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

Кафедра державного управління і місцевого самоврядування

«ЗАТВЕРДЖЕНО»
завідувач кафедри

Чикаренко І.А. _____

«31» серпня 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Інформаційна безпека в цифровому врядуванні»

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

Викладачі: д.держ.упр., проф. Квітка С.А., 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»
2023

Робоча програма навчальної дисципліни «Інформаційна безпека в цифровому врядуванні» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 281 Публічне управління та адміністрування / Нац. техн. ун-т. «Дніпровська політехніка», каф. державного управління і місцевого самоврядування. Дніпро : НТУ «ДП», 2023. 16 с.

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

Робоча програма регламентує:
– мету дисципліни;
– дисциплінарні результати навчання, сформовані на основі трансформації очікуваних результатів навчання освітньої програми;
– 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.

Погоджено рішенням науково-методичної комісії спеціальності 281 «Публічне управління та адміністрування» (протокол № 7 від 30 червня 2023 р.).

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета дисципліни «Інформаційна безпека в публічному управлінні» – формування у здобувачів вищої освіти комплексу теоретичних знань у сфері інформаційної безпеки, розвиток професійних компетентностей щодо забезпечення належного рівня інформаційної безпеки та протидії кіберзагрозам в органах публічного управління в умовах цифрової трансформації суспільства та держави.

2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Шифр ДРН	**Дисциплінарні результати навчання (ДРН)**
	Зміст
ДРН – 01	Продемонструвати *знання:* предмету і завдань дисципліни; термінології; основних понять та принципів в сфері інформаційної та кібербезпеки.
ДРН – 02	Продемонструвати *розуміння:* головних характеристик інформації як об’єкту захисту; правових, організаційних і технічних заходів щодо захисту інформації; проблематики і специфіки загроз ІБ.
ДРН – 03	Продемонструвати *розуміння:* системного підходу до опису ІБ, мети та етапів робіт щодо розбудови ІБ в умовах цифрової трансформації.
ДРН – 04	Продемонструвати вміння *аналізувати* та *оцінювати* інформаційні ризики.
ДРН – 05	Продемонструвати здатність практично *застосовувати* настанови міжнародних та національних стандартів інформаційної та кібербезпеки.
ДРН – 06	Продемонструвати здатність *розробляти* практичні рекомендації щодо реалізації системи управління інформаційною безпекою.
ДРН – 07	Продемонструвати практичні навички щодо *розроблення* політик безпеки.

3 БАЗОВІ ДИСЦИПЛІНИ

Міждисциплінарні зв’язки: вивчення курсу ґрунтуються на знаннях, отриманих з вивчених дисциплін за попереднім рівнем вищої освіти.

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	1. Загальні основи інформаційної безпеки	12
	1.1. Сутність поняття інформація. Інформаційні ресурси та процеси. Категоріювання інформації та інформаційних систем.	
	1.2. Поняття інформаційної безпеки (ІБ). Види ІБ.	
	1.3. Основні принципи формування ІБ в Україні.	
	1.4. Загрози ІБ та об’єкти захисту інформації.	
	1.5. Проблеми та особливості забезпечення інформаційної безпеки в воєнний та повоєнний період.	
ДРН – 02 ДРН – 03	**2. Характеристика інформаційної безпеки**	12
	2.1. Характеристика загроз та вразливостей інформаційної безпеки. Види загроз безпеки інформації.	
	2.2. Методи забезпечення інформаційної безпеки. Основні принципи забезпечення інформаційної безпеки в органах публічного управління.	
	2.3. Загрози безпеці інформації та сучасний стан її захисту.	
	2.4. Система технічного захисту інформації в Україні. Основні напрямки державної політики у сфері ІБ.	
ДРН – 03 ДРН – 05	**Тема 3. Стандарти інформаційної безпеки**	12
	3.1. Вітчизняні та міжнародні практика інформаційної та кібербезпеки.	
	3.2. Вітчизняна нормативно-правова база інформаційної та кібербезпеки.	

