НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра публічного управління, адміністрування та права

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Богдан КОРОБКО
«18» 08 2026року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ІНФОРМАЦІЙНА БЕЗПЕКА В ПУБЛІЧНОМУ СЕКТОРІ»

(назва навчальної дисципліни)

Підготовки — Доктор філософії
(назва ступеня вищої освіти)

Освітньої програми — Публічне управління та адміністрування
(назва освітньої програми)

Спеціальності — 281 Публічне управління та адміністрування
(код і назва спеціальності)

Полтава
2026 рік

Робоча програма навчальної дисципліни «Інформаційна безпека в публічному секторі» для здобувачів вищої освіти спеціальності 281 Публічне управління та адміністрування, третього (освітньо-наукового) рівня вищої освіти.

Складена відповідно до освітньо-наукової програми «Публічне управління та адміністрування»

Розробник: Кульчій Інна Олексіївна, к.держ.упр., доцент, завідувач кафедри публічного управління, адміністрування та права

Погоджено:

Гарант освітньої програми _____ Микола ЛАХИЖА

Робоча програма затверджена на кафедри публічного управління, адміністрування та права

Протокол від «17» 08 20 26 року № 1

Завідувач кафедри публічного управління,
адміністрування та права _____ Інна КУЛЬЧІЙ

«17» 08 20 26 року

Схвалено навчально-методичною комісією інституту фінансів, економіки, управління та права

Протокол від «18» 08 20 26 року № 1

Голова навчально-методичної комісії _____ Євгенія КАРПЕНКО

«18» 08 20 26 року

© Інна КУЛЬЧІЙ, 2026 рік
© Національний університет
імені Юрія Кондратюка, 2026 рік

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="3">Найменування показників</td><td rowspan="3">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">Форма здобуття освіти</td></tr>
<tr><td>денна</td><td>заочна</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="2">Галузь знань

28 Публічне управління та адміністрування</td><td colspan="2" rowspan="2">вибіркова</td></tr>
<tr><td>Загальна кількість годин – 120</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="5">Спеціальність

<u>281 Публічне управління та адміністрування</u></td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>2-3</td><td>2-3</td></tr>
<tr><td rowspan="3">Змістових модулів – 2</td><td colspan="2">Семестр</td></tr>
<tr><td>4-6</td><td>4-6</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Індивідуальне завдання – не передбачено</td><td rowspan="11">Ступінь вищої освіти

<u>третій (освітньо-науковий)</u></td><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>80 год.</td><td>108 год.</td></tr>
<tr><td colspan="2">Індивідуальна робота:
Х год.</td></tr>
<tr><td colspan="2">Вид контролю:
диференційований залік</td></tr>
</table>

Примітка. Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

для денної форми здобуття освіти – 40/80;

для заочної форми здобуття освіти – 12/108

2. Мета навчальної дисципліни

Метою викладання навчальної дисципліни є формування у здобувачів третього (освітньо-наукового) рівня вищої освіти системних знань про сутність, правові та організаційні засади забезпечення інформаційної безпеки в публічному секторі, про механізми захисту інформаційних ресурсів органів публічної влади та об'єктів критичної інформаційної інфраструктури, а також набуття практичних навичок виявлення, оцінювання й наукового обґрунтування шляхів мінімізації загроз інформаційній безпеці держави, регіону та територіальної громади.

Завданнями дисципліни є: опанування понятійно-категорійного апарату інформаційної та кібернетичної безпеки; засвоєння чинного законодавства України і стандартів ЄС та НАТО у цій сфері; формування вмінь аналізувати діяльність суб'єктів національної системи кібербезпеки; оволодіння методиками оцінювання ризиків та управління інцидентами інформаційної безпеки в органах публічної влади; вироблення навичок наукового дослідження проблем інформаційної безпеки публічного сектору з урахуванням викликів воєнного часу.

Дисципліна «Інформаційна безпека в публічному секторі» має забезпечити такі програмні компетентності:

– Здатність продукувати нові ідеї, розв'язувати комплексні проблеми у сфері публічного управління та адміністрування, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.

