1. Опис навчальної дисципліни

**Мова навчання:** українська

**Статус дисципліни:** вибіркова

**Передумови вивчення навчальної дисципліни:** вивчення дисципліни *«Правові засади забезпечення інформаційної безпеки України»* доцільне після оволодіння здобувачами вищої освіти базовими знаннями з основ теорії держави і права, конституційного права України, адміністративного права України, цивільного права України, трудового права, фінансового права України, міграційного права, права інтелектуальної власності.

**Предметом** вивчення навчальної дисципліни *«Правові засади забезпечення інформаційної безпеки України»* є суспільні відносини, що виникають у процесі формування, реалізації та захисту інформаційної безпеки держави, зокрема у сфері створення, збирання, зберігання, обробки, поширення та захисту інформації, протидії інформаційним загрозам, кіберзагрозам і дезінформації, а також правові, організаційні та інституційні механізми забезпечення національних інтересів України в інформаційній сфері відповідно до Конституції України та чинного законодавства.

**Інформаційний обсяг навчальної дисципліни.** На вивчення навчальної дисципліни відводиться 120 годин (4 кредити ECTS).

## 2. Мета та завдання навчальної дисципліни

**Метою** викладання навчальної дисципліни *«Правові засади забезпечення інформаційної безпеки України»* є формування у здобувачів вищої освіти фундаментальних правових знань, навичок необхідних для забезпечення обігу та захисту інформації, розуміння напрямків інформаційної діяльності у забезпеченні державної інформаційної політики, з'ясування сучасних інформаційних загроз та напрямків їх протидії, розуміння тенденцій безпекового розвитку сучасного інформаційного суспільства.

**Основними завданнями** навчальної дисципліни *«Правові засади забезпечення інформаційної безпеки України»* є оволодіння теоретико-правовими засадами інформаційної безпеки та її місцем у системі національної безпеки України; вивчення правових основ обігу, зберігання, захисту та використання інформації; аналіз державної інформаційної політики та правових механізмів її реалізації; дослідження сучасних інформаційних загроз, кіберзагроз і дезінформації та правових засобів протидії їм; з'ясування правового режиму інформаційних ресурсів і систем, у тому числі з обмеженим доступом; аналіз повноважень органів державної влади у сфері забезпечення інформаційної безпеки; формування навичок застосування норм інформаційного, адміністративного та кримінального законодавства у сфері захисту інформації; вивчення міжнародних і європейських стандартів забезпечення інформаційної безпеки та їх імплементації в Україні; розвиток здатності правової оцінки інформаційних ризиків і безпекових викликів у сучасному інформаційному суспільстві.

### **3. Компетентності та заплановані результати навчання**

Дисципліна «Правові засади забезпечення інформаційної безпеки України» забезпечує набуття здобувачами освіти **компетентностей**:

#### **Загальні компетентності (ЗК):**

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

#### **Спеціальні (фахові) компетентності (СК):**

СК3. Здатність аналізувати та оцінювати вплив Конвенції про захист прав людини та основоположних свобод, а також практики Європейського суду з прав людини на розвиток правової системи та правозастосування в Україні.

СК4. Здатність оцінювати взаємодію міжнародного права та міжнародних правових систем з правовою системою України.

СК5. Здатність використовувати сучасні правові доктрини та принципи у правотворчості та в процесі застосування інститутів публічного і приватного права, а також кримінальної юстиції.

СК6. Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію.

СК7. Здатність застосовувати знання та розуміння основних засад (принципів) та процедур судочинства в Україні.

СК8. Здатність застосовувати медіацію та інші правові інструменти альтернативного позасудового розгляду та вирішення правових спорів.

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.

СК12. Здатність розвивати та утверджувати етичні стандарти правничої діяльності, стандарти професійної незалежності та відповідальності правника.

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

#### **Програмні результати навчання (ПРН):**

ПРН 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.

