

**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**  
**«Правове забезпечення інформаційної безпеки»**

<b>Рівень вищої освіти</b>	Магістр
<b>Освітньо-професійна програма</b>	Право
<b>Заняття:</b>	II семестр
Лекції	3 чверть - 2 години на тиждень; 4 чверть – 1 година на тиждень
Семінарські	1 година на тиждень
<b>Кількість кредитів</b>	3
<b>Мова викладання</b>	Українська



**Інформація про викладача**

Прізвище, ім'я, по батькові	<b>Блінова Ганна Олександрівна</b>
Науковий ступінь	доктор юридичних наук
Наукове звання	доцент
Посада	професор кафедри цивільного, господарського та екологічного права НТУ «Дніпровська політехніка»
Контакти	Роб.тел. 0562-756-09-91; моб: 0967917242
E-mail	blinovahanna@i.ua <a href="mailto:Blinova.G.O@nmu.one">Blinova.G.O@nmu.one</a>
Профайл	<a href="http://cgp.nmu.org.ua/ua/vykl.php">http://cgp.nmu.org.ua/ua/vykl.php</a>
Персональна сторінка	<a href="https://scholar.google.com.ua/citations?user=ySm66L0AAAAJ&amp;hl=ru">https://scholar.google.com.ua/citations?user=ySm66L0AAAAJ&amp;hl=ru</a>
Консультації	ауд.10/314, 1 година на тиждень (згідно графіку індивідуальних консультацій, що розміщений на інформаційному стенді кафедри)
Місце	Національний технічний університет «Дніпровська політехніка», кафедра філософії і педагогіки, 49005 м. Дніпро, пр. Дмитра Яворницького, 19; 10 корпус, 3 поверх, ауд. 314
Онлайн-консультації	електронна пошта (щоденно, окрім вихідних і святкових днів) <a href="mailto:Blinova.G.O@nmu.one">Blinova.G.O@nmu.one</a>

## **1. МЕТА ТА РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ**

Метою вивчення навчальної дисципліни є формування у студентів відповідних дисциплінарних компетентностей, які в свою чергу впливають на формування професійних компетентностей по організації діяльності органів державної влади та місцевого самоврядування.

### **2. Компетентності за освітньою програмою:**

- здатність до пошуку, оброблення та аналізу даних про систему інформаційної безпеки з різних джерел;

- 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 у сфері захисту інформаційних прав людини.

- здатність використовувати сучасні правові доктрини електронного урядування, та принципи інформаційної безпеки у правотворчості та в процесі застосування інститутів публічного і приватного права, а також кримінальної юстиції.

- здатність обґрунтовувати та мотивувати правові рішення з проблем забезпечення інформаційної безпеки, давати розгорнуту юридичну аргументацію.

- здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності при регулюванні суспільних відносин у сфері інформаційної безпеки.

- здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень для забезпечення інформаційної безпеки держави та суспільства з належною аргументацією;

- здатність до набуття спеціальних знань вмінь та навичок, методів та засобів, необхідних для розв'язання проблем правового регулювання публічних та приватних суспільних відносин у сфері інформаційної безпеки з метою забезпечення реалізації концепції сталого розвитку.

### **Нормативний зміст, сформульований у термінах результатів навчання:**

– уміти 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;

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

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

Результати вивчення навчальної дисципліни «Правове забезпечення інформаційної безпеки» згідно з вимогами освітньої програми: знати:

#### **1) на понятійному рівні:**

– понятійно-категоріальний апарат інформаційного права та нормативно-правових актів, що регулюють суспільні відносини у сфері інформаційної безпеки;

- специфіку правового регулювання та міжнародний досвід протидії порушенням інформаційного законодавства та кіберзлочинам;
- концепції і напрями вдосконалення правового регулювання й організації діяльності суб'єктів, що забезпечують інформаційну безпеку держави та суспільства.

## **2) на фундаментальному рівні:**

- теоретико-методологічні засади правового регулювання (функції, методи, принципи) суспільних відносин у сфері забезпечення інформаційної безпеки;
- законодавчу та нормативно-правову базу діяльності суб'єктів, що забезпечують інформаційну безпеку держави та суспільства.

