НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

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

ЗАТВЕРДЖУЮ
Проректор із науково-педагогічної роботи
_____ Богдан КОРОБКО
«29» 08 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ІНФОРМАЦІЙНА БЕЗПЕКА ТА ДІДЖИТАЛІТАЦІЯ В ПУБЛІЧНОМУ УПРАВЛІННІ»

(назва навчальної дисципліни)

Підготовки — Бакалавр
(назва ступеня вищої освіти)

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

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

Полтава
2025 рік

Робоча програма навчальної дисципліни **«Інформаційна безпека та діджиталіязвція в публічному управлінні»** для студентів спеціальності **281 «Публічне управління та адміністрування»**, першого (бакалаврського) рівня вищої освіти.

Складена відповідно до освітньої програми **«Публічне управління та адміністрування»,** 2022 року.

Розробник: Кульчій Інна Олексіївна, доцент, завідувач кафедра публічного управління, адміністрування та права

Погоджено
Гарант освітньої програми _____ Аліна МИРОШНИЧЕНКО

Робоча програма затверджена на засіданні кафедри публічного управління, адміністрування та права

Протокол від «28» серпня 2025 року № 1

Завідувач кафедри публічного управління,
адміністрування та права _____ Інна КУЛЬЧІЙ

«28» серпня 2025 року

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

Протокол від «29» серпня 2025 року № 1

Голова навчально-методичної комісії _____ Євгенія КАРПЕНКО

«29» серпня 2025 року

1. **Опис навчальної дисципліни**

<table>
<tr><td rowspan="3">Найменування показників</td><td rowspan="3">Галузь знань, спеціальність, ступінь вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>форма здобуття освіти</td></tr>
<tr><td>денна</td></tr>
<tr><td>Кількість кредитів – 6</td><td rowspan="2">Галузь знань

28 Публічне управління та адміністрування</td><td rowspan="2">Вибіркова</td></tr>
<tr><td>Загальна кількість годин – 180</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="5">Спеціальність

281 Публічне управління та адміністрування</td><td>Рік підготовки:</td></tr>
<tr><td>4-й</td></tr>
<tr><td rowspan="3">Змістових модулів – 2</td><td>Семестр</td></tr>
<tr><td>8-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="9">Індивідуальне завдання – не передбачено;</td><td rowspan="9">Ступінь вищої освіти

бакалавр</td><td>32 год.</td></tr>
<tr><td>Практичні</td></tr>
<tr><td>30 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>0</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>118 год.</td></tr>
<tr><td>Індивідуальна робота:
0 год.</td></tr>
<tr><td>Вид контролю:
диференційований залік</td></tr>
</table>

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

для денної форми здобуття освіти – 62/118

2. Мета навчальної дисципліни

Формування у студентів вмінь, знань та навичок, що дозволяють оцінювати загрози інформаційній безпеці, запобігати їм, цифрові сервіси та ресурси в публічному управлінні.

Вивчення навчальної дисципліни передбачає формування та розвиток у здобувачів компетентностей, визначених освітньою програмою, зокрема:

– Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми у сфері публічного управління та адміністрування або у процесі навчання, що передбачає застосування теорій та наукових методів відповідної галузі і характеризується комплексністю та невизначеністю умов.

– Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

– Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

– Здатність бути критичним і самокритичним.

– Здатність до адаптації та дії в новій ситуації.

– Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

– Здатність забезпечувати дотримання нормативно-правових та морально-етичних норм поведінки.

– Здатність використовувати в процесі підготовки і впровадження управлінських рішень сучасні ІКТ.

– Здатність здійснювати інформаційно-аналітичне забезпечення управлінських процесів із використанням сучасних інформаційних ресурсів та технологій.

3. Передумови для вивчення дисципліни

Передумовами вивчення навчальної дисципліни «**Інформаційна безпека та діджиталізація в публічному управлінні»** є попередньо опановані дисципліни першого (бакалаврського) рівня вищої освіти.

4. Очікувані результати навчання з дисципліни

Формулювання результатів навчання базується на результатах навчання, визначених освітньою програмою (програмних результатах навчання) спеціальності 281 «Публічне управління та адміністрування»:

– Використовувати базові знання з історичних, культурних, політичних, соціальних, економічних засад розвитку суспільства.