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

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

ПРН 6. Обґрунтовано формулювати свою правову позицію, вміти опонувати, оцінювати докази та наводити переконливі аргументи.

ПРН 7. Дискутувати зі складних правових проблем, пропонувати і обґрунтовувати варіанти їх розв'язання.

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

#### 4. Структура навчальної дисципліни

| Назви змістових модулів і 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 |
| 1                                                                      | 2               | 3            | 4    | 5  | 6    | 7    | 8            | 9            | 10   | 11 | 12   | 13   |
| <b>Змістовий модуль 1.</b>                                             |                 |              |      |    |      |      |              |              |      |    |      |      |
| ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 12              | 2            | 2    |    |      | 8    | 12           | 1            | 1    |    |      | 10   |
| ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 14              | 2            | 2    |    |      | 10   | 12           | 1            | 1    |    |      | 10   |
| ТЕМА 3. Правове регулювання обігу інформації та електронне урядування. | 14              | 2            | 2    |    |      | 10   | 12           | 1            | 1    |    |      | 10   |
| ТЕМА 4. Інформація з обмеженим доступом та державна таємниця.          | 14              | 2            | 2    |    |      | 10   | 12           | 1            | 1    |    |      | 10   |
| ТЕМА 5. Захист персональних даних та міжнародні стандарти.             | 14              | 2            | 2    |    |      | 10   | 13           | 1            | 2    |    |      | 10   |
| ТЕМА 6. Кібербезпека як складова інформаційної безпеки.                | 18              | 4            | 4    |    |      | 10   | 13           | 1            | 2    |    |      | 10   |
| Тема 7. Міжнародно-правові аспекти кіберзагроз і протидії їм.          | 18              | 4            | 4    |    |      | 10   | 23           | 1            | 2    |    |      | 20   |
| Тема 8. Протидія кіберзлочинності та юридична відповідальність         | 16              | 2            | 4    |    |      | 10   | 23           | 1            | 2    |    |      | 20   |
| <i>Усього годин</i>                                                    | 120             | 20           | 22   | 0  | 0    | 78   | 120          | 8            | 12   | 0  | 0    | 100  |

## **5. Зміст програми навчальної дисципліни**

### **ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.**

Національні інтереси в інформаційній сфері. Інформаційний суверенітет держави. Система забезпечення інформаційної безпеки України.

### **ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.**

Загрози інформаційній безпеці держави, суспільства, особи. Гуманітарні аспекти інформаційної безпеки. Протидія дезінформаційним впливам.

### **ТЕМА 3. Правове регулювання обігу інформації та електронне урядування.**

Правове регулювання обігу інформації. Електронне урядування як інструмент реалізації інформаційної політики держави.

### **ТЕМА 4. Інформація з обмеженим доступом та державна таємниця.**

Інформація з обмеженим доступом: поняття, види, правові засади захисту. Державна таємниця. Організаційно-правовий механізм захисту державної таємниці.

### **ТЕМА 5. Захист персональних даних та міжнародні стандарти.**

Нормативно-правове регулювання захисту персональних даних в Україні. Міжнародні правові стандарти та засади захисту даних. Обмін податковою інформацією між країнами.

### **ТЕМА 6. Кібербезпека як складова інформаційної безпеки.**

Кібербезпека як складова інформаційної безпеки держави. Проблеми та перспективи забезпечення кібербезпеки в Україні. Державні інформаційні ресурси та правові засади забезпечення їх безпеки.

### **ТЕМА 7. Міжнародно-правові аспекти кіберзагроз і протидії їм.**

Міжнародна правова визначеність кібератак. Міжнародно-правовий аспект протидії доксингу. Міжнародне співробітництво у сфері кібербезпеки.

### **ТЕМА 8. Протидія кіберзлочинності та юридична відповідальність.**

Боротьба з кіберзлочинністю. Відповідальність за порушення вимог інформаційної безпеки.