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
	3.3. Зарубіжні стандарти інформаційної безпеки.	
	3.4. Серія стандартів ISO 27xxx.	
ДНР – 01 ДРН – 04 ДНР – 05 ДРН – 06	**4. Забезпечення систем захисту інформації**	12
	4.1. Методи і засоби забезпечення інформаційної безпеки органах публічного управління. Багаторівнева модель об'єктів інформаційної безпеки.	
	4.2. Технічні засоби захисту передавання інформації. Технічні методи захисту інформації в інформаційно-комунікаційних системах. Термінологія галузі технічного захисту інформаційних систем.	
	4.3. Загальні вимоги і етапи розроблення технічного завдання на створення комплексної системи захисту інформації (КСЗІ). Зміст загальних підрозділів ТЗ КСЗІ та зміст роботи з розроблення проекта створення і введенні в дію КСЗІ.	
	4.4. Рівні інформаційної безпеки. Технологія побудови системи захисту. Засоби виявлення атак і захисту програмного забезпечення. Безпека корпоративних інформаційних систем.	
ДНР – 01 ДРН – 02 ДРН – 04 ДРН – 05 ДРН – 07	**5. Управління інформаційною безпекою**	12
	5.1. Аналіз структури, функцій інформаційного об’єкту. Інвентаризація та категоріювання активів. Оцінювання та аналіз інформаційних ризиків. Планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ.	
	5.2. Організація роботи з персоналом. Класифікація персоналу за мірою впливу на стан ІБ. Профілактика розкрадання інформації співробітниками організації.	
	5.3. Визначення та основні поняття політики безпеки. Види моделей політики інформаційної безпеки, основні її принципи та послідовність розроблення.	
	5.4. Концептуальні засади організації захисту інформації з обмеженим доступом. Організаційно-правові основи та політика безпеки в сфері захисту інформації з обмеженим доступом.	
	5.5. Вимоги до заходів, методів і засобів захисту інформації. Документальне оформлення політики безпеки	
	5.6. Проблеми та особливості забезпечення інформаційної безпеки в воєнний та повоєнний період.	
	Практичні заняття	**60**
ДРН – 01 ДРН – 02 ДРН – 03	Опис системи. Ідентифікація загроз.	12
ДРН – 02 ДРН – 03	Ідентифікація вразливостей. Визначення вірогідності реалізації вразливостей.	12

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, *години*
ДРН – 05		
ДРН – 02 ДРН – 03 ДРН – 04 ДРН – 05	Аналіз дій. Розрахунок ризику.	12
ДРН – 04 ДРН – 05 ДРН – 06 ДРН – 07	Рекомендації з управління ризиками. Розробка політик інформаційної безпеки	12
ДРН – 06 ДРН – 07	5. Презентація результатів командної роботи щодо розробки системи управління інформаційною та кібербезпекою	12
	РАЗОМ	**120**

5.2 Командне / індивідуальне завдання

Командне / індивідуальне завдання «**Розроблення програми розвитку системи управління інформаційною та кібербезпекою»** полягає у розробленні, презентації результатів та захисті здобувачами вищої освіти концепції програми розвитку закладу охорони здоров'я. (***Мета*** індивідуального завдання – розвинути здатність практично застосовувати відповідні методи та інструменти управління у сфері розроблення системи управління інформаційною та кібербезпекою). Вітається робота в команді.

Форма проведення: розроблення, презентація та захист (відповіді на запитання, дискусія) командного / індивідуального завдання перед аудиторією (бажано використовувати MS PowerPoint).

Зміст індивідуального завдання:

На прикладі окремої організації, пов'язаної з вашим життям та / або професійною діяльністю, розробити концепцію політики інформаційної безпеки, результатом реалізації якої буде позитивний ефект для певної території / галузі / громади.

Для представлення результатів виконання завдання необхідно заповнити відповідний шаблон, який розміщено у застосунку Teams MS Office та на дистанційній платформі Moodle.