– Знати стандарти, принципи та норми діяльності у сфері публічного управління та адміністрування.

– Знати основні нормативно-правові акти та положення законодавства у сфері публічного управління та адміністрування.

– Уміти організовувати та брати участь у волонтерських/культурно-освітніх/спортивних проектах, спрямованих на формування здорового способу життя / активної громадянської позиції.

– Уміти налагодити комунікацію між громадянами та органами державної влади і місцевого самоврядування.

– Уміти коригувати професійну діяльність у випадку зміни вихідних умов.

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

Сума балів	Значення ЄКТС	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 вивчені 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 постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень

			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.	дисципліни.
60 – 63	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використання м 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/ 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 невірними, 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

усне опитування

виконання практичних завдань

✓модульний контроль

тестування

✓***підсумковий контроль***
екзамен

7. Програма навчальної дисципліни

Змістовий модуль 1. Основи інформаційної безпеки в публічному управлінні
Тема 1. Поняття інформаційної безпеки: правовий і організаційний аспекти
Інформаційна безпека в сучасному світі. Інформаційна безпека держави, особи, суспільства. Зміст поняття «правовий режим доступу до інформації». Правове регулювання відкритої інформації та інформації з обмеженим доступом (конфіденційна, таємна, службова). Поняття «інформаційна безпека», «кібербезпека» та «захист інформації».
Практичне заняття 1.

Тема 2. Загрози інформаційній безпеці: класифікація та аналіз ризиків
Класифікація загроз інформаційній безпеці. Аналіз ризиків. Управління ризиками. Сучасні тренди загроз інформаційній безпеці.
Практичне заняття 2.

Тема 3. Нормативно-правова база України у сфері інформаційної безпеки
Аналіз нормативно-правових актів у сфері інформаційної безпеки: Конституція України; Стратегія інформаційної безпеки (затверджена Указом Президента №685/2021); Закон «Про національну безпеку України»; Закон «Про інформацію»; Закон «Про захист інформації в інформаційно-комунікаційних системах»; Закон «Про основні засади забезпечення кібербезпеки України».
Практичне заняття 3.

Тема 4. Міжнародний досвід правового регулювання інформаційної безпеки
Модель Європейського Союзу в контексті інформаційної безпеки. Досвід США в питаннях правового регулювання інформаційної безпеки. Аналіз Будапештської конвенції про кіберзлочинність (2001). ISO/IEC 27001: Вимоги до системи управління інформаційною безпекою (СУІБ). Кібервійна в світі (Tallinn Manual).
Практичне заняття 4.

Тема 5. Відповідальність за порушення законодавства в сфері інформаційної безпеки
Дисциплінарна та матеріальна відповідальність. Адміністративна відповідальність. Цивільно-правова відповідальність. Кримінальна відповідальність.
Практичне заняття 5.

Тема 6. Система органів управління інформаційною безпекою в Україні
Верховна Рада України та її функції в прийнятті законів, що регулюють сферу ІБ, кібербезпеки та захисту даних. Президент України та його завдання в сфері інформаційної безпеки. Рада національної безпеки і оборони та її завдання в сфері інформаційної безпеки. Національний координаційний центр кібербезпеки (НКЦК), який об'єднує зусилля розвідки, СБУ, Міноборони та інших структур. Кабінет Міністрів України в контексті проведення державної політики, спрямовує та координує роботу в інформаційній сфері. Інші органи влади та їх завдання в сфері інформаційної безпеки держави.
Практичне заняття 6.

Тема 7. Основи захисту інформації: правові та організаційні заходи

Законодавче закріплення прав власності на інформацію. Класифікація інформації за рівнем доступу. Впровадження на державному рівні вимог щодо технічного захисту інформації. Підписання договорів про нерозголошення конфіденційної інформації. Діяльність підрозділів та служб безпеки в контексті захисту інформації. Алгоритм впровадження системи захисту інформації.

Практичне заняття 7.