## 6. Теми лекцій

| № з/п        | Назва теми                                                             | Обсяг у годинах |              |
|--------------|------------------------------------------------------------------------|-----------------|--------------|
|              |                                                                        | Денна форма     | Заочна форма |
| 1            | ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 2               | 1            |
| 2            | ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 2               | 1            |
| 3            | ТЕМА 3. Правове регулювання обігу інформації та електронне урядування. | 2               | 1            |
| 4            | ТЕМА 4. Інформація з обмеженим доступом та державна таємниця.          | 2               | 1            |
| 5            | ТЕМА 5. Захист персональних даних та міжнародні стандарти.             | 2               | 1            |
| 6            | ТЕМА 6. Кібербезпека як складова інформаційної безпеки.                | 4               | 1            |
| 7            | Тема 7. Міжнародно-правові аспекти кіберзагроз і протидії їм.          | 4               | 1            |
| 8            | Тема 8. Протидія кіберзлочинності та юридична відповідальність         | 2               | 1            |
| 9            | ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 2               | 1            |
| 10           | ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 2               | 1            |
| Усього годин |                                                                        | 20              | 8            |

## 7. Теми семінарських занять

| № з/п        | Назва теми                                                             | Обсяг у годинах |              |
|--------------|------------------------------------------------------------------------|-----------------|--------------|
|              |                                                                        | Денна форма     | Заочна форма |
| 1            | ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 2               | 1            |
| 2            | ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 2               | 1            |
| 3            | ТЕМА 3. Правове регулювання обігу інформації та електронне урядування. | 2               | 1            |
| 4            | ТЕМА 4. Інформація з обмеженим доступом та державна таємниця.          | 2               | 1            |
| 5            | ТЕМА 5. Захист персональних даних та міжнародні стандарти.             | 2               | 2            |
| 6            | ТЕМА 6. Кібербезпека як складова інформаційної безпеки.                | 4               | 2            |
| 7            | Тема 7. Міжнародно-правові аспекти кіберзагроз і протидії їм.          | 4               | 2            |
| 8            | Тема 8. Протидія кіберзлочинності та юридична відповідальність         | 4               | 2            |
| 9            | ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 2               | 1            |
| 10           | ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 2               | 1            |
| Усього годин |                                                                        | 22              | 12           |

## 8. Теми практичних занять

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

## 9. Теми лабораторних занять

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

## 10. Теми самостійної роботи

| № з/п        | Назва теми                                                             | Обсяг у годинах |              |
|--------------|------------------------------------------------------------------------|-----------------|--------------|
|              |                                                                        | Денна форма     | Заочна форма |
| 1            | ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 8               | 10           |
| 2            | ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 10              | 10           |
| 3            | ТЕМА 3. Правове регулювання обігу інформації та електронне урядування. | 10              | 10           |
| 4            | ТЕМА 4. Інформація з обмеженим доступом та державна таємниця.          | 10              | 10           |
| 5            | ТЕМА 5. Захист персональних даних та міжнародні стандарти.             | 10              | 10           |
| 6            | ТЕМА 6. Кібербезпека як складова інформаційної безпеки.                | 10              | 10           |
| 7            | Тема 7. Міжнародно-правові аспекти кіберзагроз і протидії їм.          | 10              | 20           |
| 8            | Тема 8. Протидія кіберзлочинності та юридична відповідальність         | 10              | 20           |
| 9            | ТЕМА 1. Національні інтереси та інформаційний суверенітет держави.     | 8               | 10           |
| 10           | ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір.           | 10              | 10           |
| Усього годин |                                                                        | 78              | 100          |



## 11.Завдання для самостійної роботи

Самостійна робота з дисципліни *«Правові засади забезпечення інформаційної безпеки України»* спрямована на поглиблене опрацювання теоретичних і прикладних аспектів правового забезпечення інформаційної безпеки держави відповідно до структури курсу та його тематичного наповнення. Вона забезпечує системне засвоєння національного та міжнародного законодавства у сфері інформаційної безпеки, формування навичок правового аналізу інформаційних загроз, механізмів їх протидії та відповідальності за порушення вимог інформаційної безпеки.