## **3) на практично-творчому рівні:**

- юридичні норми для подальшого вдосконалення законодавства України, яке врегульовує питання відповідальності за порушення законодавства, що визначає засади інформаційної безпеки;
- види правопорушень та злочинів у інформаційній сфері;
- організаційні та правові аспекти функціонування алгоритмів захисту відомостей у інформаційних ресурсах та інфраструктурі;
- заходи правового впливу у разі виявлення факту вчинення інформаційного правопорушення, яке порушує інтереси фізичної або юридичної особи.

вміти:

### **1) на репродуктивному рівні:**

- відтворювати основні поняття та категорії організації діяльності суб'єктів забезпечення інформаційної безпеки щодо протидії правопорушенням у інформаційній сфері;
- узагальнювати вітчизняний та світовий досвід протидії кіберзлочинам;
- вирішувати тести та виконувати індивідуальні завдання.

### **2) на алгоритмічному рівні:**

- застосовувати загальні та спеціальні алгоритми аналізу і оцінювання діяльності щодо протидії інформаційним правопорушенням;
- надавати кваліфіковані правові консультації, роз'яснення та інші види правової допомоги щодо використання та захисту інформації з обмеженим доступом, а також відновлення порушених прав у цій сфері;
- визначати основні проблеми у протидії інформаційним правопорушенням та кіберзлочинам;
- кваліфіковано оцінювати своєчасність та ефективність вжитих державою заходів правового характеру з метою протидії різним видам правопорушень в інформаційній сфері.

### **3) на евристичному рівні:**

- аналізувати і коментувати нормативно-правові акти, які регулюють питання забезпечення інформаційної безпеки.

### **4) на творчому рівні:**

- вичерпно, логічно і творчо викладати інформацію в усній і письмовій формі, ґрунтовно висловлюватись та дискутувати, використовуючи набуті дисциплінарні компетентності з правового забезпечення інформаційної безпеки.

### 3. Результати навчання

#### 3.1 Програмні результати навчання

<b>РН3</b>	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.
<b>РН4</b>	Здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.
<b>РН8</b>	Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.

#### 3.2. ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Шифр ПРН	Дисциплінарні результати навчання (ДРН)	
	Шифр	Зміст
<b>РН3</b>	<b>ДРН 3.1-Ф4</b>	Проводити збір інформації про суб'єктний склад, зміст, особливості, правове регулювання та практику його застосування щодо суспільних відносин у сфері інформаційної безпеки, інтегрований аналіз цих відомостей 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.
<b>РН4</b>	<b>ДРН 4.1-Ф4</b>	Використовувати у своїй діяльності алгоритми забезпечення інформаційної безпеки з урахуванням яких здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.
<b>РН8</b>	<b>ДРН 8.1-Ф4</b>	Оцінювати достовірність інформації та надійність її джерел з урахуванням положень нормативно-правових актів у сфері інформаційної безпеки, ефективно опрацьовувати та використовувати бази даних для проведення наукових досліджень та правозастосовної діяльності у тому числі у сфері інформаційної безпеки.

#### 4. Структура курсу

<b>Шифр и ДРН</b>	<b>Види та тематика навчальних занять</b>	<b>Обсяг складових, години</b>
<b>ЛЕКЦІЇ</b>		<b>42</b>
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 1.</b> Інформаційне право та інформаційна безпека. Національні інтереси в інформаційній сфері та інформаційний суверенітет держави.	5
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 2.</b> Система забезпечення інформаційної безпеки України. Загрози інформаційній безпеці держави, суспільства, особи.	5
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 3.</b> Правове регулювання обігу інформації та електронне урядування. Інформація з обмеженим доступом, її види та правові засади захисту	5
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 4.</b> Державна таємниця та організаційно-правовий механізм її захисту	5
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 5.</b> Нормативно-правове регулювання захисту персональних даних в Україні	5
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 6.</b> Міжнародні правові стандарти засади захисту даних	5
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 7.</b> Державні інформаційні ресурси та правові засади забезпечення їх безпеки.	4
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 8.</b> Кібербезпека як складова інформаційної безпеки держави. Проблеми та перспективи забезпечення кібербезпеки в Україні.	4
ДРН 3.1-Ф4 ДРН 4.1-Ф4 ДРН 8.1-Ф4	<b>Тема 9.</b> Боротьба з кіберзлочинністю. Відповідальність за порушення вимог інформаційної безпеки	4
<b>СЕМІНАРСЬКІ ЗАНЯТТЯ</b>		<b>48</b>
<b>Шифр и ДРН</b>	<b>Види та тематика навчальних занять</b>	<b>Обсяг складових, години</b>
ДРН 3.1-Ф4 ДРН 4.1-Ф4	<b>Тема 1.</b> Інформаційне право та інформаційна безпека. Національні інтереси в інформаційній сфері та	2

