НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра комп'ютерних та інформаційних технологій і систем

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Богдан КОРОБКО
«28» 08 2026 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ»

(назва навчальної дисципліни)

підготовки **Доктор філософії**
(назва ступеня вищої освіти)
Освітньо-наукової програми **ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА**
(назва освітньої програми)

Спеціальності **G5 ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ, ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА**
(код і назва спеціальності)

Полтава
2026 рік

Робоча програма навчальної дисципліни «Методологія захисту інформації в інфокомунікаційних системах» для здобувачів освіти спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка» третього (освітньо-наукового) рівня вищої освіти.

Розробники: Здоренко Юрій Миколайович, кандидат технічних наук, доцент кафедри комп'ютерних та інформаційних технологій і систем.

Погоджено

Погоджено:
Гарант освітньої програми _____ Олександр ШЕФЕР

Робоча програма затверджена на засіданні кафедри комп'ютерних та інформаційних технологій і систем

Протокол від « 26 » 08 2026 року № 1

Завідувач кафедри комп'ютерних та інформаційних технологій і систем

« 26 » 08 2026 року _____ Олена ДВІРНА

Схвалено навчально-методичною комісією навчально-наукового інституту інформаційних технологій та робототехніки

Протокол від « 27 » 08 2026 року № 1

Голова навчально-методичної комісії навчально-наукового інституту інформаційних технологій та робототехніки

_____(Олександр ШЕФЕР)

« 27 » серпня 2026 року

© Здоренко Ю.М., 2026 рік
© Національний університет
імені Юрія Кондратюка, 2026 рік

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="3">Найменування показників</td><td rowspan="3">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">форма здобуття освіти</td></tr>
<tr><td>денна</td><td>заочна</td></tr>
<tr><td>Кількість кредитів – 3</td><td rowspan="2">Галузь знань
G Інженерія, виробництво та будівництво</td><td colspan="2" rowspan="2">вибіркова</td></tr>
<tr><td>Загальна кількість годин – 90</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="8">Спеціальність
G5 «Електроніка, електронні комунікації, приладобудування та радіотех-ніка»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>2/3й</td><td>2/3й</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td colspan="2">Семестр</td></tr>
<tr><td>4/5</td><td>4/5</td></tr>
<tr><td rowspan="11">Індивідуальне завдання – не передбачено</td><td colspan="2">Лекції</td></tr>
<tr><td>16 год.</td><td>4 год.</td></tr>
<tr><td rowspan="10">Ступінь вищої освіти
<u>третій</u>
<u>(освітньо-науковий)</u></td><td colspan="2">Практичні</td></tr>
<tr><td>8 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>66 год.</td><td>82 год.</td></tr>
<tr><td colspan="2">Індивідуальна робота:</td></tr>
<tr><td colspan="2">0</td></tr>
<tr><td colspan="2">Вид контролю: диф. залік</td></tr>
</table>

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

для денної форми здобуття освіти – 24/66
для заочної форми здобуття освіти – 8/82

2. Мета навчальної дисципліни

Мета – формування базових уявлень, знань і умінь в області сучасних методологічних аспектів захисту інформації, а саме, вмінь застосовувати сукупність методів для створення і використання ефективної системи захисту інформаційних ресурсів в інформаційно-комунікаційних системах на основі використання сучасних технологій.

Під час вивчення даної дисципліни набуваються такі компетентності:

Здатність здобувача продукувати нові ідеї, розв'язувати комплексні проблеми у галузі електроніки, автоматизації та електронних комунікацій, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

Здатність критично аналізувати, оцінювати і синтезувати нові та комплексні наукові рішення.

Здатність визначати й аналізувати актуальні наукові проблеми та застосовувати сучасні підходи до вирішення складних дослідницьких завдань у межах професійної та наукової інноваційної діяльності.

Здатність виконувати оригінальні дослідження в області телекомунікацій та радіотехніки, отримувати нові наукові результати щодо вирішення актуальних завдань і проблем із використанням відповідного науково-методичного апарату.