У межах самостійної роботи здобувачі вищої освіти опрацьовують питання, що охоплюють національні інтереси в інформаційній сфері, інформаційний суверенітет держави, систему забезпечення інформаційної безпеки України, а також загрози інформаційній безпеці держави, суспільства й особи та їх гуманітарний вимір. Окрема увага приділяється аналізу дезінформаційних впливів і правових механізмів їх нейтралізації.

Самостійне опрацювання тематичних блоків передбачає дослідження правового регулювання обігу інформації, електронного урядування, правового режиму інформації з обмеженим доступом, державної таємниці та організаційно-правових механізмів її захисту. Значне місце відведено вивченню нормативно-правових засад захисту персональних даних, міжнародних стандартів у цій сфері та правових аспектів обміну податковою інформацією між державами.

У процесі самостійної роботи здобувачі освіти аналізують кібербезпеку як складову інформаційної безпеки держави, правові засади захисту державних інформаційних ресурсів, проблеми та перспективи розвитку кібербезпеки в Україні, а також міжнародно-правові аспекти визначеності кібератак і протидії доксингу. Окремо опрацьовуються питання боротьби з кіберзлочинністю та юридичної відповідальності за порушення вимог інформаційної безпеки.

Самостійна робота передбачає опрацювання нормативно-правових актів, судової практики, доктринальних і аналітичних джерел з урахуванням усіх тем дисципліни та спрямована на формування цілісного уявлення про сучасний стан, виклики й перспективи правового забезпечення інформаційної безпеки України.

Нижче подано варіанти завдань для самостійної роботи, що відповідають змісту окремих тем дисципліни та спрямовані на поглиблене опрацювання навчального матеріалу. Необхідно обрати одну з тем та виконати два завдання.

### ТЕМА 1. Національні інтереси та інформаційний суверенітет держави

1) Підготувати письмову позицію для дискусії щодо співвідношення інформаційного суверенітету держави та свободи інформації, з використанням візуалізації ключових національних інтересів в інформаційній сфері.

2) Провести пошуковий аналіз стратегічних документів України у сфері інформаційної безпеки та узагальнити основні елементи системи її забезпечення.

### ТЕМА 2. Загрози інформаційній безпеці та гуманітарний вимір

1) Проаналізувати кейс дезінформаційної кампанії, спрямованої на суспільство або окремі соціальні групи, та визначити правові механізми протидії.

2) Підготувати письмові тези для дискусії щодо гуманітарних наслідків інформаційних загроз для особи, суспільства та держави з опорою на наукову літературу.

### ТЕМА 3. Правове регулювання обігу інформації та електронне урядування

1) Проаналізувати практичну ситуацію, пов'язану з використанням електронного урядування, та змодельовати можливі інформаційні ризики і способи реагування.

2) Здійснити пошукове опрацювання національних і міжнародних рекомендацій щодо електронного урядування та узагальнити вимоги до безпечного обігу інформації.

### ТЕМА 4. Інформація з обмеженим доступом та державна таємниця

1) Розв'язати кейс щодо неправомірного доступу до інформації з обмеженим доступом, визначивши вид інформації та правові наслідки порушення режиму її захисту.

2) Скласти письмову модель реагування органу державної влади на загрозу розголошення державної таємниці із застосуванням практичного методу.

### ТЕМА 5. Захист персональних даних та міжнародні стандарти

1) Проаналізувати ситуацію витоку персональних даних і змодельовати правові механізми

захисту та відповідальності суб'єктів.

2) Провести пошуковий аналіз рішень ЄСПЛ або міжнародних стандартів у сфері захисту даних та підготувати узагальнений аналітичний висновок.

