Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Кафедра державного управління і місцевого самоврядування

«ЗАТВЕРДЖЕНО»
завідувач кафедри
Чикаренко І.А. _____
«39» серпня 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Інформаційна безпека в публічному управлінні»

Галузь знань ……...	28 Публічне управління та адміністрування
Спеціальність …….....	281 Публічне управління та адміністрування
Рівень вищої освіти ……	перший (бакалаврський)
Статус ……..	вибіркова, фахова
Загальний обсяг ..……	4 кредити ECTS (120 годин)
Форма підсумкового контролю …….	диференційований залік
Термін викладання …….	4-та чверть
Термін викладання ……	8-й семестр, 15 чверть
Мова викладання ……	українська

Викладач: к.х.н., доц. Кравцов О.В.

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

Дніпро
НТУ «ДП»
2025

Робоча програма навчальної дисципліни «Інформаційна безпека в публічному управлінні» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-науковою програмою «Публічне управління та адміністрування» спеціальності 281 «Публічне управління та адміністрування» / Нац. техн. ун-т. «Дніпровська політехніка», каф. державного управління і місцевого самоврядування. Дніпро : НТУ «ДП», 2025. 17 с.

Розробник:
Кравцов Олег Валентинович, доцент, кандидат хімічних наук, доцент кафедри державного управління і місцевого самоврядування.

Робоча програма регламентує:

– мету дисципліни;
– дисциплінарні результати навчання;
– базові дисципліни;
– обсяг і розподіл за формами організації освітнього процесу та видами навчальних занять;
– програму дисципліни (тематичний план за видами навчальних занять);
– алгоритм оцінювання рівня досягнення дисциплінарних результатів навчання (шкали, засоби, процедури та критерії оцінювання);
– інструменти, обладнання та програмне забезпечення;
– рекомендовані джерела інформації.

Робоча програма призначена для реалізації компетентнісного підходу під час планування освітнього процесу, викладання дисципліни, підготовки здобувачів вищої освіти до контрольних заходів, контролю провадження освітньої діяльності, внутрішнього та зовнішнього контролю забезпечення якості вищої освіти, акредитації освітніх програм у межах спеціальності.

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета дисципліни формуванні у майбутніх управлінців комплексної системи теоретичних знань та практичних навичок щодо організації захисту інформаційних ресурсів, забезпечення інформаційної безпеки органів публічної влади, опанування методів протидії дезінформації та маніпулятивним технологіям, а також ефективного управління ризиками в інформаційній сфері на місцевому, регіональному та загальнодержавному рівнях.

2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Шифр ДРН	**Дисциплінарні результати навчання (ДРН)**
	Зміст
ДРН – 01	Знати та інтерпретувати положення НПА щодо забезпечення інформаційної безпеки в системі публічного управління.
ДРН – 02	Продемонструвати знання інституційної структури національної системи кібербезпеки, включаючи ролі ДССЗЗІ, CERT-UA та галузевих команд реагування.
ДРН – 03	Розуміти архітектуру безпеки електронного урядування, принципи захищеного доступу до мережі Інтернет для органів влади та вимоги до авторизованих систем.
ДРН – 04	Демонструвати здатність до ефективного збирання, аналізу та верифікації інформації у професійній діяльності.
ДРН – 05	Застосовувати практичні аспекти кібергігієни, захисту персональних даних та конфіденційної інформації при роботі в інформаційно-комунікаційних системах.
ДРН – 06	Демонструвати здатність до ідентифікації дезінформації, розпізнавання ворожих інформаційно-психологічних операцій та дотримання етичних норм у цифровій комунікації.
ДРН – 07	Вміти розробляти організаційні заходи щодо створення та підтримки системи управління інформаційною безпекою в органах публічного управління

3 БАЗОВІ ДИСЦИПЛІНИ

Міждисциплінарні зв’язки: вивчення курсу ґрунтуються на знаннях, отриманих з дисциплін «Вступ до фаху», «Основи публічного управління та адміністрування», «Політичні інститути та процеси», «Правознавство» «Інформаційні технології в публічному управлінні»

4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Вид навчальних занять	**Обсяг,** *години*	**Розподіл за формами навчання**, *години*			
		Денна / Вечірня		**Заочна**	
		аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота
Лекційні	60	20	40	4	56
Практичні	60	40	20	6	54
Лабораторні	-	-	-	-	-
Семінари	-	-	-	-	-
РАЗОМ	120	60	60	10	110