Уміння аналізувати функціонування систем передачі й захисту інформації та інтерпретувати результати аналізу, застосовувати інтелектуальні методи для оцінки ефективності їхніх характеристик та робити обґрунтовані висновки щодо покращення пропускної здатності, якості та надійності каналів зв'язку.

Здатність застосовувати у професійній діяльності теоретичні знання, інструменти та методи для здійснення ефективного інформаційного пошуку, структурування інформації, формулювання наукових та професійних завдань в області телекомунікацій та радіотехніки.

Здатність впровадження новітніх технологій у процесі проєктування перспективних та модернізації існуючих радіотехнічних та телекомунікаційних систем і мереж та захисту інформації.

3. Передумови для вивчення дисципліни

Передумовою для вивчення навчальної дисципліни є дисципліни, що формують основу підготовки здобувачів вищої освіти другого (магістерського) рівня та попередньо опановані дисципліни третього (освітньо-наукового) рівня вищої освіти.

4. Очікувані результати навчання з дисципліни

У результаті вивчення навчальної дисципліни «Методологія захисту інформації в інфокомунікаційних системах» аспіранти повинні сформувати такі програмні результати навчання (знання й уміння):

Мати необхідні теоретичні та методичні знання в сфері телекомунікацій та радіотехніки і на межі предметних галузей, для проведення наукових і прикладних досліджень на високому рівні сучасних досягнень галузі електроніки, автоматизації та електронних комунікацій.

Визначати актуальні наукові та практичні проблеми у сфері телекомунікацій та радіотехніки.

Вміти розробляти, обґрунтовувати та впроваджувати інноваційні проекти і технічні рішення у сфері телекомунікацій та радіотехніки, застосовуючи отримані наукові знання та навички.

5. Критерії оцінювання результатів навчання

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

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

Сума балів	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 вивченні інших дисциплін.	**Високий**, що повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.
82 – 89	**B**	**Добре**	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.	**Достатній**, що забезпечує здобувачу самостійне вирішення основних практичних задач.
74 - 81	**C**	**Добре**	Здобувач загалом добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для рішення характерних/типових практичних завдань на професійному рівні. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають ускладнення.	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.
64 - 73	**D**	**Задовільно**	Здобувач засвоїв основний	**Середній**,

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

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання є:

поточний контроль

- *тестування*
- *виконання практичних робіт*
- *виконання завдань самостійної роботи*

модульний контроль

- *тестування*

підсумковий контроль

- *диференційований залік*

1. Програма навчальної дисципліни

Змістовий модуль 1. Методологія захисту інформації в інформаційно-телекомунікаційних системах.

Тема 1. Методологічні аспекти захисту інформації в ІТС.

Форми та способи захисту інформації в ІТС. Методологічні основи інформаційної безпеки.

Тема 2. Принципи кібернетичного впливу в інформаційно-телекомунікаційних системах. Природа кібернетичного впливу в інформаційно-телекомунікаційних системах. Огляд методів кібернетичного впливу.

Практичне заняття № 1

Тема 3. Методики аналізу трафіку в інформаційно-телекомунікаційних системах. Можливості та базові прийоми застосування утиліти tcpdump. Аналіз трафіку транспортного та мережевого рівня. Аналіз трафіку прикладного рівня. Програмне забезпечення Wireshark для аналізу мережевого трафіку.

Практичне заняття № 2

Тема 4. Методи та засоби захисту інформації при роботі з системами керування базами даних. Методи аутентифікації користувачів СКБД. Методи та засоби захисту даних в сучасних СКБД. Аналіз вразливостей.

Практичне заняття № 3

Тема 5. Методи технічного захисту інформації. Сучасні комплекси технічного захисту інформації. Складові елементи ТЗІ. Характеристики комплексів ТЗІ.

Змістовий модуль 2. Криптографічний захист інформації в ІТС та методи стеганографії.