ДРН 8.1-Ф4	інформаційний суверенітет держави.	
	<b>Тема 2.</b> Система забезпечення інформаційної безпеки України. Загрози інформаційній безпеці держави, суспільства, особи.	2
	<b>Тема 3.</b> Правове регулювання обігу інформації та електронне урядування. Інформація з обмеженим доступом, її види та правові засади захисту	2
	<b>Тема 4.</b> Державна таємниця та організаційно-правовий механізм її захисту	2
	<b>Тема 5.</b> Нормативно-правове регулювання захисту персональних даних в Україні	2
	<b>Тема 6.</b> Міжнародні правові стандарти засади захисту даних	2
	<b>Тема 7.</b> Державні інформаційні ресурси та правові засади забезпечення їх безпеки.	2
	<b>Тема 8.</b> Кібербезпека як складова інформаційної безпеки держави. Проблеми та перспективи забезпечення кібербезпеки в Україні.	2
	<b>Тема 9.</b> Боротьба з кіберзлочинністю. Відповідальність за порушення вимог інформаційної безпеки	3
	<b>РАЗОМ</b>	<b>47</b>

## 5. Технічне обладнання та/або програмне забезпечення

Спеціально обладнана проектором аудиторія 10/307 або 10/310 для проведення лекційних та семінарських занять.

Для навчання необхідно мати з собою гаджети зі стільниковим інтернетом.

Студент повинен мати активований акаунт університетської пошти (student.i.p@nmu.one) на Office 365 та бути зареєстрованим у СУДН «Moodle» на дистанційний курс з навчальної дисципліни «Правове забезпечення інформаційної безпеки».

## 6. Система оцінювання та вимоги

Сертифікація навчальних досягнень здобувачів вищої освіти здійснюється за допомогою прозорих процедур, що ґрунтуються на об'єктивних критеріях відповідно до Положення НТУ «Дніпровська політехніка» «Про оцінювання результатів навчання здобувачів вищої освіти НТУ «Дніпровська політехніка»».

Досягнутий рівень компетентностей відносно очікуваних, що ідентифікований під час контрольних заходів, відображає реальний результат навчання здобувача вищої освіти за дисципліною.

**6.1.** Оцінювання навчальних досягнень здобувачів вищої освіти НТУ «Дніпровська політехніка» здійснюється за рейтинговою (100-бальною) та інституційною шкалами. Остання необхідна (за офіційною відсутністю національної шкали) для конвертації (переведення) оцінок мобільних здобувачів.

*Шкали оцінювання навчальних досягнень здобувачів вищої освіти НТУ «ДП»*

Рейтингова	Інституційна
90...100	відмінно / Excellent
74...89	добре / Good
60...73	задовільно / Satisfactory
0...59	незадовільно / Fail

Кредити ЄКТС навчальної дисципліни зараховується, якщо здобувач вищої освіти отримав підсумкову оцінку не менше 60-ти балів. Нижча оцінка вважається академічною заборгованістю, що підлягає ліквідації відповідно до Положення про організацію освітнього процесу НТУ «Дніпровська політехніка».

**6.2.** Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь, комунікації, автономності та відповідальності здобувача вищої освіти за вимогами Національної рамки кваліфікацій до 6-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Здобувач вищої освіти на контрольних заходах має виконувати завдання, орієнтовані виключно на демонстрацію дисциплінарних результатів навчання (розділ 3).

Засоби діагностики, що надаються здобувачам вищої освіти на контрольних заходах у вигляді завдань для поточного та підсумкового контролю, формуються шляхом конкретизації вихідних даних та способу демонстрації дисциплінарних результатів навчання.

Види засобів діагностики та процедур оцінювання для поточного та підсумкового контролю дисципліни подано нижче.