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

5.1 Тематичний план та розподіл обсягу часу за видами навчальних занять

Шифри ДРН	**Види та тематика навчальних занять**	**Обсяг складових,** *години*
	ЛЕКЦІЇ	**60**
ДРН – 01 ДРН – 02 ДРН – 03	**1. Теоретичні засади інформаційної безпеки держави. Національна система кібербезпеки.**	8
	1.1. Понятійно-категоріальний апарат та складові інформаційної безпеки держави (національні інтереси, загрози, вразливості).	
	1.2. Основні принципи формування ІБ в Україні. Інституційна модель кібербезпеки.	
	1.3. Державна політика та стратегічне планування у сфері кіберзахисту.	
	1.4. Міжнародна співпраця у сфері кібербезпеки та інтеграція України до європейського й євроатлантичного безпекового простору.	
ДРН – 02 ДРН – 03	**2. Нормативно-правове забезпечення інформаційної безпеки.**	8
	2.1. Базове законодавства України у сфері інформаційої безпеки.	
	2.2. Євроінтеграційні процеси: адаптація українського законодавства до вимог ЄС (імплементація директиви NIS2, стандартів GDPR).	
	2.3. Огляд ключових законодавчих змін, ініціатив та нових постанов КМУ у сфері кібербезпеки.	
	2.4. Юридична відповідальність за правопорушення у кіберпросторі (кіберзлочини, витік службової інформації, недбалість).	
ДРН – 04	**Тема 3. Кібергігієна та захист персональних даних у цифровій державі.**	8

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
ДРН – 05 ДРН – 06	3.1. Ключові правила кібергігієни на робочому місці: управління паролями, багатофакторна автентифікація (MFA), безпека електронної пошти.	
	3.2. Соціальна інженерія та фішинг: методи розпізнавання атак на державних службовців.	
	3.3. Правові та практичні аспекти обробки персональних даних (ЗУ «Про захист персональних даних», принципи мінімізації даних).	
	3.4. Ризики використання мобільних пристроїв (BYOD) та правила поведінки посадовців у соціальних мережах.	
ДНР – 03 ДРН – 07	**4. Основи захисту інформації.**	10
	4.1. Основи технічного та криптографічного захисту інформації: цілі, завдання, нормативні документи..	
	4.2. Етапи створення системи захисту інформації в організації.	
	4.3. Моделювання загроз, визначення моделі порушника та оцінка ризиків для інформаційно-комунікаційних систем.	
	4.4. Рівні інформаційної безпеки. Технологія побудови системи захисту. Засоби виявлення атак і захисту програмного забезпечення. Безпека корпоративних інформаційних систем.	
ДРН – 03 ДРН – 07	**5. Організаційно-управлінські аспекти інформаційної безпеки**	10
	5.1. Аналіз інформаційного середовища: аудит активів, категоріювання ресурсів та планування заходів з обробки інформаційних ризиків.	
	5.2. Організація безпечної роботи з персоналом: класифікація співробітників за рівнем доступу та превентивні заходи щодо внутрішніх порушників.	
	5.3. Концептуальні засади політик безпеки: термінологія, класифікація моделей захисту та алгоритм формування внутрішньої нормативної бази.	
	5.4. Вимоги до заходів, методів і засобів захисту інформації. Документальне оформлення політики безпеки	
	5.4. Контроль ефективності: внутрішній аудит та оцінка відповідності системи управління інформаційною безпекою.	
ДРН – 04 ДРН – 06	**6. Гібридні загрози, боротьба з дезінформацією та маніпулятивним контентом.**	8
	6.1. Сутність гібридної війни в інформаційному просторі: дезінформація та пропаганда.	
	5.2. Методологія розпізнавання ІПСО та алгоритми протидії зовнішній інформаційній агресії.	
	5.3. Роль стратегічних комунікацій у забезпеченні національної безпеки та побудова довіри через прозорість влади.	
ДРН – 03 ДРН – 05 ДРН – 06	**Тема 7. Майбутнє кібербезпеки: штучний інтелект та новітні виклики.**	8
	7.1. Штучний інтелект у сфері безпеки: автоматизація	