Тема 6. Сучасні аспекти криптографічного захисту інформації. Сучасні методи криптографічного захисту інформації. Необоротне шифрування. Програмно-технічні методи автентифікації. Поняття про електронний цифровий підпис**.**

Тема 7. Методи захисту інформації з використанням служб прикладного рівня SSH та SFTP. Призначення та зміст пакета OpenSSH. Конфігурування служби SSH. Основні прийоми застосування клієнтських програм пакетів SSH та SFTP.

Практичне заняття №4

Тема 8. Управління ризиками ІБ. Методи аналізу кіберінцидентів. Аналіз ризиків інформаційної безпеки в інфокомунікаційних системах. Контроль інформаційної безпеки. Способи аналізу вторгнень. Виявлення та усунення вразливостей ІТС.

8. Структура навчальної дисципліни

а) для денної форми здобуття освіти

Назви змістовних модулів і тем	Кількість годин					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1 Методологія захисту інформації в інформаційно-телекомунікаційних системах.						
Тема 1. Методологічні аспекти захисту інформації в ІТС	12	2	2			8
Тема 2. Принципи кібернетичного впливу в інформаційно-телекомунікаційних системах.	10	2				8
Тема 3. Методики аналізу трафіку в інформаційно-телекомунікаційних системах.	10	2				8
Тема 4. Методи та засоби захисту інформації при роботі з системами керування базами даних.	12	2	2			8
Тема 5. Методи технічного захисту інформації. Сучасні комплекси технічного захисту інформації.	12	2	2			8
Разом за змістовим модулем 1	**56**	**10**	**6**	**0**	**0**	**40**
Змістовий модуль 2 Криптографічний захист інформації в ІТС та методи стеганографії.						
Тема 6. Сучасні аспекти криптографічного захисту інформації.	12	2	2			8
Тема 7. Сучасні аспекти криптографічного захисту інформації.	10	2				8
Тема 8. Управління ризиками ІБ. Методи аналізу кіберінцидентів.	12	2				10
Разом за змістовим модулем 2	**34**	**6**	**2**	**0**	**0**	**26**
Усього годин	***90***	***16***	***8***	***0***	***0***	***66***

б) для заочної форми здобуття освіти

Назви змістовних модулів і тем	Кількість годин					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1 Теоретичні основи інтелектуальної обробки та адаптивності						
Тема 1. Методологічні аспекти захисту інформації в ІТС	14	2	2			10
Тема 2. Принципи кібернетичного впливу в інформаційно-телекомунікаційних системах.	10					10
Тема 3. Методики аналізу трафіку в інформаційно-телекомунікаційних системах.	10					10
Тема 4. Методи та засоби захисту інформації при роботі з системами керування базами	10					10

даних.						
Тема 5. Методи технічного захисту інформації. Сучасні комплекси технічного захисту інформації.	10					10
Разом за змістовим модулем 1	**54**	**2**	**2**	**0**	**0**	**50**
Змістовий модуль 2 Високопродуктивна модулярна обробка в системі залишкових класів						
Тема 6. Сучасні аспекти криптографічного захисту інформації.	14	2	2			10
Тема 7. Сучасні аспекти криптографічного захисту інформації.	10					10
Тема 8. Управління ризиками ІБ. Методи аналізу кіберінцидентів.	12					12
Разом за змістовим модулем 2	**36**	**2**	**2**	**0**	**0**	**32**
Усього годин	***90***	***4***	***4***	***0***	***0***	***82***

9. Перелік питань для семінарських занять

№ заняття	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
-	Семінарські заняття не передбачені*	-	-

10. Перелік питань для практичних занять

№ заняття	Тема заняття та перелік питань	Кількість годин	
		для денної форми	заочної форми
Модуль 1			
1	Практичне заняття 1. Дослідження структури інформаційно-телекомунікаційної системи. Методи тестування на вразливості вузлів ІТМ.	2	2
2	Практичне заняття 2. Методи та засоби захисту даних в СКБД. Резервне зберігання даних. Створення образу системи. Шифрування даних.	2	-
3	Практичне заняття 3. Базові методи використання системи PGP для захисту даних при передачі повідомлень. Перевірка цілісності документа з використанням алгоритму розрахунку контрольної суми.	2	-
Модуль 2			
4	Практичне заняття 4. Базові методи розгортання та використання захищених служб віддаленого доступу SSH та SFTP для захисту інформації.	2	2
Всього:		**8**	**4**