ПОТОЧНИЙ КОНТРОЛЬ			ПІДСУМКОВИЙ КОНТРОЛЬ	
Навчальне заняття	засоби діагностики	процедури	засоби діагностики	процедури
Лекції	контрольні завдання за кожною темою	усне опитування, бліц-опитування, виконання завдань під час лекцій  методи евристичних питань, мозкового штурму, діалогового спілкування	підсумкове тестування у формі контрольної роботи (КР)	визначення середньозваженого результату поточних контролів;  підсумкове тестування у формі КР під час іспиту за бажанням здобувача вищої освіти  надання відповідей під час іспиту
Семінарські заняття	контрольні завдання за кожною темою	усне опитування, тестування, виконання завдань під час семінару  виступ-презентація, робота в малих групах, реферат/ ессе/ наукова доповідь		

**6.3.** Здобувачі вищої освіти можуть отримати підсумкову оцінку з дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Поточна успішність складається з успішності за оцінки за роботу на семінарських заняттях (оцінюється 8 занять, участь у одному занятті максимально може принести здобувачу вищої освіти 8 балів).

*Критерії оцінювання за відповідний вид навчальної діяльності студента.*

**Оцінювання** з курсу навчальної дисципліни «Правове забезпечення інформаційної безпеки» здійснюється з урахуванням розподілу отриманих балів за відповідний вид навчальної діяльності студента: 1) поточне тестування за кожною темою; 2) участь у форумі (дистанційно) або аудиторна робота на семінарських заняттях (очно); 3) виконання самостійної роботи; 4) виконання індивідуальних завдань.

**Тестування** – це метод ефективної перевірки рівня засвоєння знань, умінь і навичок із навчальної дисципліни. Тестування з навчальної дисципліни «Правове забезпечення інформаційної безпеки» здійснюється за кожною темою.

**Веб-форум або просто Форум** – інтернет-ресурс, популярний різновид спілкування в інтернеті, для проведення дискусій, на якому користувачі обмінюються досвідом та ідеями з певної заданої теми.

В рамках навчальної дисципліни «Правове забезпечення інформаційної безпеки» передбачено проведення форуму за кожною з тем (дистанційно) та обговорення на семінарському занятті результатів виконаного здобувачами певного завдання, підготовленої презентації (очно) з використанням методів мозкового штурму, евристичних питань та діалогового спілкування. За умови очного навчання за кожною темою проводиться робота в малих групах.



**Самостійна робота студента (СРС)** є основним засобом засвоєння навчального матеріалу у вільний від аудиторних занять час. Самостійна робота включає: попереднє опрацювання інформаційного забезпечення за всіма видами навчальних занять та розв'язання завдань самоконтролю опанування дисциплінарними результатами навчання відповідно до робочої програми дисципліни.

**Індивідуальні завдання** студентів включають виконання розрахункових, графічних, розрахунково-графічних робіт, есе, рефератів, презентацій, оформлення звітів, аналіз практичних ситуацій, підготовка реферативних матеріалів із фахових публікацій, курсових проектів (робіт), кваліфікаційних робіт, власні дослідження до конференцій, участь в олімпіадах тощо. Індивідуальні завдання сприяють більш поглибленому вивченню студентом теоретичного матеріалу, формуванню вмінь використання знань для вирішення відповідних практичних завдань, підвищення рівня підготовки і розкриття індивідуальних творчих здібностей.

Індивідуальними завданнями студентів в рамках вивчення навчальної дисципліни «Правове забезпечення інформаційної безпеки» є підготовка презентації за запропонованою темою та виступ з нею на семінарському занятті.

У таблиці наведено розподіл максимальної кількості балів за певний вид навчальної роботи студента за темами навчальної дисципліни

*Розподіл балів за видами навчальної роботи студента*

Теми	Тестування з теми	Участь у форумі, семінарському у занятті	Індивідуальні і завдання	Самостійна робота	Підсумкова (тестова) роботи	Підсумкова оцінка
1.	3	3	2	2	20	
2.	3	3	2	2		
3.	3	3	2	2		
4.	3	3	2	2		
5.	3	3	2	2		
6.	3	3	2	2		
7.	2	2	2	2		
8.	2	2	1	1		
9	2	2	1	1		
<b>Разом</b>	<b>24</b>	<b>24</b>	<b>16</b>	<b>16</b>	<b>20</b>	<b>100</b>
	<b>48</b>		<b>32</b>			

Викладач, враховуючи досягнення здобувача з дисципліни, його системну та активну участь і роботу на платформі MOODLE, може додати **0-10 балів**.