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
ДРН – 07	моніторингу загроз та використання ШІ в системах підтримки рішень.	
	7.2. Новітні ризики: дипфейки, квантові загрози та еволюція методів соціальної інженерії.	
	7.3. Стратегічні напрями зміцнення цифрової стійкості публічного управління в Україні.	
	Практичні заняття	**60**
ДРН – 01 ДРН – 02 ДРН – 03	1. Правовий аналіз інцидентів витоку інформації та відповідальності розпорядників систем.	8
ДРН – 04 ДРН – 06	2. Розпізнавання ІПСО та алгоритм реагування на дезінформаційні кампанії.	10
ДРН – 03 ДРН – 05 ДРН – 07	3. Проектування організаційної структури захисту інформації в органах місцевого самоврядування. Ідентифікація вразливостей. Визначення вірогідності реалізації вразливостей.	12
ДРН – 03 ДРН – 05 ДРН – 07	4. Створення моделі загроз та моделі порушника для органу публічного управління.	12
ДРН – 03 ДРН – 05 ДРН – 07	5. Рекомендації з управління ризиками. Розробка політик інформаційної безпеки	10
ДРН – 01 ДРН – 03 ДРН – 07	6. Презентація результатів роботи щодо розробки системи управління інформаційною та кібербезпекою	8
	РАЗОМ	**120**

6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

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

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

6.1 Шкали

Оцінювання навчальних досягнень здобувачів вищої освіти НТУ «ДП» здійснюється за рейтинговою (100-бальною) та інституційною шкалами.

Остання необхідна (за офіційною відсутністю національної шкали) для конвертації (переведення) оцінок мобільних студентів.

Шкали оцінювання навчальних досягнень студентів НТУ «ДП»

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

Загальні критерії досягнення результатів навчання відповідають описам 6-го кваліфікаційного рівня НРК.

6.2 Засоби та процедури

Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь, комунікації, автономності та відповідальності здобувача вищої освіти за вимогами НРК до 6-го кваліфікаційного рівня (для першого (бакалаврського) рівня вищої освіти) 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 2).

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.

Засоби діагностики (контрольні завдання) для поточного та підсумкового контролю дисципліни затверджуються кафедрою.

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

Засоби діагностики та процедури оцінювання

ПОТОЧНИЙ КОНТРОЛЬ			**ПІДСУМКОВИЙ КОНТРОЛЬ**	
навчальне заняття	**засоби діагностики**	**процедури**	**засоби діагностики**	**процедури**
лекції	контрольні завдання за кожною темою	виконання завдання під час лекцій	комплексна контрольна робота (ККР)	визначення середньозваженого результату поточних контролів; виконання ККР під час заліку за бажанням здобувача вищої освіти
практичні	командне / індивідуальне завдання	виконання завдань під час самостійної роботи		

Під час поточного контролю лекційні заняття оцінюються шляхом визначення якості виконання контрольних конкретизованих завдань. Практичні

заняття оцінюються якістю виконання контрольного або командного / індивідуального завдання.

Якщо зміст певного виду занять підпорядковано декільком складовим, то інтегральне значення оцінки може визначатися з урахуванням вагових коефіцієнтів, що встановлюються викладачем.

За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, підсумковий контроль здійснюється без участі здобувача вищої освіти шляхом визначення середньозваженого значення поточних оцінок.

Незалежно від результатів поточного контролю кожен здобувач вищої освіти під час заліку має право виконувати ККР, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.

Кількість конкретизованих завдань ККР повинна відповідати відведеному часу на виконання. Кількість варіантів ККР має забезпечити індивідуалізацію завдання.

Значення оцінки за виконання ККР визначається середньою оцінкою складових (конкретизованих завдань) і є остаточним.

Інтегральне значення оцінки виконання ККР може визначатися з урахуванням вагових коефіцієнтів, що встановлюється кафедрою для кожної складової опису кваліфікаційного рівня НРК.

6.3 Критерії

Реальні результати навчання здобувача вищої освіти ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії студента для демонстрації досягнення результатів навчання.

Для оцінювання виконання контрольних завдань під час поточного контролю лекційних і практичних занять в якості критерію використовується коефіцієнт засвоєння, що автоматично адаптує показник оцінки до рейтингової шкали:

$$Oi = 100\ a/m,$$

де a – число правильних відповідей або виконаних суттєвих операцій відповідно до еталону рішення; m – загальна кількість запитань або суттєвих операцій еталону.

Індивідуальні завдання та комплексні контрольні роботи оцінюються експертно за допомогою критеріїв, що характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.

Зміст критеріїв спирається на компетентністні характеристики, визначені НРК для освітньо-наукового рівня вищої освіти (подано нижче).