11. Перелік питань для лабораторних занять

№ заняття	Тема заняття та перелік питань	Кількість годин для	
		денної форми	заочної форми
Лабораторні заняття не передбачені			

12. Самостійна робота

Мета самостійної роботи полягає у формуванні у здобувачів вищої освіти здатності до самостійного поглиблення та закріплення теоретичних знань з методології захисту інформації в інфокомунікаційних системах, набутті практичних навичок застосування методів і засобів забезпечення інформаційної безпеки, аналізу загроз та оцінювання ефективності механізмів захисту інформації, а також розвитку дослідницьких компетентностей, необхідних для проведення самостійних наукових досліджень у сфері електронних комунікацій і радіотехніки на рівні доктора філософії.

Види самостійної роботи аспіранта:

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

Питання для самостійного вивчення аспірантами

№ з/п	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
1	**Тема 1. Методологічні аспекти захисту інформації в ІТС.** Нормативно-правове забезпечення захисту інформації в ІТС. Методи захисту інформації в інфокомунікаціях.	8	10
2	**Тема 2. Принципи кібернетичного впливу в інформаційно-телекомунікаційних системах.** Конфіденційність, цілісність та доступність інформації в ІТС. Кібербезпека ІТС та захист інформаційних ресурсів та сервісів.	8	10
3	**Тема 3. Методики аналізу трафіку в інформаційно-телекомунікаційних системах.** Сніфери в ІТС. Семирівнева модель взаємодії відкритих систем. Протоколи передавання даних в ІТС.	8	10
4	**Тема 4. Методи та засоби захисту інформації при роботі з системами керування базами даних.** Керування правами доступу користувачів в сучасних СКБД. Загрози безпеки в БД.	8	10
5	**Тема 5. Методи технічного захисту інформації. Сучасні комплекси технічного захисту інформації.** Характеристики комплексів ТЗІ. Технічні характеристики сучасних шифраторів.	8	10
6	**Тема 6. Сучасні аспекти криптографічного захисту інформації.** Симетричне та асиметричне шифрування.	8	10
7	**Тема 7. Методи захисту інформації з використанням служб прикладного рівня SSH та SFTP.** Протокол SSH. Захист даних. Протокол FTP. Захист файлів.	8	10
8	**Тема 8. Управління ризиками ІБ. Методи аналізу кіберінцидентів.** Класифікація загроз ІБ. Способи виявлення та нейтралізації загроз ІБ.	10	12
	Разом	**66**	**82**

13. Індивідуальне завдання

Не передбачено планом.

14. Методи навчання

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

Словесні та наочні методи навчання використовуються під час лекцій, індивідуальних та групових консультацій, практичні – при проведенні практичних занять.

Під час проведення лекцій та практичних занять використовуються такі словесні методи як розповідь і пояснення.

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

Методи, що дозволяють формувати soft skills**:** аналітичне та критичне мислення, командна взаємодія, вирішення комплексних завдань, комунікативні та презентаційні навички, адаптивність та гнучкість мислення, увага до деталей, етичність та професійна відповідальність і тайм-менеджмент.

15. Методи контролю

Поточний контроль успішності засвоєння здобувачами вищої освіти навчального матеріалу здійснюється шляхом виконання практичних робіт, оцінювання знань здобувачів під час самостійних робіт, тестування або в ході індивідуальних співбесід зі здобувачами під час консультацій.

Модульний контроль є частиною поточного контролю і має на меті перевірку засвоєння здобувачем вищої освіти 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 або самостійної роботи.

Підсумковий контроль здійснюється у формі диференційованого заліку.