– Здатність до абстрактного мислення, аналізу та синтезу.

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

– Здатність генерувати нові ідеї (креативність). Здатність приймати науково обґрунтовані рішення в умовах невизначеності, що потребує розробки нових методів та проведення дослідницько-інноваційної діяльності.

– Здатність розв’язувати комплексні проблеми публічного управління та адміністрування на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

– Здатність приймати науково обґрунтовані рішення в умовах невизначеності, що потребує розробки нових методів та проведення дослідницько-інноваційної діяльності.

3. Передумови для вивчення дисципліни

Передумовою вивчення навчальної дисципліни «Інформаційна безпека в публічному секторі» є знання, здобуті на другому (магістерському) рівні вищої освіти, а також знання, отримані здобувачами при вивченні обов'язкових компонентів освітньо-наукової програми.

4. Очікувані результати навчання з дисципліни

У результаті вивчення навчальної дисципліни здобувачі вищої освіти повинні:

- розробляти та досліджувати фундаментальні та прикладні моделі процесів і систем публічного управління та адміністрування, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів на рівні держави, регіону, громади та дотичних міждисциплінарних напрямах;

- застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу великих масивів даних та/або складної структури, спеціалізоване програмне забезпечення та інформаційні системи;

- знати та розуміти організаційно-правові, політичні та економічні засади організації управлінської діяльності інституцій публічного сектору у сучасних умовах, світовий досвід використання існуючих теорій у практичній діяльності на рівні держави, регіону та територіальних громад.

5. Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом вивчення навчальної дисципліни.

Мінімальний пороговий рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати в мінімальну позитивну оцінку числової (рейтингової) шкали.

Сума балів	ЄКТС значення	Оцінка за національною шкалою	Критерій оцінювання	Рівень компетентності
90 – 100	**A**	**Відмінно**	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін.	**Високий**, що повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.
82 – 89	**B**	**Добре**	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.	**Достатній**, що забезпечує здобувачу самостійне вирішення основних практичних задач.
74 - 81	**C**	**Добре**	Здобувач загалом добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для рішення характерних/типових практичних завдань на професійному рівні. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають ускладнення.	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.

64 - 73	**D**	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень дисципліни.
60 – 63	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень і володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використанням основних теоретичних положень пояснюються з труднощами. Виконання практичних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній,** що є мінімально допустимим у всіх складових навчальної дисципліни.
35 - 59	**FX**	**Незадовільно** з можливістю повторного складання екзамену/ диф.заліку	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних і лабораторних робіт в більшості є неправильними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький**, не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни.
0 – 34	**F**	**Незадовільно** з обов'язковим повторним вивченням дисципліни	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний**, здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:

✓ ***поточний контроль***

- *виконання практичних робіт*

- *тестування*
- *самостійна робота*

✓***модульний контроль*** *– тестування*

✓***підсумковий контроль*** *– диференційований залік*

7. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО СЕКТОРУ

Тема 1. Інформаційна безпека як складова національної безпеки України.

Поняття, зміст та структура інформаційної безпеки. Співвідношення понять «інформаційна безпека», «кібербезпека», «кіберзахист», «інформаційно-психологічна безпека». Національні інтереси в інформаційній сфері. Інформаційна безпека в системі публічного управління: об'єкти, суб'єкти, рівні забезпечення.

Практичне заняття № 1

Тема 2. Нормативно-правове забезпечення інформаційної безпеки.

Закони України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про захист персональних даних». Стратегія інформаційної безпеки та Стратегія кібербезпеки України. Підзаконні акти та відомче регулювання.

Практичне заняття № 2.

Тема 3. Інституційна система забезпечення інформаційної безпеки.

Рада національної безпеки і оборони України та Національний координаційний центр кібербезпеки. Держспецзв'язку, Служба безпеки України, Національна поліція, Міністерство оборони України. Команди реагування на кіберінциденти. Повноваження органів місцевого самоврядування. Публічно-приватне партнерство у сфері кібербезпеки.

Практичне заняття № 3.

Тема 4. Загрози інформаційній безпеці публічного сектору та управління ризиками.