Тема 8. Правові способи захисту та протидії деструктивним інформаційним впливам в сегменті публічного управління

Дезінформація, пропаганда, маніпуляції громадською думкою та кібератаки на органи влади. Правовий режим заборони використання програмних продуктів, розроблених країнами-агресорами, в органах державної влади. Аналіз діяльності СБУ та Держспецзв'язку в контексті правового режиму захисту державних реєстрів від деструктивного втручання.

Практичне заняття 8.

Тема 9. Кібергігієна для публічних службовців

Правила кібергігієни. Формування культури кібергігієни. Ризики порушень правил кібергігієни. Захист власних та державних даних. Безпечне користування пристроями та додатками.

Практичне заняття 9.

Змістовий модуль 2. Діджиталізація в публічному управлінні

Тема 10. Основи діджиталізації: концепції та підходи

Поняття діджиталізації, цифровізації. Використання цифрових технологій для покращення окремих процесів в системі публічного управління та адміністрування. Виклики діджиталізації в умовах війни.

Практичне заняття 10.

Тема 11. Стратегії цифрової трансформації в системі публічного управління

Аналіз Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України», Закону України «Про електронні комунікації», Стратегії цифрової трансформації публічної служби до 2025 року. Розвиток цифрової інфраструктури (модернізація державних реєстрів, забезпечення обміну даними між органами влади).

Практичне заняття 11.

Тема 12 Сучасні сервіси та платформи в публічному управлінні

Інформаційні платформи у сучасному суспільстві. Державні і приватні інформаційні платформи: аналіз та оцінка. Платформи і створення в них економічної вартості.

Практичне заняття 12.

Тема 13. Використання штучного інтелекту в публічному управлінні

Етичні, правові, безпекові аспекти застосування штучного інтелекту у публічному секторі. Інструменти, рішення щодо впровадження ШІ в процес ухвалення управлінських рішень. Розумні рішення для викликів ШІ. Нові компетентності публічних службовців у добу ШІ.

Практичне заняття 13.

Тема 14. Blockchain-технології в публічному управлінні

Сутність Blockchain-технології. Напрями використання блокчейн-технології у публічній сфері України. Проблеми при використанні блокчейн-технології. Сфери використання блокчейн-технології (реєстри; податкова звітність, моніторинг бюджетних закупівель; захист критичної інфраструктури та даних у надзвичайних ситуація).

Практичне заняття 14.

Тема 15. Big Data у публічному управлінні

Big Data як інноваційний інструмент цифрової трансформації публічного управління. Big Data - інструмент реалізації принципів належного (Good Governance) та розумного врядування (Smart Governance). Виклики впровадження технологій великих даних в публічному управлінні.

Практичне заняття 15.

8. Структура навчальної дисципліни

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. Основи інформаційної безпеки в публічному управлінні						
Тема 1. Поняття інформаційної безпеки: правовий і організаційний аспекти	12	4	2			6
Тема 2. Загрози інформаційній безпеці: класифікація та аналіз ризиків	12	2	2			8
Тема 3 Нормативно-правова база України у сфері інформаційної безпеки	12	2	2			8
Тема 4. Міжнародний досвід правового регулювання інформаційної безпеки	12	2	2			8
Тема 5. Відповідальність за порушення законодавства в сфері інформаційної безпеки	12	2	2			8
Тема 6 . Система органів управління інформаційною безпекою в Україні	12	2	2			8
Тема 7. Основи захисту інформації: правові та організаційні заходи	12	2	2			8
Тема 8. Правові способи захисту та протидії деструктивним інформаційним впливам в сегменті публічного управління	12	2	2			8
Тема 9. Кібергігієна для публічних службовців	12	2	2			8
Разом за змістовим модулем 1	**108**	**20**	**18**			**70**
Змістовий модуль 2. Діджиталізація в публічному управлінні						
Тема 10. Основи діджиталізації: концепції та підходи	12	2	2			8
Тема 11 Стратегії цифрової трансформації в системі публічного управління	12	2	2			8
Тема 12. Сучасні сервіси та платформи в публічному управлінні	12	2	2			8
Тема 13 Використання штучного інтелекту в публічному управлінні	12	2	2			8
Тема 14 Blockchain-технології в публічному управлінні	12	2	2			8
Тема 15. Big Data у публічному управлінні	12	2	2			8
Разом за змістовим модулем 2	**72**	**12**	**12**			**48**
Усього годин	**180**	**32**	**30**			**118**