16. Розподіл балів, які отримують аспіранти

Схема нарахування балів* з навчальної дисципліни
«Методологія захисту інформації в інфокомунікаційних системах» за видами робіт

а) для денної форми здобуття освіти

Види робіт/контролю	***Перелік тем***							
	Тема 1	*Тема 2*	*Тема 3*	*Тема 4*	*Тема 5*	*Тема 6*	*Тема 7*	*Тема 8*
	Практичне заняття							
	1			2	3	4		
Виконання практичних завдань	**9**			**9**	**9**	**9**		
Тестування				**4**		**4**		
Виконання завдань самостійної роботи	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
Модульний контроль					**5**			**5**
Всього	**11**	**2**	**2**	**15**	**16**	**15**	**2**	**7**
Диференційований залік	***30***							
Всього за результатами вивчення навчальної дисципліни	***100***							

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

Схема нарахування балів* для заочної форми здобуття освіти з навчальної дисципліни «Методологія захисту інформації в інфокомунікаційних системах» за видами робіт

Види робіт/контролю	***Перелік тем***							
	Тема 1	*Тема 2*	*Тема 3*	*Тема 4*	*Тема 5*	*Тема 6*	*Тема 7*	*Тема 8*
	Практичне заняття							
	1					2		
Виконання практичних завдань	**9**					**9**		
Тестування	**5**					**5**		
Виконання завдань самостійної роботи	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
Модульний контроль					**5**			**5**
Всього	**18**	**4**	**4**	**4**	**9**	**18**	**4**	**9**
Диференційований залік	***30***							
Всього за результатами вивчення навчальної дисципліни	***100***							

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

Шкала та критерії оцінювання виконання практичних завдань

Бали для денної форми здобуття освіти	Бали для заочної форми здобуття освіти	Критерії оцінювання
7-9	7-9	Завдання виконано в повному обсязі. Програмний код працює коректно та оптимізовано. Здобувач вищої освіти продемонстрував глибоке розуміння теми, навів вичерпні висновки з аналізом результатів
1-6	1-6	Робота виконана не в повному обсязі або містить суттєві помилки в коді чи схемі підключення. Відсутні висновки. Продемонстровано лише мінімальну здатність застосовувати інструменти на практиці.
0	0	Не виконано практичну роботу або виконано із суттєвими помилками.

Шкала та критерії оцінювання знань здобувачів вищої освіти за результатами складання тестування для денної форми навчання

№	Завдання	Бали	Критерії оцінювання
1	Тестування	0-4	Кожна правильна відповідь оцінюється у фіксовану кількість балів (0,16×25=4), правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання знань здобувачів вищої освіти за результатами складання тестування для заочної форми навчання

№	Завдання	Бали	Критерії оцінювання
1	Тестування	0-5	Кожна правильна відповідь оцінюється у фіксовану кількість балів (0,2×25=5), правильність відповідей перевіряється відповідно до ключа тестів.

Оцінювання модульного контролю у формі тестування:

- кожна правильна відповідь оцінюється у фіксовану кількість балів *для денної форми здобуття освіти (0,2×25=5); для заочної форми здобуття освіти (0,2×25=5);*
- правильність відповідей перевіряється відповідно до ключа тестів.

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

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

Шкала та критерії оцінювання виконання завдань самостійної роботи

Бали для денної форми здобуття освіти	Бали для заочної форми здобуття освіти	Критерії оцінювання
2	4-6	Виконання завдань самостійної роботи здійснене у повному обсязі, не містить помилок, що дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти на високому рівні.
1	2-3	Виконання завдань самостійної роботи здійснене у повному обсязі, містить помилки та неточності, що дає можливість оцінити рівень формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти як достатній.
0	0-1	Завдання самостійної роботи не виконано та/або результати не відповідають поставленим завданням та/або завдання виконано із суттєвими помилками.

Шкала оцінювання: національна та ECTS

100-бальна рейтингова система оцінювання	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою для екзамену, диференційованого заліку, курсового проекту (роботи), практики
90 – 100	**A** – відмінно	**5** – відмінно
82 – 89	**B** – дуже добре	**4** – добре
74 – 81	**C** – добре	
64 – 73	**D** – задовільно	**3** – задовільно
60 – 63	**E** – достатньо	
35 – 59	**FX** – незадовільно з можливістю повторного складання	**2 –** незадовільно
0 – 34	**F** – незадовільно з обов'язковим повторним вивченням дисципліни	

Правила модульно-рейтингового оцінювання знань

Загальна трудомісткість дисципліни – 100 балів, із них:

– при підсумковому контролі у вигляді диференційованого заліку 70 балів відведено на поточний контроль, а 30 балів – на підсумковий.