Класифікація загроз: зовнішні та внутрішні, технічні та організаційні. Кібератаки на органи публічної влади: типові вектори. Інсайдерські ризики та людський чинник. Загрози ланцюга постачання. Особливості загроз в умовах воєнного стану. Методологія ризик-орієнтованого підходу: ідентифікація активів, оцінювання та обробка ризиків. Стандарти ISO/IEC серії 27000 та NIST Cybersecurity Framework.

Практичне заняття № 4.

Практичне заняття № 5

ЗМІСТОВИЙ МОДУЛЬ 2. ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ

Тема 5. Захист інформації в інформаційно-комунікаційних системах органів публічної влади.

Комплексна система захисту інформації: призначення, склад, порядок створення та оцінювання відповідності. Технічний та криптографічний захист інформації. Політика інформаційної безпеки органу публічної влади. Розмежування доступу та управління обліковими записами. Хмарні технології в публічному секторі: переваги та ризики. Кіберзахист державних інформаційних ресурсів та критичної інформаційної інфраструктури в

умовах збройної агресії та гібридних загроз. Особливості впровадження та функціонування електронного документообігу в умовах воєнного стану.

Практичне заняття № 6.

Тема 6. Кіберзахист об'єктів критичної інформаційної інфраструктури.

Критична інфраструктура та критична інформаційна інфраструктура: поняття і критерії віднесення. Загальні вимоги до кіберзахисту. Секторальні особливості. Аудит інформаційної безпеки. Забезпечення безперервності діяльності та відновлення після інцидентів.

Практичне заняття № 7.

Тема 7. Захист персональних даних та інформації з обмеженим доступом.

Правовий режим персональних даних. Принципи опрацювання даних та права суб'єкта даних. Загальний регламент ЄС про захист даних (GDPR) та адаптація законодавства України. Службова інформація та державна таємниця. Відповідальність за порушення режиму захисту інформації.

Практичне заняття № 8.

Тема 8. Управління інцидентами, інформаційно-психологічна безпека та оцінювання стану інформаційної безпеки.

Виявлення, реєстрація та реагування на інциденти. Взаємодія з командами реагування на кіберінциденти. Комунікації під час інциденту. Протидія дезінформації та інформаційно-психологічним впливам. Індикатори та критерії оцінювання стану інформаційної безпеки, міжнародні індекси кібербезпеки. Методи наукового дослідження проблем інформаційної безпеки: системний аналіз, моделювання, експертні методи, кейс-стаді.

Практичне заняття № 9.

Практичне заняття № 10.

8. Структура навчальної дисципліни

а) для денної форми здобуття освіти

Назви змістовних модулів і тем	Кількість годин					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО СЕКТОРУ						
Тема 1. Інформаційна безпека як складова національної безпеки України	15	2	2			11
Тема 2. Нормативно-правове забезпечення інформаційної безпеки	15	2	2			11
Тема 3. Інституційна система забезпечення інформаційної безпеки	15	2	2			11
Тема 4. Загрози інформаційній безпеці публічного сектору та управління ризиками	15	4	4			7
Разом за змістовим модулем 1	**60**	**10**	**10**			**40**
ЗМІСТОВИЙ МОДУЛЬ 2. ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ						
Тема 5. Захист інформації в інформаційно-комунікаційних системах органів публічної влади	15	2	2			11

Тема 6. Кіберзахист об'єктів критичної інформаційної інфраструктури	15	2	2			11
Тема 7. Захист персональних даних та інформації з обмеженим доступом	15	2	2			11
Тема 8. Управління інцидентами, інформаційно-психологічна безпека та оцінювання стану інформаційної безпеки	15	4	4			7
Разом за змістовим модулем 2	**60**	**10**	**10**			**40**
Усього годин	***120***	***20***	***20***			***80***