9. Перелік питань для семінарських занять

№ з/п	Тема заняття та перелік питань	Кількість годин
	Семінарські заняття не передбачені*	

10. Перелік питань для практичних занять

№ з/п	Тема заняття та перелік питань	Кількість годин для
Змістовий модуль 1. Основи інформаційної безпеки в публічному управлінні		
1	Тема 1. Поняття інформаційної безпеки: правовий і організаційний аспекти. Інформаційна безпека держави, особи, суспільства. Зміст поняття «правовий режим доступу до інформації». Правове регулювання відкритої інформації та інформації з обмеженим доступом (конфіденційна, таємна, службова). Поняття «інформаційна безпека», «кібербезпека» та «захист інформації».	2
2	Тема 2. Загрози інформаційній безпеці: класифікація та аналіз ризиків Класифікація загроз інформаційній безпеці. Аналіз ризиків. Управління ризиками. Сучасні тренди загроз інформаційній безпеці.	2
3	Тема 3. Нормативно-правова база України у сфері інформаційної безпеки Аналіз нормативно-правових актів у сфері інформаційної безпеки: Конституція України; Стратегія інформаційної безпеки (затверджена Указом Президента №685/2021); Закон «Про національну безпеку України»; Закон «Про інформацію»; Закон «Про захист інформації в інформаційно-комунікаційних системах»; Закон «Про основні засади забезпечення кібербезпеки України».	2
4	Тема 4. Міжнародний досвід правового регулювання інформаційної безпеки Модель Європейського Союзу в контексті інформаційної безпеки. Досвід США в питаннях правового регулювання інформаційної безпеки. Аналіз Будапештської конвенції про кіберзлочинність (2001). Кібервійна в світі (Tallinn Manual).	2
5	Тема 5. Відповідальність за порушення законодавства в сфері інформаційної безпеки Дисциплінарна та матеріальна відповідальність. Адміністративна відповідальність. Цивільно-правова відповідальність. Кримінальна відповідальність.	2
6	Тема 6. Система органів управління інформаційною безпекою в Україні Верховна Рада України та її функції в прийнятті законів, що регулюють сферу ІБ, кібербезпеки та захисту даних. Президент України та його завдання в сфері інформаційної безпеки. Рада національної безпеки і оборони та її завдання в сфері інформаційної безпеки. Національний координаційний центр кібербезпеки (НКЦК), який об'єднує зусилля розвідки, СБУ, Міноборони та інших структур. Кабінет Міністрів України в контексті проведення державної політики, спрямовує та координує роботу в інформаційній сфері. Інші органи влади та їх завдання в сфері інформаційної безпеки держави.	2
7	Тема 7. Основи захисту інформації: правові та організаційні заходи Законодавче закріплення прав власності на інформацію. Класифікація інформації за рівнем доступу. Впровадження на державному рівні вимог щодо технічного захисту інформації. Підписання договорів про нерозголошення конфіденційної інформації. Діяльність підрозділів та служб безпеки в контексті захисту інформації. Алгоритм впровадження системи захисту інформації.	2