Отримані бали на семінарських заняттях (максимально 48 балів) та бали за самостійну та індивідуальну роботу (максимально 32 бали) додаються до оцінки з підсумкової (тестової) роботи в кінці семестру (20 балів) та є підсумковою оцінкою за вивчення навчальною дисципліни. Максимально за поточною успішністю

здобувач вищої освіти може набрати **100 балів**.

Загальна оцінка з навчальної дисципліни «Правове забезпечення інформаційної безпеки» визначається за накопичувальною системою, тобто сума всіх балів, отриманих за виконання певного виду робіт студента.

<p><b>Підсумкове оцінювання у VI семестрі (якщо здобувач вищої освіти набрав менше 60 балів та/або прагне поліпшити оцінку)</b></p>	<p>Іспит відбувається у письмовій формі, складається з 20 тестових запитань. Складається у VI семестрі Правильна відповідь на одне запитання тесту оцінюється у 5 бал. Максимальна кількість балів за іспит: 100</p>
---	--

#### 6.4. Критерії оцінювання за роботу на семінарських заняттях:

*Загальні критерії досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК (магістр)*

**Інтегральна компетентність** – здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі професійної правничої діяльності або у процесі навчання, що передбачає застосування правових доктрин, принципів і правових інститутів і характеризується комплексністю та невизначеністю умов

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
<b>Знання</b>		
<p>Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань</p>	<p>Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: - високим ступенем володіння інформацією за питанням; - спеціалізованих концептуальних знань на рівні новітніх досягнень; - критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей</p>	95-100
	<p>Відповідь містить не суттєві помилки або описки</p>	90-94
	<p>Відповідь правильна, але має певні неточності</p>	85-89
	<p>Відповідь правильна, але має певні неточності й недостатньо обґрунтована</p>	80-84
	<p>Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена</p>	74-79
	<p>Відповідь фрагментарна</p>	70-73
	<p>Відповідь демонструє нечіткі уявлення студента про об'єкт вивчення</p>	65-69
	<p>Рівень знань мінімально задовільний</p>	60-64

	Рівень знань незадовільний	<60
<b>Уміння / навички</b>		
<p>Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур;</p> <p>здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах;</p> <p>здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності</p>	Відповідь характеризує уміння: - виявляти проблеми; - формулювати гіпотези; - розв'язувати проблеми; - оновлювати знання; - інтегрувати знання; - провадити інноваційну діяльність; - провадити наукову діяльність	95-100
	Відповідь характеризує уміння застосовувати знання в практичній діяльності з не суттєвими помилками	90-94
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь незадовільний	<60
<b>Комунікація</b>		
Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	<p>Зрозумілість відповіді (доповіді). Мова:</p> <ul style="list-style-type: none"> <li>- правильна;</li> <li>- чиста;</li> <li>- ясна;</li> <li>- точна;</li> <li>- логічна;</li> <li>- виразна;</li> <li>- лаконічна.</li> </ul> <p>Комунікаційна стратегія:</p> <ul style="list-style-type: none"> <li>- послідовний і несуперечливий розвиток думки;</li> <li>- наявність логічних власних суджень;</li> <li>- доречна аргументації та її відповідність відстоюваним положенням;</li> <li>- правильна структура відповіді (доповіді);</li> <li>- правильність відповідей на запитання;</li> <li>- доречна техніка відповідей на запитання;</li> </ul>	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
	<ul style="list-style-type: none"> <li>- здатність робити висновки та формулювати пропозиції;</li> <li>- використання іноземних мов у професійній діяльності</li> </ul>	
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
<b><i>Відповідальність і автономія</i></b>		
<p>Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів;</p> <p>відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів;</p> <p>здатність продовжувати навчання з високим ступенем автономії</p>	<p>Відмінне володіння компетенціями:</p> <ul style="list-style-type: none"> <li>- використання принципів та методів організації діяльності команди;</li> <li>- ефективний розподіл повноважень в структурі команди;</li> <li>- підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини);</li> <li>- стресовитривалість;</li> <li>- саморегуляція;</li> <li>- трудова активність в екстремальних ситуаціях;</li> <li>- високий рівень особистого ставлення до справи;</li> <li>- володіння всіма видами навчальної діяльності;</li> <li>- належний рівень фундаментальних знань;</li> <li>- належний рівень сформованості загальнонавчальних умінь і навичок</li> </ul>	95-100
	Упевнене володіння компетенціями автономності та відповідальності з незначними хибами	90-94
	Добре володіння компетенціями автономності та відповідальності (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями автономності та відповідальності (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями автономності та	74-79