**ТЕМА 6. Кібербезпека як складова інформаційної безпеки**

1) Розв'язати кейс щодо кіберінциденту в державному інформаційному ресурсі та запропонувати модель правового реагування.

2) Проаналізувати статистику кіберзлочинів в Україні за останні роки та визначити основні тенденції та ризики з використанням пошукового методу.

**ТЕМА 7. Міжнародно-правові аспекти кіберзагроз і протидії їм**

1) Підготувати письмові тези для дискусії щодо міжнародної правової визначеності кібератак і проблем кваліфікації таких дій.

2) Проаналізувати міжнародні рекомендації або документи щодо протидії доксингу та узагальнити можливості їх застосування в Україні.

**ТЕМА 8. Протидія кіберзлочинності та юридична відповідальність**

1) Розв'язати кейс щодо притягнення до відповідальності за порушення вимог інформаційної безпеки, визначивши вид правової відповідальності.

2) Підготувати письмовий аналітичний висновок щодо ефективності національних механізмів боротьби з кіберзлочинністю з опорою на судову практику та статистичні дані.

Самостійна робота оцінюється під час поточного контролю теми на відповідному занятті. Засвоєння тем, які виносяться лише на самостійну роботу, контролюється при підсумковому контролі.

## **12. Питання для підготовки до підсумкового контролю (диференційований залік)**

1. Поняття національних інтересів у інформаційній сфері та їх значення для державної політики.
2. Інформаційний суверенітет держави: зміст, ознаки та сучасні виклики.
3. Місце інформаційної безпеки у системі національної безпеки України.
4. Система забезпечення інформаційної безпеки України: структура, суб'єкти та механізми.
5. Повноваження та роль органів державної влади у сфері інформаційної безпеки.
6. Поняття загроз інформаційній безпеці та їх сучасна класифікація.
7. Загрози інформаційній безпеці держави в умовах цифровізації та гібридної війни.
8. Загрози інформаційній безпеці суспільства та демократичним процесам.
9. Загрози інформаційній безпеці особи: приватність, репутація, цифрова ідентичність.
10. Цифровий слід особи та його вплив на інформаційну безпеку і приватність.
11. Гуманітарні та соціальні аспекти інформаційної безпеки.
12. Дезінформація, маніпуляція та пропаганда: поняття і правова оцінка.
13. Правові механізми протидії дезінформаційним та інформаційно-психологічним впливам.
14. Інформаційно-психологічні операції як інструмент впливу на державу і суспільство.
15. Роль соціальних мереж і цифрових платформ у формуванні загроз інформаційній безпеці.
16. OSINT і SOCINT як інструменти збору інформації: правові межі та ризики зловживань.
17. Поняття обігу інформації та його правове регулювання.
18. Принципи правового регулювання обігу інформації в Україні та ЄС.
19. Електронне урядування: поняття, форми та правові засади.
20. Інформаційні ризики та виклики у сфері електронного урядування.
21. Поняття інформації з обмеженим доступом та її правова характеристика.
22. Види інформації з обмеженим доступом та особливості правового режиму.
23. Правові, організаційні та технічні засади захисту інформації з обмеженим доступом.
24. Державна таємниця як об'єкт правової охорони.
25. Поняття, ознаки та класифікація державної таємниці.
26. Організаційно-правовий механізм захисту державної таємниці.
27. Поняття персональних даних та їх правовий режим.
28. Нормативно-правове регулювання захисту персональних даних в Україні.