8	Тема 8. Правові способи захисту та протидії деструктивним інформаційним впливам в сегменті публічного управління Дезінформація, пропаганда, маніпуляції громадською думкою та кібератаки на органи влади. Правовий режим заборони використання програмних продуктів, розроблених країнами-агресорами, в органах державної влади. Аналіз діяльності кіберцентрів, які забезпечують правовий режим захисту державних реєстрів від деструктивного втручання.	2
9	Тема 9. Кібергігієна для публічних службовців Правила кібергігієни. Формування культури кібергігієни. Ризики порушень правил кібергігієни. Захист власних та державних даних. Безпечне користування пристроями та додатками.	2
Змістовий модуль 2. Діджиталізація в публічному управлінні		
10	Тема 10. Основи діджиталізації: концепції та підходи Поняття діджиталізації, цифровізації. Використання цифрових технологій для покращення окремих процесів в системі публічного управління та адміністрування. Виклики діджиталізації в умовах війни.	2
11	Тема 11. Стратегії цифрової трансформації в системі публічного управління Аналіз Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України», Закону України «Про електронні комунікації», Стратегії цифрової трансформації публічної служби до 2025 року. Розвиток цифрової інфраструктури (модернізація державних реєстрів, забезпечення обміну даними між органами влади).	2
12	Тема 12 Сучасні сервіси та платформи в публічному управлінні Інформаційні платформи у сучасному суспільстві. Державні і приватні інформаційні платформи: аналіз та оцінка. Платформи і створення в них економічної вартості. Трансформації на ринках праці під впливом платформ; Майбутнє інформаційних платформ.	2
13	Тема 13. Використання штучного інтелекту в публічному управлінні Етичні, правові, безпекові аспекти застосування штучного інтелекту у публічному секторі. Інструменти, рішення щодо впровадження ШІ в процес ухвалення управлінських рішень. Розумні рішення для викликів ШІ. Нові компетентності публічних службовців у добу ШІ.	2
14	Тема 14. Blockchain-технології в публічному управлінні Сутність Blockchain-технології. Напрями використання блокчейн-технології у публічній сфері України. Проблеми при використанні блокчейн-технології. Сфери використання блокчейн-технології (реєстри; податкова звітність, моніторинг бюджетних закупівель; захист критичної інфраструктури та даних у надзвичайних ситуація).	2
15	Тема 15. Big Data у публічному управлінні Big Data як інноваційний інструмент цифрової трансформації публічного управління. Big Data - інструмент реалізації принципів належного (Good Governance) та розумного врядування (Smart Governance). Виклики впровадження технологій великих даних в публічному управлінні.	2
	Всього	**30**

11. Перелік питань для лабораторних занять

№ з/п	Тема заняття та перелік питань	Кількість годин
	Лабораторні заняття не передбачені*	

12. Самостійна робота

Метою самостійної роботи студента є: навчитися користуватися бібліотечними фондами і каталогами, працювати з історичними та літературними джерелами, складати конспекти, аналізувати матеріал, порівнювати різні наукові концепції та робити висновки.

Види самостійної роботи студента:

- опрацювання лекційного матеріалу;
- підготовка до практичних занять;
- опрацювання тем курсу, які виносяться на самостійне вивчення, за списками літератури, рекомендованими в робочій програмі навчальної дисципліни;
- підготовка до виконання модульної контрольної роботи (тестування);
- відвідування консультацій (згідно графіку консультацій кафедри);
- підготовка до складання екзамену за контрольними питаннями.

Питання для самостійного вивчення студентами

№ з/п та тема	Теми занять та перелік питань	Кількість годин для
Змістовий модуль 1. Основи інформаційної безпеки в публічному управлінні		
1	Тема 1. Поняття інформаційної безпеки: правовий і організаційний аспекти. Що таке «політика інформаційної безпеки» органу влади? Які обов'язкові розділи вона повинна містити та як забезпечується її дотримання персоналом? Порівняйте основні підходи до побудови систем управління інформаційною безпекою (СУІБ). Яке значення має стандарт ISO/IEC 27001 для сучасних організацій?	6
2	Тема 2. Загрози інформаційній безпеці: класифікація та аналіз ризиків Поняття вразливість та поняття загрози: аналіз змісту. Актуальні загрози для хмарних сервісів. Внутрішні загрози та зовнішні атаки: особливості та відмінності.	8
3	Тема 3. Нормативно-правова база України у сфері інформаційної безпеки Аналіз закону України ««Про електронні комунікації» (безпека мереж). Аналіз закону України «Про критичну інфраструктуру».	8
4	Тема 4. Міжнародний досвід правового регулювання інформаційної безпеки Шкідливе програмне забезпечення. Аналіз особливостей мобільних загроз. Модель загроз STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Спробуйте застосувати її до будь-якого онлайн-сервісу, яким ви користуєтесь.	8
5	Тема 5. Відповідальність за порушення законодавства в сфері інформаційної безпеки Відповідальність за втручання в роботу об’єктів критичної	8