6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Сертифікація досягнень здобувачів вищої освіти здійснюється за допомогою прозорих процедур, що ґрунтуються на об'єктивних критеріях

відповідно до Положення університету «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

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

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 7-го кваліфікаційного рівня (для другого (магістерського) 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 7-го кваліфікаційного рівня за НРК (магістр)

Опис кваліфікаційного рівня	**Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії**	**Показник оцінки**
	Знання	
♦ спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: – спеціалізованих концептуальних знань на рівні новітніх досягнень; – критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей	95-100
	Відповідь містить не грубі 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 студента про об’єкт вивчення	65-69
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
	***Уміння*/навички**	
♦ спеціалізовані уміння/навички розв’язання проблем, необхідні для проведення досліджень та/або провадження інноваційної	Відповідь характеризує уміння: – виявляти проблеми; – формулювати гіпотези; – розв’язувати проблеми; – оновлювати знання; – інтегрувати знання; – провадити інноваційну діяльність; – провадити наукову діяльність	95-100

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
діяльності з метою розвитку нових знань та процедур; ♦ здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; ♦ здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності з не грубими 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 має певні неточності при реалізації трьох вимог	74-79
	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		
♦ зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	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; – використання іноземних мов у професійній діяльності	95-100
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79

Опис кваліфікаційного рівня	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показник оцінки
	Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
Відповідальність і автономія		
♦ управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів; □ відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів; □ здатність продовжувати навчання з високим ступенем автономії	Відмінне володіння компетенціями: – використання принципів та методів організації діяльності команди; – ефективний розподіл повноважень в структурі команди; – підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини); – стресовитривалість; – саморегуляція; – трудова активність в екстремальних ситуаціях; – високий рівень особистого ставлення до справи; – володіння всіма видами навчальної діяльності; – належний рівень фундаментальних знань; – належний рівень сформованості загальнонавчальних умінь і навичок	95-100
	Упевнене володіння компетенціями відповідальності і автономії з незначними хибами	90-94
	Добре володіння компетенціями відповідальності і автономії (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями відповідальності і автономії (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями відповідальності і автономії (не реалізовано чотири вимоги)	74-79
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано п'ять вимог)	70-73
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями відповідальності і автономії (рівень фрагментарний)	60-64
	Рівень відповідальності і автономії незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

1. Технічні засоби навчання (комп'ютерне та мультимедійне обладнання).
2. Дистанційна платформа Moodle.
3. MS Office (застосунок Teams).

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні

1. Захист інформації в публічному управлінні та адмініструванні : конспект лекцій / уклад. О.В. Кравцов. Дніпро : ДРІДУ НАДУ, 2019. 62 с. 1 електрон. опт. диск (CD-ROM).

2. Методичні вказівки до виконання практичних завдань з дисципліни «Захист інформації в публічному управлінні та адмініструванні». Створення системи менеджменту інформаційної безпеки / уклад. О.В. Кравцов. Дніпро : ДРІДУ НАДУ, 2019. 28 с. 1 електрон. опт. диск (CD-ROM).

Нормативні документи

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

3. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

4. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

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

6. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 14.05.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 15.10.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text.

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. Азарова А. О., Ткачук Л. М., Нікіфорова Л. О. та ін. Публічне управління та адміністрування в контексті захисту його інформаційного простору. *Вісник ЖДТУ. Серія «Економіка, управління та адміністрування».* 2019. № 2. С. 149–155.

2. Антонюк А.О. Основи захисту інформації в автоматизованих системах : навч. посіб. Київ: КМ Академія, 2003. 244 с.

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

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

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

6. 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.

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

8. Інформаційна безпека держави : підручник / В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; в 2 т. Т.1. / за заг. ред.. В. В. Остроухова. Київ : ДНУ «Книжкова палата Україна», 2016. 264 с.

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

10. Науменко Н. Ю., Дубницький В. І. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. *Вісник економічної науки України*. 2019. № 1 (36). С. 35–39.

11. 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.

12. 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.

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

14. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною. *Системи управління, навігації та зв'язку : зб. наук. пр*. Полтава : ПНТУ, 2017. Т 1 (41). С. 38–42.

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 другого (магістерського) рівня вищої освіти
спеціальності 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