29. Міжнародні та європейські стандарти захисту персональних даних.
30. Права суб'єктів персональних даних та механізми їх захисту.
31. Біометричні та інші чутливі персональні дані як об'єкт підвищеного правового захисту.
32. Роль практики ЄСПЛ у сфері захисту персональних даних та приватності.
33. Кібербезпека як складова інформаційної безпеки держави.
34. Основні загрози у сфері кібербезпеки та кіберстійкості.
35. Державні інформаційні ресурси та їх правовий режим.
36. Захист державних інформаційних ресурсів і критичної інформаційної інфраструктури.
37. Проблеми забезпечення кібербезпеки в Україні.
38. Перспективи розвитку системи кібербезпеки в Україні та ЄС.
39. Поняття кібератаки та проблеми її міжнародно-правової кваліфікації.
40. Міжнародно-правові підходи до регулювання кібероперацій (Tallinn Manual, Будапештська конвенція).
41. Інформаційна безпека в умовах збройного конфлікту та гібридної війни.
42. Інформаційна безпека та міжнародне гуманітарне право.
43. Поняття доксингу та його загроза правам людини й інформаційній безпеці.
44. Міжнародно-правові та національні підходи до протидії доксингу.
45. Поняття та основні форми кіберзлочинності.
46. Основні види кіберзлочинів та їх правова характеристика.
47. Міжнародне співробітництво у боротьбі з кіберзлочинністю.
48. Генеративний штучний інтелект як джерело нових загроз інформаційній безпеці.
49. Deepfake та згенерований контент: правові та безпекові виклики.
50. Кримінально-правові засоби протидії кіберзлочинності.
51. Адміністративна відповідальність за порушення законодавства у сфері інформаційної безпеки.
52. Цивільно-правова відповідальність у сфері інформаційних правовідносин.
53. Дисциплінарна відповідальність за порушення режимів захисту інформації.
54. Юридична відповідальність у сфері інформаційної безпеки: поняття, види та проблеми застосування.
55. Роль судової практики у забезпеченні інформаційної безпеки.
56. Співвідношення свободи вираження поглядів, свободи інформації та вимог інформаційної безпеки.
57. Сучасні тенденції розвитку правового забезпечення інформаційної безпеки України.

### 13. Методи навчання

**Методи навчання на лекціях:** вербальний метод у формі лекції та дискусії щодо міжнародних і національних аспектів інформаційної безпеки. Застосовується візуалізація та передбачена робота з літературою: рішеннями ЄСПЛ, аналіз міжнародних документів щодо кібербезпеки. Використовуються ІКТ - робота з офіційними реєстрами, аналітичними платформами, електронними ресурсами.

**Методи навчання на практичних, семінарських заняттях:** вербальний метод у форматі дискусій щодо інформаційних загроз, стандартів захисту, наслідків порушення ІБ. Використовується візуалізація та робота з літературою. Кейс-метод застосовується для розв'язання ситуацій щодо витоку даних, дезінформаційних кампаній, кіберінцидентів. Практичний метод передбачає моделювання методів реагування та аналіз механізмів захисту. Пошуковий метод реалізується через самостійне опрацювання статистики кіберзлочинів, рішень ЄСПЛ, міжнародних рекомендацій.

### 14. Методи оцінювання

У процесі вивчення дисципліни «Правові засади забезпечення інформаційної безпеки України» використовуються такі методи оцінювання:

Для поточного контролю: включають усне й письмове опитування, аналіз ситуаційних завдань, підготовку есе, індивідуальних проєктів із моделювання механізмів інформаційного захисту;

Для підсумкового контролю: у формі усної або письмової відповіді та вирішення правового кейсу.

## 15. 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 диференційований залік.

Завершальним етапом досягнення запланованих програмних результатів навчання з навчальної дисципліни «Правові засади забезпечення інформаційної безпеки України» є підсумковий контроль – диференційований залік.

## 16. Критерії та порядок оцінювання результатів навчання

Для оцінювання знань здобувачів вищої освіти застосовуються контрольні заходи у формі поточного та підсумкового контролю знань у відповідності 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 «Правові засади забезпечення інформаційної безпеки України» відбувається за такими рекомендованими балами:

| Види навчальної діяльності здобувачів вищої освіти                                                                                                                                        | Кількість балів |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Аудиторна робота</b>                                                                                                                                                                   |                 |
| Відповідь на практичному, семінарському, лабораторному занятті                                                                                                                            | 1-5             |
| Вирішення ситуаційних завдань, розв'язання задач тощо                                                                                                                                     | 1-5             |
| Тестування                                                                                                                                                                                | 1-5             |
| Практичний кейс тощо                                                                                                                                                                      | 1-10            |
| Інші види аудиторної роботи*                                                                                                                                                              |                 |
| <b>Самостійна робота</b>                                                                                                                                                                  |                 |
| 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 у відповідності до «Положення про оцінювання знань здобувачів вищої освіти».