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
	відповідальності (не реалізовано чотири вимоги)	
	Задовільне володіння компетенціями автономності та відповідальності (не реалізовано п'ять вимог)	70-73
	Задовільне володіння компетенціями автономності та відповідальності (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями автономності та відповідальності (рівень фрагментарний)	60-64
	Рівень автономності та відповідальності незадовільний	<60

## 7. Політика курсу

**7.1. Політика щодо академічної доброчесності.** Академічна доброчесність студентів є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів.

Політика щодо академічної доброчесності регламентується положенням «Положення про систему запобігання та виявлення плагіату в Національному технічному університеті «Дніпровська політехніка» та реалізується із дотриманням положень Кодексу академічної доброчесності НТУ «Дніпровська політехніка».

Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі).

У разі порушення студентом академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

### 7.2. Комунікаційна політика.

Студенти повинні мати активовану університетську пошту.

Обов'язком студента є перевірка один раз на тиждень (щонеділі) поштової скриньки на Офіс365.

Протягом тижнів самостійної роботи обов'язком студента є робота з дистанційним курсом «Правове забезпечення інформаційної безпеки» (<https://do.nmu.org.ua>)

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

### 7.3. Політика щодо перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку.

### 7.4. Відвідування занять.

Для студентів денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, відрядження, які необхідно підтверджувати документами у разі тривалої (два тижні) відсутності. Про відсутність на занятті та причини відсутності студент має повідомити викладача або особисто, або через старосту. Якщо студент захворів, ми рекомендуємо залишатися вдома і навчатися за допомогою дистанційної платформи. Студентам, чий стан здоров'я є незадовільним і може вплинути на здоров'я інших студентів, буде пропонуватися залишити заняття (така відсутність вважатиметься пропуском з причини хвороби). Семінарські та практичні заняття не проводяться повторно, ці оцінки неможливо отримати під час консультації. За об'єктивних причин (наприклад, міжнародна мобільність або в період епідемій) навчання може відбуватися дистанційно - в онлайн-формі, за графіком, погодженим з викладачем.

**7.5. Бонуси.** Студенти, які регулярно відвідували лекції (мають не більше двох пропусків без поважних причин) та мають написаний конспект лекцій отримують додатково 2 бали до результатів оцінювання до підсумкової оцінки.

**7.6. Участь в анкетуванні.** Наприкінці вивчення курсу та перед початком сесії студентам буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на університетські поштові скриньки здобувачів вищої освіти. Заповнення анкет є важливою складовою навчальної активності здобувачів вищої освіти, що дозволить оцінити дієвість застосованих методів викладання та врахувати пропозиції стосовно покращення змісту навчальної дисципліни «Правове забезпечення інформаційної безпеки».

## **8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ**

### **8.1 Нормативно-правові акти:**

1. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-ХІІ. Відомості Верховної Ради (ВВР). 1994. № 16. Стаття 93.
2. Про інформацію: Закон України від 02.10.1992 р. № 2657-ХІІ. Відомості Верховної Ради України. 1992. № 48. Стаття 650.
3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI (у редакції від 19.10.2017). Відомості Верховної Ради України. 2010. № 34. Стор. 1188. Стаття 481.
4. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року № 2163-VIII. <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. Урядовий кур'єр. 2017. № 181.

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. Урядовий кур'єр. 2017. № 217.

7. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. Урядовий кур'єр. 2018. № 88.

8. 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>

9. Про Державний реєстр виборців: Закон України від 22.02.2007 р. № 698-V. Відомості Верховної Ради України. 2007. № 20. Стор. 764. Стаття 282.

10. Про Державний реєстр фізичних осіб-платників податків та інших обов'язкових платежів: Закон України від 22.12.1994 р. № 320/94-ВР. URL: <https://zakon.rada.gov.ua/laws/320/94>.

11. 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>.

12. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України (ВВР). 2011. № 32. Стаття 314.

13. Про доступ до інформації, що знаходиться у розпорядженні державних органів: Рекомендація № R (81) 19 Комітету Міністрів Ради Європи 1981 р. URL: <http://cedem.org.ua/library/re81-19>.