Загальні критерії досягнення результатів навчання для 6-го кваліфікаційного рівня за НРК (бакалавр)

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	Знання	
♦ концептуальні наукові та практичні знання, критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: - концептуальних знань; - високого ступеню володіння станом питання; - критичного осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності	95-100
	Відповідь містить негрубі помилки або описки	90-94
	Відповідь правильна, але має певні неточності	85-89
	Відповідь правильна, але має певні неточності й недостатньо обґрунтована	80-84
	Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена	74-79
	Відповідь фрагментарна	70-73
	Відповідь демонструє нечіткі уявлення здобувача вищої освіти про об'єкт вивчення	65-69
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
	Уміння/навички	
♦ поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв’язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання	Відповідь характеризує уміння: - виявляти проблеми; - формулювати гіпотези; - розв'язувати проблеми; - обирати адекватні методи та інструментальні засоби; - збирати та логічно й зрозуміло інтерпретувати інформацію; - використовувати інноваційні підходи до розв’язання завдання	95-100
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності з негрубими помилками	90-94
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але	74-79

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	має певні неточності при реалізації трьох вимог	
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння/навички застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	рівень умінь/навичок незадовільний	<60
	Комунікація	
♦ донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації; ♦ збір, інтерпретація та застосування даних; ♦ спілкування з професійних питань, у тому числі іноземною мовою, усно та письмово	Вільне володіння проблематикою галузі. Зрозумілість відповіді (доповіді). Мова: - правильна; - чиста; - ясна; - точна; - логічна; - виразна; - лаконічна. Комунікаційна стратегія: - послідовний і несуперечливий розвиток думки; - наявність логічних власних суджень; - доречна аргументації та її відповідність відстоюваним положенням; - правильна структура відповіді (доповіді); - правильність відповідей на запитання; - доречна техніка відповідей на запитання; - здатність робити висновки та формулювати пропозиції	95-100
	Достатнє володіння проблематикою галузі з незначними хибами. Достатня зрозумілість відповіді (доповіді) з незначними хибами. Доречна комунікаційна стратегія з незначними хибами	90-94
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п’ять вимог)	74-79
	Задовільне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Часткове володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев’ять вимог)	65-69
	Фрагментарне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
Відповідальність і автономія		
♦ управління складною технічною або професійною діяльністю чи проектами; ♦ спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах; ♦ формування суджень, що враховують соціальні, наукові та етичні аспекти; ♦ організація та керівництво професійним розвитком осіб та груп; ♦ здатність продовжувати навчання із значним ступенем автономії	Відмінне володіння компетенціями менеджменту особистості, орієнтованих на: 1) управління комплексними проектами, що передбачає: - дослідницький характер навчальної діяльності, позначена вмінням самостійно оцінювати різноманітні життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію; - здатність до роботи в команді; - контроль власних дій; 2) відповідальність за прийняття рішень в непередбачуваних умовах, що включає: - обґрунтування власних рішень положеннями нормативної бази галузевого та державного рівнів; - самостійність під час виконання поставлених завдань; - ініціативу в обговоренні проблем; - відповідальність за взаємовідносини; 3) відповідальність за професійний розвиток окремих осіб та/або груп осіб, що передбачає: - використання професійно-орієнтовних навичок; - використання доказів із самостійною і правильною аргументацією; - володіння всіма видами навчальної діяльності; 4) здатність до подальшого навчання з високим рівнем автономності, що передбачає: - ступінь володіння фундаментальними знаннями;	95-100

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	- самостійність оцінних суджень; - високий рівень сформованості загальнонавчальних умінь і навичок; - самостійний пошук та аналіз джерел інформації	
	Упевнене володіння компетенціями менеджменту особистості (не реалізовано дві вимоги)	90-94
	Добре володіння компетенціями менеджменту особистості (не реалізовано три вимоги)	85-89
	Добре володіння компетенціями менеджменту особистості (не реалізовано чотири вимоги)	80-84
	Добре володіння компетенціями менеджменту особистості (не реалізовано шість вимог)	74-79
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано сім вимог)	70-73
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано вісім вимог)	65-69
	Рівень відповідальності і автономії фрагментарний	60-64
	Рівень відповідальності і автономії незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Комп'ютерне та мультимедійне обладнання.

Активований корпоративний акаунт НТУ «ДП» (student.i.p@nmu.one).

Microsoft Office 365. Застосунки Microsoft Office: Teams, Forms, Whiteboard, OneNote.

Платформа дистанційного навчання НТУ «ДП» Moodle.

Підключення до Internet.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Нормативні документи

1. Конституція України.
2. Закон України «Про інформацію» від 2.10.1992 р.
3. Закон України «Про державну таємницю» від 21.01.1994 р.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
5. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р.

6. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.
7. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII.
8. Стратегія кібербезпеки України. Затверджено Указом Президента України від 14 травня 2021 року № 447/2021.
9. Стратегія інформаційної безпеки України. Затверджено Указом Президента України від 15 жовтня 2021 року № 685/2021.
10. Доктрина інформаційної безпеки України : Затверджено Указом Президента України від 25.02.2017 р. № 47/2017.
11. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
12. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
13. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.
14. ДСТУ ISO/IEC 27000:2017 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів (ISO/IEC 27000:2016, IDT).
15. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
16. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
17. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).
18. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT)
19. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

Додаткові

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. Інформаційна безпека. Менеджмент інформаційної безпеки держави [Електронний ресурс]: курс лекцій: навч. посіб. / В. О. Ананьїн, В. В.

Горлинський, А. В. Гангал. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,73 Мбайт). – Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського 2025. – 140 с.

3. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

4. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, М.В. Ворохоб. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 1016 с

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

6. Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід : монографія / ред. С. Чернов, В. Воронкова, В. Банах, та ін. ; ЗДІА. Запоріжжя : ЗДІА, 2017. 603 с.

7. Савченко, О. С. Проблеми запровадження цифровізації у систему публічного управління. Таврійський науковий вісник. Серія: Публічне управління та адміністрування, 2022, № 3, 102–108. URL: https://doi.org/10.32851/tnv-pub.2022.3.14.

8. Дячек, О., Рябченко, К., & Доценко, А. Безпека даних в інформаційно-комунікаційному середовищі та її складність для нових бізнес-моделей. Економіка та суспільство, 2022, 38. URL: https://doi.org/10.32782/2524-0072/2022-38-16.

9. Герасимюк, К. Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування, 2021, № 3 (97), 36–40. URL: https://doi.org/10.26642/ema-2021-3(97)-36-40.

10. Хох В. Д. Дослідження методів аудиту систем управління інформаційною безпекою / В. Д. Хох, Є. В. Мелешко, О.А. Смірнов // Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава : ПНТУ, 2017. Т 1 (41). С. 38–42.

11. Марущак А. Вплив тіньових інформаційних технологій на інформаційну безпеку суб'єкта господарювання / А. Марущак, О. Скіцько // Безпека інформації. 2018. Т. 24, № 1. С. 69–74.

12. Науменко Н. Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону / Н. Ю. Науменко, В. І. Дубницький // Вестник экономической науки Украины. 2019. № 1 (36). С. 35–39.

13. Термінологічний словник з питань технічного захисту інформації /за ред. Проф. В.О. Хорошка 3-є видання. Київ: Поліграф Колсалтинг, 2003. 268 с.

14. Домарев В.В. Безопасность информационных технологий. Системный подход. Київ: ТИД ДС, 2004. 992 с.

15. Антонюк А.О. Основи захисту інформації в автоматизованих

системах. Навч. посібн. Київ: КМ Академія, 2003. 244 с.

16. Защита информации и безопасность компьютерных систем/ В.В. Домарёв. Київ: Диа Софт», 1999. 480 с.

17. Дорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно «Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)», США, «Оранжевая книга». Бизнес и безопасность, 1998, № 1, с. 19–21.

Інформаційні ресурси

1. CERT-UA. Команда реагування на комп’ютерні надзвичайні події України. URL: https://cert.gov.ua.
2. Державна служба спеціального зв’язку та захисту інформації України. URL: http://www.dsszzi.gov.ua.
3. ТОВ «ТЗІ». URL: http://tzi.com.ua
4. Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології». URL: https://vaibit.org.ua.
5. Інфобезпека. URL: http://www.infobezpeka.com.
6. ЕПОС. URL: http://www.epos.ua.
7. Міністерство цифрової трансформації України. Центральний засвідчувальний орган. URL: http://czo.gov.ua.
8. ISO/IEC 27001. URL: https://www.iso27001security.com.

Навчальне видання

Робоча програма вибіркової навчальної дисципліни
«Інформаційна безпека в публічному управлінні»
для здобувачів першого (бакалаврського) рівня вищої освіти
спеціальностей 281 Публічне управління та адміністрування

Розробник:
Кравцов Олег Валентинович

Підготовлено до виходу в світ
у Національному технічному університеті
«Дніпровська політехніка».
Свідоцтво про внесення до Державного реєстру ДК № 1842
4960050, м. Дніпро, просп. Д. Яворницького, 19