### **Підсумковий контроль**

Максимальна кількість балів за екзамен з початкової дисципліни «Правові засади забезпечення інформаційної безпеки України» складає **40 балів**.

Для визначення ступеня засвоєння навчальної дисципліни та контрольної оцінювання знань здобувачів вищої освіти за підсумковим контролем застосовуються критерії у відповідності до «Положення про оцінювання знань здобувачів вищої освіти».

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

#### **Порядок переведення оцінок у систему ECTS**

| Сума балів за всі види навчальної діяльності | ОЦІНКА ECTS | ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ                              |                                                             |
|----------------------------------------------|-------------|------------------------------------------------------------|-------------------------------------------------------------|
|                                              |             | для екзамену<br>курсової роботи (проекту), практики        | для заліку<br>(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 |

## **17. 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 | Самостійна робота |                      |      |
| 6                                           | 6  | 6  | 6  | 6  | 6  | 7  | 7  | 10                | 40                   | 100  |

### *Для заочної форми здобуття освіти*

| Поточний контроль та самостійна робота - 60 |                   | Підсумковий контроль | Сума |
|---------------------------------------------|-------------------|----------------------|------|
| Контрольна робота                           | Самостійна робота |                      |      |
| 50                                          | 10                | 40                   | 100  |

## **18. Методичне забезпечення**

Методичне забезпечення дисципліни «Правові засади забезпечення інформаційної безпеки України» узагальнено в комплексі навчально-методичного забезпечення, який включає:

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

## 19. Рекомендована література

### Нормативно-правові акти:

1. Про державну таємницю: Закон України від 21.01.1994 р. № 3855- XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI ( у редакції від 19.10.2017). URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
4. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
5. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20.09.2017 р. № 649-р. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text>
6. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 08.11.2017 р. № 797-р. URL: <https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text>
7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України від 26 серпня 2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
8. Про Державний реєстр виборців: Закон України від 22.02.2007 р. № 698-V. URL: <https://zakon.rada.gov.ua/laws/show/698-16#Text>
9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від від 25 лютого 2017 року № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text>
10. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
11. Про доступ до судових рішень: Закон України від 22.12.2005 р. № 3262-IV. URL: <https://zakon.rada.gov.ua/laws/show/3262-15#Text>
12. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
13. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>
14. Про Реєстр осіб, які мають право на пільги: Постанова Кабінету Міністрів України від 29.01.2003 р. № 117. URL: <https://zakon.rada.gov.ua/laws/show/117-2003-%D0%BF#Text>
15. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>
16. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI. <https://zakon.rada.gov.ua/laws/show/5492-17#Text>
17. Про Єдиний державний реєстр ветеранів війни: Постанова Кабінету Міністрів України від 14.08.2019 р. № 700. URL: <https://zakon.rada.gov.ua/laws/show/700-2019-%D0%BF#Text>

### Основна:

1. Блінова Г.О. Інформаційні бази даних поліції превентивної діяльності як складова інтегрованої системи управління ризиками у сфері публічної безпеки та цивільного захисту: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 84 с.
2. Бочковий О.В., Блінова Г.О., Прокопов С.О., Мамедова Є.А. Інформаційне забезпечення діяльності патрульної поліції: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 112 с.
3. Блінова Г.О., Прокопов С.О. Інформаційне забезпечення підрозділів ювенальної превенції Національної поліції України: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 64 с.