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

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

Присутність на лекціях та 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 здобувача вищої освіти на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

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

17. Методичне забезпечення

1. Здоренко Ю.М. Опорний конспект лекцій з дисципліни «Методологія захисту інформації в інфокомунікаційних системах» для здобувачів денної форми навчання спеціальності G5 Електроніка, електронні комунікації, приладобудування та радіотехніка. – Полтава, 2026. – 38 с.
2. Здоренко Ю.М. Методичні вказівки до практичних робіт з дисципліни «Методологія захисту інформації в інфокомунікаційних системах» для здобувачів денної форми навчання спеціальності G5 Електроніка, електронні комунікації, приладобудування та радіотехніка. – Полтава, 2026. – 16 с.

18. Рекомендована література

Базова

1. Хлапонін Ю.І. Комплексні системи захисту інформації: конспект лекцій / Ю.І. Хлапонін. - Київ: КНУБА, 2022. – 84 с.
2. Стасюк, Марта. Елементи математичних основ криптографії: навчальний посібник / Марта СТАСЮК – Львів: ЛДУ БЖД, 2021. – 216 с.
3. О. І. Алєнін, А. В. Габінет, О. П. Роковий, С. Г. Стіренко, О. О. Ілляшенко, А. А. Стрєлкіна Методи та засоби технічного аудиту інформаційної безпеки комп'ютерних систем та мереж. Практикум / під ред. В.С. Харченко «ХАІ». 2017. – 136 с.
4. Onyshchenko, S., Haitan, O., Yanko, A., Rudenko, O, Zdorenko Y. Method for detection of the modified DDoS cyber attacks on a web resource of an Information and Telecommunication Network based on the use of intelligent systems. Proceedings of the Modern Data Science Technologies Workshop (MoDaST 2024), pp. 219–235. CEUR, Lviv Polytechnic National University, Lviv, Ukraine, (2024). ISSN: 16130073 https://ceur-ws.org/Vol-3723/paper12.pdf.
5. Krasnobayev V., Yanko A., Hlushko A., Kruk O., Kruk O., Gakh V. Cyberspace protection system based on the data comparison method. In: Economic and cyber security, PC TECHNOLOGY CENTER, 2023. pp. 3–29.

6. Yurii Zdorenko, Alina Yanko, Mykhailo Myziura, Nadiia Fesokha Development of a fuzzy risk assessment model for information security management Technology audit and production reserves — No. 4/2(84), pp. 71-79, 2025.

7. Yanko A., Laktionov O., Pedchenko N., Bilko S. Data Error Correction Method for Increasing the Information Protection of an Automated Robotic Platform: A monograph. Warsaw: E-SCIENCE SPACE, 2024. 74 p.

Допоміжна

1. Закон України Про національну безпеку України (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2469-19

2. Закон України про внесення змін до Закону України "Про захист інформації в автоматизованих системах" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2594-15

3. Адміністрація Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835

4. Здоренко Ю.М., Андрєєв А. С., Бочкар В. О. Методи забезпеченння доступності інформаційних ресурсів на основі використання мікросервісної архітектури веб-додатків. Збірник тез доповідей II Міжнар. наук.-практичної конференції «Інновації та перспективні шляхи розвитку інформаційних технологій», Черкаський державний технологічний університет, 06 груд. 2023 р., м. Черкаси, 204с

19. Інтернет- ресурси

1. Сторінка курсу на платформі Moodle: https://dist.nupp.edu.ua/course/view.php?id=8080

2. Стратегія кібербезпеки України: Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

3. MATLAB Documentation: Deep Learning Toolbox & Signal Processing. URL: https://uk.mathworks.com/help/deeplearning/