б) для заочної форми здобуття освіти

Назви змістовних модулів і тем	**Кількість годин**					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО СЕКТОРУ						
Тема 1. Інформаційна безпека як складова національної безпеки України	15	2				13
Тема 2. Нормативно-правове забезпечення інформаційної безпеки	15					15
Тема 3. Інституційна система забезпечення інформаційної безпеки	15					15
Тема 4. Загрози інформаційній безпеці публічного сектору та управління ризиками	15		2			13
Разом за змістовим модулем 1	**60**	**2**	**2**			**56**
ЗМІСТОВИЙ МОДУЛЬ 2. ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ						
Тема 5. Захист інформації в інформаційно-комунікаційних системах органів публічної влади	15	2	2			11
Тема 6. Кіберзахист об’єктів критичної інформаційної інфраструктури	15					15
Тема 7. Захист персональних даних та інформації з обмеженим доступом	15					15
Тема 8. Управління інцидентами, інформаційно-психологічна безпека та оцінювання стану інформаційної безпеки	15	2	2			11
Разом за змістовим модулем 2	**60**	**4**	**4**			**52**
Усього годин	***120***	***6***	***6***			***108***

9. Перелік питань для семінарських занять

Тема заняття та перелік питань	**Кількість годин**	
	для денної форми	для заочної форми
Семінарські заняття не передбачені		

10. Перелік питань для практичних занять

	Кількість годин

Тема заняття та перелік питань	денна форма	заочна форма
Практичне заняття 1. Інформаційна безпека як складова національної безпеки України. 1. Поняття, зміст та структура інформаційної безпеки. 2. Співвідношення понять «інформаційна безпека», «кібербезпека», «кіберзахист», «інформаційно-психологічна безпека». 3. Національні інтереси в інформаційній сфері. 4. Інформаційна безпека в системі публічного управління: об'єкти, суб'єкти, рівні забезпечення.	2	-
Практичне заняття 2. Нормативно-правове забезпечення інформаційної безпеки. 1. Система джерел законодавства України у сфері інформаційної та кібернетичної безпеки. 2. Аналіз стратегічних документів і стану їх реалізації. 3. Опрацювання кейсів щодо застосування норм про захист інформації. 4. Виявлення прогалин і колізій у чинному регулюванні.	2	–
Практичне заняття 3. Інституційна система забезпечення інформаційної безпеки 1. Розмежування повноважень суб'єктів національної системи кібербезпеки. 2. Аналіз механізмів міжвідомчої координації. 3. Повноваження органів місцевого самоврядування у сфері інформаційної безпеки. 4. Публічно-приватне партнерство: аналіз практики.	2	–
Практичне заняття 4-5. Загрози інформаційній безпеці публічного сектору та управління ризиками 1. Побудова моделі загроз для обраного органу публічної влади. 2. Класифікація та ранжування загроз за ймовірністю та наслідками. 3. Оцінювання ризиків за ризик-орієнтованим підходом. 4. Обґрунтування заходів обробки ризиків.	4	2
Практичне заняття 6. Захист інформації в інформаційно-комунікаційних системах органів публічної влади. 1. Структура та зміст політики інформаційної безпеки органу публічної влади. 2. Розроблення фрагмента політики (розмежування доступу, управління обліковими записами). 3. Аналіз призначення та складу комплексної системи захисту інформації. 4. Кіберзахист державних інформаційних ресурсів та критичної інформаційної інфраструктури в умовах збройної агресії та гібридних загроз. 5. Особливості впровадження та функціонування електронного документообігу в умовах воєнного стану.	2	2
Практичне заняття 7. Кіберзахист об'єктів критичної інформаційної інфраструктури. 1. Критерії віднесення об'єктів до критичної інформаційної інфраструктури: практикум. 2. Аналіз загальних вимог до кіберзахисту.	2	-

3. Розроблення елементів плану забезпечення безперервності діяльності.		
Практичне заняття 8. Захист персональних даних у публічному секторі. 1. Правові підстави опрацювання персональних даних розпорядниками інформації. 2. Порівняльний аналіз вимог законодавства України та GDPR. 3. Кейс-аналіз витоку персональних даних: дії органу влади. 4. Формулювання пропозицій щодо вдосконалення національного регулювання.	2	–
Практичне заняття 9-10. Управління інцидентами та оцінювання стану інформаційної безпеки. 1. Розроблення алгоритму реагування на кіберінцидент в органі публічної влади. 2. Комунікації під час інциденту: моделювання ситуації. 3. Розроблення системи індикаторів оцінювання стану інформаційної безпеки. 4. Підготовка аналітичної записки та її презентація.	4	2
Усього	***20***	***6***