4. Petro S. Korniienko, Oleh V. Plakhotnik, Hanna O. Blinova, Zhanna O. Dzeiko, Gennadii O. Dubov. Contemporary Challenges and the Rule of Law in the Digital Age. Studies of Applied Economics. DOI: 10.25115/eea.v39i9.5773. Volume 39-9, September 2021 // ISSN: 1133-3197

5. Енциклопедія соціогуманітарної інформології / коорд. проекту та заг. ред. проф. К. І. Беляков. Київ: Видавничий дім «Гельветика», 2021. Т. 2. 436 с.

6. Кушнір І. П., Курилюк Ю. Б., Царенко О. М., Сорока А. З. Правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: підручник. Хмельницький. Вид-во: ПП «Монускрипт», 2022. 432 с.

7. Чернявська Б. В., Ковальчук А. Ю. Міжнародно-правовий аспект протидії доксингу в цифрову епоху. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Том 4 № 85. С. 257-263. URL: <https://doi.org/10.24144/2307-3322.2024.85.4.37>

8. Alla Kovalchuk, Bogdana Cherniavska Європейський досвід протидії дезінформаційним впливам// ScienceRise: Juridical Science, 2024, Випуск 2 (28), с. 50-54.

9. Ковальчук, А. Ю., Гавловський, В. Д., & Чернявська, Б. В. (2024). Міжнародна правова визначеність масштабних кібератак. // ScienceRise: Juridical Science, 2024, Випуск 4, с. 90-96 DOI <https://doi.org/10.32782/chern.v4.2024.15>

10. Ковальчук, А. Ю., Чернявська, Б. В., Ковальчук М.С. (2023) Організація обміну податковою інформацією між країнами як захід запобігання легалізації коштів, отриманих злочинним шляхом Часопис Київського університету права, (3), 75-78.

11. Хромова О.І. Гуманітарні аспекти інформаційної безпеки / О. І. Хромова, О. О. Маруховський, Б. В. Чернявська // Epistemological studies in Philosophy, Social and Political Sciences. - 2022. - Т. 5. № 2. - С. 76-84.

#### **Інформаційні ресурси:**

1. Офіційний сайт ВРУ - <http://zakon.rada.gov.ua>
2. Офіційний сайт Президента України - <http://www.president.gov.ua/>
3. Офіційний сайт Уповноваженого Верховної Ради України з прав людини - <https://www.ombudsman.gov.ua/>
4. Кіберполіція. Національна поліція України. – <https://cyberpolice.gov.ua/>

#### **Допоміжна**

1. Кушнір І. П., Курилюк Ю. Б., Царенко О. М., Сорока А. З. Правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: підручник. Хмельницький. Вид-во: ПП «Монускрипт», 2022. 432 с.

2. Чернявська Б. В., Ковальчук А. Ю. Міжнародно-правовий аспект протидії доксингу в цифрову епоху. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Том 4 № 85. С. 257-263. URL: <https://doi.org/10.24144/2307-3322.2024.85.4.37>

3. Доступ до публічної інформації для державних службовців і службовців органів місцевого самоврядування: навчально-методичний посібник для тренерів / Кабанов О.М., Олексіюк Т.О. за заг. ред. Алюшиної Н.О. та Лубінця Д.В. Публікацію підготовлено та виготовлено за підтримки проекту «Права людини для України», який реалізує ПРООН в Україні та фінансує Міністерство закордонних справ Данії впродовж 2019–2023 років. Думки, висновки чи рекомендації належать автору цих рекомендацій і не обов'язково відображають погляди Міністерства закордонних справ Данії, ПРООН чи інших агенцій ООН. ISBN 978-617-7627-69-1 – Київ: ВАІТЕ, 2023. – 144 с.

4. Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. – Тернопіль 2023. – 88 с.

5. Левченко О. В. ЛЗ8 Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /О. В. Левченко. -Житомир : Видавець ПП “Євро-Волинь”, 2021. - 172 с.