	інфраструктури (енергетика, логістика). Відповідальність для адміністраторів державних реєстрів за будь-які несанкціоновані дії з даними громадян.	
6	Тема 6. Система органів управління інформаційною безпекою в Україні Боротьба з кібертероризмом, шпигунством та дезінформацією, що загрожує національній безпеці. Захист державних таємниць. Аналіз роботи CERT-UA. Розслідування кіберзлочинів: фінансове шахрайство, піратство, втручання в приватні системи.	8
7	Тема 7. Основи захисту інформації: правові та організаційні заходи Використання паролів та шифрів для захисту інформації. Криптографічний спосіб захисту інформації.	8
8	Тема 8. Правові способи захисту та протидії деструктивним інформаційним впливам в сегменті публічного управління Аналіз ризиків деструктивного впливу в органах державної влади. Блокування веб-ресурсів, соцмереж та телеканалів, які є інструментами деструктивного впливу.	8
9	Тема 9. Кібергігієна для публічних службовців Кіберзагрози від месенджерів та Інтернет-сервісів. Порядок використання зовнішніх носіїв інформації.	8
Змістовий модуль 2. Діджиталізація в публічному управлінні		
10	Тема 10. Основи діджиталізації: концепції та підходи Етапи цифрової трансформації в системі публічного управління. Українська екосистема «Дія».	8
11	Тема 11. Стратегії цифрової трансформації в системі публічного управління Аналіз роботи системи «Трембіта». Розвиток цифрових компетентностей державних службовців.	8
12	Тема 12 Сучасні сервіси та платформи в публічному управлінні Аналіз програми «Цифрова Європа».	8
13	Тема 13. Використання штучного інтелекту в публічному управлінні Відповідальність при використанні ШІ. Переваги та ризики використання ШІ в органах влади.	8
14	Тема 14. Blockchain-технології в публічному управлінні Міжнародний досвід використання блокчейн-технології. Декларація про створення Європейського блокчейн-партнерства (European Blockchain Partnership).	8
15	Тема 15. Big Data у публічному управлінні Технології Big Data в управлінні просторово-економічним розвитком міста і регіону. Застосування технологій аналізу великих масивів даних у політичній та соціальній сферах.	8
	Всього	**118**

13. Індивідуальні завдання

Не передбачено планом

14. Методи навчання

При викладанні навчальної дисципліни «Інформаційна безпека та діджиталізація в публічному управлінні» застосовуються словесні, наочні та практичні методи навчання, поєднані з сучасними інтерактивними технологіями. Це сприяє не лише засвоєнню теоретичних знань, а й формуванню практичних навичок і soft skills, необхідних майбутнім фахівцям у сфері публічного управління та адміністрування.

Для підвищення ефективності освітнього процесу використовуються сучасні технічні засоби - мультимедійні пристрої (проектор, інтерактивна дошка, комп'ютери) та спеціалізоване програмне забезпечення. Під час занять застосовуються платформи Microsoft Teams, Zoom - для дистанційного навчання та консультацій, Moodle - для організації навчального процесу, тестування та комунікації зі студентами.

Для аналізу нормативних актів, стандартів інформаційної безпеки, кіберзагроз та цифрових трансформацій використовуються електронні бази даних, наукові ресурси з кібербезпеки та офіційні сайти державних органів і міжнародних організацій (наприклад, сайти NIST, ENISA, Міністерства цифрової трансформації України). Це дозволяє студентам працювати з реальними матеріалами, що відображають сучасні тенденції розвитку інформаційної безпеки та діджиталізації в публічному секторі.

Словесні методи (лекції, пояснення, бесіди, дискусії) застосовуються для формування фундаментальних знань і роз'яснення складних концепцій, таких як криптографія, GDPR, цифрові платформи управління та ризики кібератак. Активне залучення студентів до обговорень сприяє кращому розумінню та розвитку критичного мислення.

Практичні методи спрямовані на розвиток професійних компетенцій і включають аналіз кейсів на основі реальних інцидентів кібербезпеки в державних установах, розбір прикладів цифрової трансформації (наприклад, е-урядування), моделювання систем захисту даних, підготовку політик безпеки та розв'язання ситуаційних завдань з діджиталізації процесів. Значну увагу приділено тренінгам з використання інструментів моніторингу загроз, аудиту систем і реагування на кіберінциденти.