11. Перелік питань для лабораторних занять

Тема заняття та перелік питань	Кількість годин	
	для денної форми	для заочної форми
Лабораторні заняття не передбачені		

12. Самостійна робота

Метою самостійної роботи здобувача вищої освіти є: користуватися бібліотечними фондами і каталогами (у тому числі електронними), працювати з нормативно-правовими, науковими та аналітичними джерелами, складати конспекти, тези, плани, аналізувати матеріал, порівнювати різні наукові концепції та формулювати висновки.

Види самостійної роботи здобувача:

– опрацювання лекційного матеріалу;

– підготовка до практичних занять;

– опрацювання тем курсу, які виносяться на самостійне вивчення, за списками літератури, рекомендованими в робочій навчальній програмі дисципліни;

– підготовка до виконання модульного контролю;

– відвідування консультацій (згідно з графіком консультацій кафедри);

– підготовка до складання диференційованого заліку за контрольними питаннями.

Питання для самостійного вивчення здобувачами вищої освіти

№ з/п	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО СЕКТОРУ			
Тема 1. Інформаційна безпека як складова національної безпеки України.			
1	Наукові підходи до визначення змісту інформаційної безпеки.	6	7

2	Інформаційна безпека на рівні територіальної громади.	5	6
Тема 2. Нормативно-правове забезпечення інформаційної безпеки.			
3	Стратегія інформаційної безпеки: зміст та стан реалізації.	5	7
4	Стандарти НАТО і ЄС у сфері кібербезпеки та їх імплементація в Україні.	6	8
Тема 3. Інституційна система забезпечення інформаційної безпеки.			
5	Національна система кібербезпеки: структура та проблеми координації.	5	7
6	Публічно-приватне партнерство у сфері кіберзахисту.	6	8
Тема 4. Загрози інформаційній безпеці публічного сектору та управління ризиками.			
7	Типові вектори кібератак на органи публічної влади; загрози ланцюга постачання в публічних закупівлях IT-рішень.	4	7
8	Стандарти ISO/IEC серії 27000 та NIST Cybersecurity Framework як інструменти управління ризиками.	3	6
ЗМІСТОВИЙ МОДУЛЬ 2. ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ			
Тема 5. Захист інформації в інформаційно-комунікаційних системах органів публічної влади.			
9	Порядок створення комплексної системи захисту інформації.	6	6
10	Хмарні технології в публічному секторі: переваги та ризики.	5	5
Тема 6. Кіберзахист об'єктів критичної інформаційної інфраструктури.			
11	Критерії віднесення об'єктів до критичної інформаційної інфраструктури.	5	7
12	Забезпечення безперервності діяльності органу публічної влади.	6	8
Тема 7. Захист персональних даних та інформації з обмеженим доступом.			
13	Права суб'єкта персональних даних та механізми їх реалізації.	5	7
14	Службова інформація: порядок віднесення та зняття обмеження доступу.	6	8
Тема 8. Управління інцидентами, інформаційно-психологічна безпека та оцінювання стану інформаційної безпеки.			
15	Порядок реагування на кіберінциденти в органі публічної влади; протидія дезінформації як завдання публічного управління.	3	5
16	Міжнародні індекси кібербезпеки: методологія та результати для України; методи наукового дослідження проблем інформаційної безпеки публічного сектору.	4	6
Разом		**80**	**108**

13. Індивідуальне завдання

Не передбачено планом.

14. Методи навчання

При викладанні дисципліни застосовуються словесні, наочні та практичні методи навчання.

Словесні та наочні методи навчання використовуються під час лекцій, індивідуальних та групових консультацій.

Під час проведення лекційних занять використовуються такі словесні методи, як розповідь і пояснення.

До числа наочних методів, які застосовуються при викладанні дисципліни, належать: ілюстрація, демонстрація, презентація.