14. Про доступ до судових рішень: Закон України від 22.12.2005 р. № 3262-IV. Відомості Верховної Ради України. 2006. № 15. Ст. 128.

15. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Стор. 5. Стаття 400.

16. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275.

17. Про Єдиний державний автоматизований реєстр осіб, які мають право на пільги: Постанова Кабінету Міністрів України від 29.01.2003 р. № 117. Урядовий кур'єр. 2003. № 23.

18. 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>

19. 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. Відомості Верховної Ради України. 2013. № 51. Стор. 2733. Стаття 716.

20. 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>.

21. Про Єдину інформаційно-аналітичну систему управління соціальною підтримкою населення України (E-SOCIAL): Постанова Кабінету Міністрів України від 17.07.2019 р. №676. URL: <https://www.kmu.gov.ua/npras/pro-yedinu-informacijno>.

## **8.2 Навчально-методичні та наукові джерела:**

1. Мужанова Т. М. Інформаційна безпека держави. Навчальний посібник. Державний університет телекомунікацій. Київ. 2019. 131 с. [https://nubip.edu.ua/sites/default/files/u34/posibnik\\_ibd\\_muzhanova\\_2019.pdf](https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf)

2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

3. Інформаційна безпека держави : підручник / [ В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін. ] ; в 2 т. Т.1. / за аг. ред.. В.В. Остроухова. К. : ДНУ «Книжкова палата Україна», 2016. 264

4. Вишня В. Б. Основи інформаційної безпеки : навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро : ДДУВС, 2020. 128 с. URL: <https://er.dduvs.in.ua/handle/123456789/4206>

5. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. : іл.

6. Блінова Г.О. Інформаційне забезпечення органів публічної адміністрації в Україні: адміністративно-правові засади : монографія. Запоріжжя: Видавничий дім «Гельветика», 2019. 503 с.

7. Blinova G.O., Demchuk A.M., Yatsyshyn M.M. Ukrainian legislation regulating information support of public administration bodies: history, present, perspectives. New and traditional approaches in modern legal research : collective monograph / H. O. Blinova, O. V. Dykyi, V. Dyntu, A. V. Khridochkin, etc. Lviv-Toruń: Liha-Pres, 2019. 284 p. pp. 1–26

8. Blinova A.A., Kelman M.S. Legal regulation of use of public electronic information resources by public administration bodies during development of of Ukraine as a digital country. Juridical sciences and their role in the formation of legal culture of a modern person : collective monograph. Lviv : Liha-Pres, 2019. 256 p. pp. 1–27.

9. Blinova A.A., Holovko K.V. International and foreign experience of legal regulation of the process of information support of public administration bodies in the conditions of digitization of public administration. Issues of the state of modern legal education and professional culture of lawyers : collective monograph / A. A. Blinova, K.V. Holovko, A.V. Khridochkin, O. Yu. Dubynskyi, etc. – Lviv-Toruń: Liha-Pres, 2019. – 252 p. pp. 1–30.

10. 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.

11. 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.

12. 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.

13. Блінова Г.О. The mechanism of information support bodies public administration: concept, content, elements. *Visegrad Journal on Human Rights*. № 6. 2018 p. P. 44 – 48

14. 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

15. Мельник П., Костенко О., Блинова Х., Шинкаренко И. (2021). Опыт защиты персональных данных в Интернете и возможности их признания и защиты в Украине. *Ius Humanum. Юридический журнал*, 10 (2), 87-100. URL: <https://doi.org/https://doi.org/10.31207/ih.v10i2.288>

16. Блінова Г.О., Потіп М.М. Судовий захист приватно-правових таємниць: вітчизняний та іноземний досвід. *Приватне та публічне право* № 4. 2021. С.27-34

17. Блінова Г.О., Потіп М.М. Процесуальні аспекти захисту таємниці про стан здоров'я. *Право і суспільство*. № 6. 2021. С. 28-36

18. Блінова Г.О., Потіп М.М. Таємниця особистого життя: зміст та захист. *Юридичний науковий електронний журнал* № 12. 2021. С. 113-116

19. Блінова Г.О. Правові засади використання електронних інформаційних ресурсів в концепції цифрової держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*, (2), 53–60. URL: <https://doi.org/10.54929/pmtl-issue2-2021-10>