Формування soft skills відбувається через роботу в малих групах, де студенти навчаються командній взаємодії, розподілу ролей у проектах діджиталізації та спільному прийняттю рішень. Використовуються ділові ігри, симуляції кібератак і відновлення систем, дебати й дискусії, які розвивають навички аргументації, публічних виступів і ведення переговорів у сфері інформаційної безпеки.

Для стимулювання творчого та аналітичного мислення застосовуються мозкові штурми, кейс-методи та ситуаційні вправи, що дозволяють працювати з реальними прикладами цифрових трансформацій і кіберзагроз, шукати ефективні шляхи їх вирішення та впровадження.

Поєднання традиційних і сучасних методів навчання у викладанні дисципліни «Інформаційна безпека та діджиталізація в публічному управлінні» сприяє формуванню у студентів не лише ґрунтовних теоретичних знань, а й практичних навичок, здатності до критичного аналізу та ефективної комунікації, важливих для роботи у сфері публічного управління та адміністрування.

15. Методи контролю

Поточний контроль успішності засвоєння студентами навчального матеріалу може здійснюватися шляхом опитування й оцінювання знань студентів під час практичних занять; оцінювання результатів виконання модульних тестів.

Модульний контроль є частиною поточного контролю і має на меті перевірку засвоєння студентом певної сукупності знань та вмінь, що формують відповідний модуль. Він реалізується шляхом проведення спеціальних контрольних заходів (у формі тестування), проводиться наприкінці кожного змістового модулю за рахунок аудиторних занять, під час групових консультацій або ж за рахунок часу, відведеного на самостійну роботу студентів. На підставі результатів модульного контролю здійснюється міжсесійний контроль (атестація).

Підсумковий контроль здійснюється у формі екзамену

16. Розподіл балів, які отримують студенти

Схема нарахування балів* за видами робіт

Види робіт/контролю	Перелік тем														
	Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 7	Тема 8	Тема 9	Тема 10	Тема 11	Тема 12	Тема 13	Тема 14	Тема 15
	Практичні заняття														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Виконання практичних завдань	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Усне опитування	2		2		2			2				2		2	
Тестування (модульний контроль)									4						4
Виконання завдань самостійної роботи	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Всього за темами	4	2	4	2	4	2	2	4	6	2	2	4	2	4	6
Всього	50														
Екзамен	50														
Всього за результатами вивчення навчальної дисципліни	100														

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

Шкала та критерії оцінювання виконання завдань на практичних занять

Бали	Критерії оцінювання
1	Питання розкрито повністю, що свідчить про відмінне засвоєння матеріалу відповідно вказаних програмних результатів навчання. Студент вільно володіє науково-понятійним апаратом.
0,5	Механічне відтворення матеріалу з деякими помилками, неточності у використанні науково-понятійного апарату.
0	Відсутність відповіді на теоретичне питання, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти.

Шкала та критерії оцінювання відповіді за результатами усного опитування для денної форм здобуття освіти:

Бали	Критерії оцінювання
2	Питання розкрито повністю, що свідчить про відмінне засвоєння матеріалу відповідно вказаних програмних результатів навчання. Студент вільно володіє науково-понятійним апаратом.
1	Механічне відтворення матеріалу з деякими помилками, неточності у використанні науково-понятійного апарату.
0	Відсутність відповіді на теоретичне питання, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти.

Оцінювання тестування (модульний контроль) для денної форми здобуття освіти:

- кожна правильна відповідь оцінюється у фіксовану кількість балів (0,2×20=4) правильність відповідей перевіряється відповідно до ключа тестів**.**

Шкала та критерії оцінювання виконання завдань самостійної роботи

Бали	Критерії оцінювання
1	Виконано завдання практичної роботи в повному обсязі, належним чином оформлено висновки, в яких відображено здатність до практичного застосування отриманих знань.
0,5	Виконано завдання практичної роботи із несуттєвими помилками або не в повному обсязі, оформлено висновки, які частково розкривають практичне завдання.
0	Не виконано практичну роботу або виконано із суттєвими помилками.