З метою формування soft skills використовуються:

– методи мотивації навчання (створення ситуації інтересу, пізнавальні ділові ігри – симулятивні, ситуаційні, рольові, навчальні диспути, дискусії);

– активні/інтерактивні методи навчання (лекція-бесіда, лекція-дискусія, лекція-конференція, лекція із заздалегідь запланованими помилками, лекція-візуалізація, проблемна лекція, брейнстормінг, круглий стіл, ситуаційний аналіз, метод «Експертна оцінка»);

– проблемні методи навчання (створення ситуації вибору, зіткнення різних думок аспірантів, висування проблемного питання, постановка навчальних проблемних завдань на пояснення явища);

– бінарні методи навчання (наочно-інформаційний, наочно-проблемний, наочно-евристичний);

– прийом створення ситуації зацікавленості (використання актуальних кейсів, парадоксальних фактів, аналогій, зіставлення наукових і практичних тлумачень окремих явищ).

15. Методи контролю

Поточний контроль успішності засвоєння здобувачами навчального матеріалу здійснюється шляхом оцінювання знань здобувачів під час практичних занять, оцінювання виконання здобувачами самостійної роботи, проведення і перевірки тестів або в ході індивідуальних співбесід зі здобувачами під час консультацій. Вибір конкретних форм і методів поточного конролю знань здобувачів залежить від викладача і доводиться до їхнього відома на першому практичному занятті.

Модульний контроль є частиною поточного контролю і має на меті перевірку засвоєння здобувачем певної сукупності знань та вмінь, що формують відповідний змістовий модуль. Він реалізується шляхом проведення спеціальних контрольних заходів (у формі тестування), проводиться наприкінці кожного змістового модуля за рахунок аудиторних занять, під час групових консультацій або ж за рахунок часу, відведеного на самостійну роботу здобувачів.

Підсумковий контроль здійснюється у формі диференційованого заліку, який виставляється за сумою балів, набраних здобувачем за результатами поточного та модульного контролю впродовж семестру.

16. Розподіл балів, які отримують здобувачі освіти

Схема нарахування балів* для денної форми здобуття освіти з навчальної дисципліни «Інформаційна безпека в публічному секторі» за видами робіт

Види робіт/контролю	***Перелік тем***									
	Тема 1	*Тема 2*	*Тема 3*	*Тема 4*		*Тема 5*	*Тема 6*	*Тема 7*	*Тема 8*	
	Практичне заняття									
	1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
Тестування	3	3	3	3	3	3	3	3	3	3
Виконання практичних завдань	2	2	2	2	2	2	2	2	2	2
Виконання завдань самостійної роботи	2	2	2	2		2	2	2	2	

Модульний контроль				2				2
Всього за темами	*7*	*7*	*7*	***14***	*7*	*7*	*7*	***14***
Диференційований залік	***30***							
Всього за результатами вивчення навчальної дисципліни	***100***							

*В таблиці вказана максимальна кількість балів, які можна набрати за видами робіт

Схема нарахування балів* для заочної форми здобуття освіти з навчальної дисципліни «Інформаційна безпека в публічному секторі» за видами робіт

Види робіт/контролю	***Перелік тем***							
	Тема 1	*Тема 2*	*Тема 3*	*Тема 4*	*Тема 5*	*Тема 6*	*Тема 7*	*Тема 8*
	Практичне заняття							
	-	***-***	***-***	***1***	***2***	***-***	***-***	***3***
Тестування	2	2	2	2	2	2	2	2
Виконання практичних завдань				4	4			4
Виконання завдань самостійної роботи	5	5	5	5	5	5	5	5
Модульний контроль				1				1
Всього за темами	*7*	*7*	*7*	***12***	***11***	*7*	*7*	***12***
Диференційований залік	***30***							
Всього за результатами вивчення навчальної дисципліни	***100***							

*В таблиці вказана максимальна кількість балів, які можна набрати за видами робіт

Оцінювання тестування:

- кожна правильна відповідь оцінюється у фіксовану кількість балів *(0,3×10=3) – для денної форми здобуття освіти;*
- кожна правильна відповідь оцінюється у фіксовану кількість балів *(0,2×10=2) – для заочної форми здобуття освіти;*
- правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання виконання практичних завдань:

Бали		Критерії оцінювання
для денної форми здобуття освіти	для заочної форми здобуття освіти	
2	4	Практичну роботу виконано в повному обсязі та безпомилково. Результати чітко систематизовано, графіки/таблиці/розрахунки оформлено належним чином. Сформульовано вичерпні та аргументовані висновки, які повністю відображають глибину практичного застосування отриманих знань, виявляють критичний аналіз та вміння робити самостійні узагальнення.

1,5	3	Завдання практичної роботи виконано в повному обсязі, але допущено незначні огріхи чи неточності у розрахунках/оформленні. Висновки сформульовано повністю, проте їм бракує глибини аналізу або аргументації.
1	2	Завдання виконано щонайменше на 70%, є окремі несуттєві помилки. Висновки мають поверхневий характер та лише частково висвітлюють результати роботи.
0,5	1	Завдання виконано частково (менше ніж на 50%) або з суттєвими помилками. Висновки сформульовано формально, без належного зв'язку з виконаними практичними кроками.
0	0	Практичну роботу не виконано, відсутні будь-які результати або висновки, або роботу виконано з критичними помилками, що унеможливлюють зарахування.

Шкала та критерії оцінювання виконання завдань самостійної роботи

Бали для денної форми здобуття освіти	Бали для заочної форми здобуття освіти	Критерії оцінювання
2	5	Виконання завдань самостійної роботи здійснене у повному обсязі, не містить помилок, що дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти на високому рівні.
1	3	Виконання завдань самостійної роботи здійснене у повному обсязі, містить помилки та неточності, що дає можливість оцінити рівень формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти як достатній.
0	0	Завдання самостійної роботи не виконано та/або результати не відповідають поставленим завданням та/або завдання виконано із суттєвими помилками.

Оцінювання міжсесійного контролю (тестування) :

- кожна правильна відповідь оцінюється у фіксовану кількість балів *(0,2×10=1) – для денної форми;*
- кожна правильна відповідь оцінюється у фіксовану кількість балів *(0,1×10=1) – для заочної форми;*
- правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання знань здобувачів вищої освіти за результатами складання диференційованого заліку у формі тестування

№	Завдання	Бали	Критерії оцінювання
1	Тестування	0-30	Кожна правильна відповідь оцінюється у фіксовану кількість балів (1×30=30), правильність відповідей перевіряється відповідно до ключа тестів.

Шкала оцінювання: національна та ECTS

100-бальна рейтингова система оцінювання	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою для екзамену, диференційованого заліку, курсового проекту (роботи), практики
90 – 100	**A** – відмінно	**5** – відмінно
82 – 89	**B** – дуже добре	**4** – добре

74 – 81	**C** – добре	
64 – 73	**D** – задовільно	**3** – задовільно
60 – 63	**E** – достатньо	
35 – 59	**FX** – незадовільно з можливістю повторного складання	**2** – незадовільно
0 – 34	**F** – незадовільно з обов'язковим повторним вивченням дисципліни	

Правила модульно-рейтингового оцінювання знань

Загальна трудомісткість дисципліни – 100 балів, із них: ори семестровому контролі у вигляді диференційованого заліку на поточний контроль відведено 70 балів.

1. Поточний контроль. Бали, отримані впродовж семестру, за видами навчальної діяльності розподіляються наступним чином:

- робота на практичних заняттях (виконання *практичних завдань*, а в разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних занять) – до *70* балів.

Присутність на лекціях і практичних заняттях не оцінюється в балах. Пропуски занять підлягають обов'язковому відпрацюванню в індивідуальному порядку під час консультацій. Пропущене заняття має бути відпрацьоване впродовж двох наступних тижнів. При тривалій відсутності здобувача на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

Здобувач, який повністю виконав програму навчальної дисципліни і отримав достатню рейтингову оцінку (*не менше 35 балів*), допускається до підсумкового контролю з дисципліни.

2. Підсумковий контроль Підсумковим контролем є *диференційований залік*. Здійснюється відповідно до вимог «Положення про організацію освітнього процесу в Національному університеті «Полтавська політехніка імені Юрія Кондратюка».

17. Методичне забезпечення

1. Кульчій І.О. Конспект лекцій із дисципліни «Інформаційна безпека в публічному секторі» для здобувачів третього (освітньо-наукового) рівня вищої освіти. Полтава : Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2026. 178 с.

2. Кульчій І.О. Методичні вказівки до практичних занять із дисципліни «Інформаційна безпека в публічному секторі» для здобувачів третього (освітньо-наукового) рівня вищої освіти. Полтава : Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2026. 38 с.

3. Кульчій І.О. Методичні вказівки до самостійної роботи з дисципліни «Інформаційна безпека в публічному секторі» для здобувачів третього (освітньо-наукового) рівня вищої освіти. Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2026. 33 с.

18. Рекомендована література

Нормативно-правові акти

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII . URL: https://zakon.rada.gov.ua/laws/show/2469-19

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19

4. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17

7. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12

8. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021

9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

10. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518 (у редакції станом на 2025 р.). URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

Базова:

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К. 2024. №6 (червень). 364 с. URL: https://ippi.org.ua/sites/default/files/2024-6.pdf

2. Інформаційна безпека: сучасний стан, проблеми та перспективи : матеріали науково-практичної конференції / за заг. ред. О. В. Віннічук. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с. URL: https://politkaf.kpnu.edu.ua/

3. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. URL: https://duikt.edu.ua/uploads/l_1426_56444238.pdf

4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. . URL: https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AU7gw4X7N-ccr6JWTlXrp2wQkzgsA382geutxOirTCraPAmMfPFAsGjj

5. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. Edelweiss Applied Science and Technology Vol. 8 №. 6 (2024.) p. 1467-1480

6. Кульчій І., Лук'янов О., Сапіжак І. Організаційно-інформаційне та правове забезпечення розвитку державної служби України від набуття незалежності. Наукові інновації та передові технології. 2023. № 10 (24). URL: http://perspectives.pp.ua/index.php/nauka/article/view/6106 https://doi.org/10.52058/2786-5274-2023-10(24)-124-136

7. Кульчій І.О., Лучко Ю.І., Іваненко Р.О. Роль блокчейн технологій у забезпеченні кібербезпеки // Наука і техніка сьогодні». №6 (34) 2024 С. 98-970 http://perspectives.pp.ua/index.php/nts/article/view/12723

8. Діденко О. Г., Кульчій І. О. Цифрові інструменти як засіб інноваційного управління проєктами у територіальних громадах. Електронне наукове видання «Публічне адміністрування та національна безпека». 2025. № 7. URL: https://www.inter-nauka.com/issues/administration2025/7/11178

9. Polishchuk, V., Yurakh, V., Kravchenko, O., Warawa, W., Kulchii, I. LEGAL REGULATION OF CYBERSECURITY AND PRIVACY ON THE INTERNET AS SDG's. Journal of Lifestyle and SDG'S Review, 2024, 4(1) URL: https://ojs.sdgsreview.org/LifestyleJournal/article/view/1666

Допоміжна

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

2. NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : NIST, 2024. URL: https://www.nist.gov/cyberframework

3. Пугачов О. І. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2024. № 12. URL: https://reicst.com.ua/pmtl/issue/view/issue_12_2024

19. Інтернет ресурси

1. Сторінка курсу на платформі Moodle: https://dist.nupp.edu.ua/course/view.php?id=8008

2. Офіційний вебпортал Верховної Ради України. Законодавство України. URL: https://zakon.rada.gov.ua

3. Офіційний вебсайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua

4. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua

5. Офіційний вебсайт Ради національної безпеки і оборони України. URL: https://www.rnbo.gov.ua

6. EUR-Lex. Доступ до права Європейського Союзу. URL: https://eur-lex.europa.eu/

7. Інформаційна безпека: курс для навчання. URL: https://prometheus.org.ua/prometheus-free