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

№	Завдання	Бали	Критерії оцінювання
1	Тестування	0-50	Кожна правильна відповідь оцінюється у фіксовану кількість балів (1×50=50), 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	

Правила модульно-рейтингового оцінювання знань

Загальна трудомісткість дисципліни – 100 балів, із них:

при підсумковому контролі у вигляді екзамену 50 балів відведено на поточний контроль, а 50 балів – на підсумковий (для допуску до екзамену необхідно мати не менше 25 балів поточної успішності).

1. Поточний контроль. Бали, отримані впродовж семестру, за видами навчальної діяльності розподіляються наступним чином (розподіл орієнтовний): робота на практичних заняттях (усні відповіді, виконання практичних завдань, тести, а в разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних занять), – до 50 балів.

Присутність на лекціях і практичних 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 студента на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

Студент, який повністю виконав програму навчальної дисципліни і отримав достатню рейтингову оцінку (не менше 25 балів у випадку екзамену), допускається до підсумкового контролю з дисципліни.

2. Підсумковий контроль Підсумковим контролем є екзамен. Він здійснюється відповідно до вимог «Положення про організацію освітнього процесу в Національному університеті «Полтавська політехніка імені Юрія Кондратюка».

17. Методичне забезпечення

1. Кульчій І.О. Методичні рекомендації для практичних занять та самостійної роботи з дисципліни «Інформаційна безпека та діджиталізація в публічному управлінні» для студентів першого (бакалаврського) рівня вищої освіти спеціальності 281 Публічне управління та адміністрування, 2024 16 с.
2. Кульчій І.О. Курс лекцій з дисципліни «Інформаційна безпека та діджиталізація в публічному управлінні» для студентів першого (бакалаврського) рівня вищої освіти спеціальності 281 Публічне управління та адміністрування. Полтава, 2025. 87 с.

18. Рекомендована література

Базова

1. 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.
2. Панченко О.А., Гнатенко В.С. Інформаційна безпека у сучасному вимірі: монографія. К.: КВІЦ. 2023. 404 с.
3. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки : монографія : електрон. наук. вид. / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2023. 152 с.
4. Інформаційна безпека : навч. посібн.; за заг. ред. Ю. Я. Бобало, І. В. Горбатого. Львів : вид-во Львівської політехніки, 2019. 580 с. URL: https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
5. Прудеус М. Основи маніпуляції: Відео-курс, 2022. URL: https://www.youtube.com/playlist?list=PL8G81iuosceius5hg2F9JQUx8oQaFfcdY

6. Digital Government Index 2023: OECD Results and Key Findings. Paris : OECD Publishing, 2024. URL: https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html

Допоміжна

1. Разумей Г. Ю. Діджиталізація публічного управління як складник цифрової трансформації України / Г. Ю. Разумей, М. М. Разумей // Публічне управління та митне адміністрування. 2020. -№ 2(25). С. 139 – 145
2. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL: http://zakon4.rada.gov.ua/laws/show/2657-12
3. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19
4. Закон України «Про основні засади забезпечення кібербезпеки України», від 05.10.2017. URL: http://zakon.rada.gov.ua/laws/show/2163-19
5. Закон України «Про національну програму інформатизації» від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#n191
6. Стратегія інформаційної безпеки України; затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
7. Стратегія кібербезпеки України: Безпечний кіберпростір – запорука успішного розвитку країни, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
8. Інформаційна безпека. URL: https://prometheus.org.ua/course/course-v1:Internews+INFOS101+UA_2021_T3
9. Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IH101+2021_T3/about
10. Дезінформація: види, інструменти та способи захисту. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DISINFO101+2021_T2/about
11. Цифрова безпека та комунікація в онлайні URL: https://vumonline.ua/course/digital-security-and-communication-online
12. 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. 2024. Vol. 8 № 6. URL: https://learning-gate.com/index.php/2576-8484/article/view/2263
13. 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

19. Інтернет ресурси

1. Сторінка курсу на платформі Moodle: https://dist.nupp.edu.ua/course/view.php?id=5588
2. Президент України – www.prezident.gov.ua
3. Верховна Рада України – www.rada.gov.ua
4. Кабінет Міністрів України – www.kmu.gov.ua