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
«__» 08 2026 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Корпоративна безпека електронно-комунікаційних мереж»
(назва навчальної дисципліни)

Підготовки	Доктор філософії (назва ступеня вищої освіти)
Освітньо-наукова програма	Телекомунікації та радіотехніка (назва освітньо-наукової програми)
Спеціальності	G5 Електроніка, електронні комунікації, приладобудування та радіотехніка (код і назва спеціальності)

Полтава
2026 рік

Робоча програма навчальної дисципліни «**Корпоративна безпека електронно-комунікаційних мереж**» для здобувачів вищої освіти спеціальності G5 Електроніка, електронні комунікації, приладобудування та радіотехніка, третього (освітньо-наукового) рівня вищої освіти.

Розробник: Живило Є.О, кандидат технічних наук, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем.

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 » серпня 2026 року № 1

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

_____(Олександр ШЕФЕР)

« 27 » серпня 2026 року

© Живило Є. О., 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 радіотехніка</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>2/3й</td><td>2/3й</td></tr>
<tr><td rowspan="2">Змістових модулів – 1</td><td colspan="2">Семестр</td></tr>
<tr><td>4/5й</td><td>4/5й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>16 год</td><td>4 год</td></tr>
<tr><td rowspan="10">Індивідуальні завдання
не передбачено</td><td colspan="2">Практичні, семінарські</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:
0 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">Диференційований 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

Метою є формування у здобувачів освіти системних знань і практичних навичок із забезпечення захисту інформаційних ресурсів, електронно-комунікаційних мереж та корпоративних систем від сучасних кіберзагроз, а також ознайомлення з правовими нормами, міжнародними стандартами безпеки та методами управління ризиками.

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 ініціювати та виконувати наукові дослідження, що приводять до отримання нових знань та наукових результатів із дотриманням належної академічної доброчесності.

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.

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 ефективно використовувати дослідницькі навички та знання в предметній області спеціальності.

Здатність проектувати, обслуговувати, експлуатувати обладнання телекомунікації та радіотехніки; мати детальні знання спеціальної області дослідження в поєднанні зі знаннями загальної наукової складової.

Здатність застосовувати отримані знання та навички для створення власних інноваційних проектів і рішень у сфері телекомунікацій та радіотехніки.

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 «Корпоративна безпека електронно-комунікаційних мереж» здобувачі вищої повинні сформувати такі програмні результати навчання (знання й уміння):

Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, статистичні методи аналізу даних та/або складної структури.

Уміти системно мислити, формувати принципово нові ідеї, пропонувати способи розв'язання поставлених наукових та практичних задач в умовах неповної або обмеженої інформації, демонструючи гнучкість у прийнятті рішень.

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 виконувати самостійно науково-дослідну діяльність в сфері телекомунікацій і радіотехніки з використанням сучасних методів наукових досліджень, дотримуючись академічної доброчесності та правил професійної етики.

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 вищої 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	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.

			викликають ускладнення.	
64 - 73	**D**	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень дисципліни.
60 – 63	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень і володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використанням основних теоретичних положень пояснюються з труднощами. Виконання практичних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній,** що є мінімально допустимим у всіх складових навчальної дисципліни.
35 - 59	**FX**	**Незадовільно** з можливістю повторного складання екзамену/ диференційованого 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 занять 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/диференційованого 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: виконання практичних завдань, виконання завдань самостійної роботи, тестування, ***диференційований залік***.

7. Програма навчальної дисципліни

Змістовий модуль 1

Основи корпоративної безпеки електронно-комунікаційних мереж та правові аспекти

Тема 1. Огляд політик та стандартів корпоративної безпеки електронно-комунікаційних мереж.

Огляд стандартів та політик безпеки (ISO/IEC 27001, NIST). Визначення політик безпеки в організації. Нормативні акти та закони щодо захисту інформації.

Практичне заняття № 1.

Тема 2. Архітектура безпеки в корпоративних системах

Види архітектур безпеки: периметральна, багатоетапна, гнучка. Роль мережевої безпеки. Безпека хмарних технологій у корпоративному середовищі.

Тема 3. Основи управління ризиками в корпоративній безпеці

Визначення, оцінка та управління ризиками. Методи зменшення та адаптації до ризиків. Впровадження контрзаходів для мінімізації ризиків.

Практичне заняття № 2.

Тема 4. Захист даних та управління доступом

Методи захисту даних. Стратегії управління доступом. Важливість аутентифікації та авторизації.

Практичне заняття № 3.

Тема 5. Інформаційна безпека та кіберзахист

Захист від кіберзагроз (атаки, віруси, шкідливе ПЗ). Використання міжмережевих екранів, антивірусних систем та систем виявлення загроз. Роль моніторингу та реагування на інциденти безпеки.

Тема 6. Приватність та конфіденційність даних

Визначення конфіденційності та приватності даних. Політики та регуляції (GDPR, CCPA, NIST Privacy Framework). Методи анонімізації та псевдонімізації даних.

Тема 7. Безпека комунікацій та передачі даних

Захист каналів зв’язку (VPN, SSL/TLS, шифрування). Проблеми безпеки при обміні даними. Виявлення та запобігання витокам даних.

Практичне заняття № 4.

Тема 8. Системи моніторингу та реагування на інциденти безпеки

Створення систем моніторингу. Процес виявлення, аналізу та реагування на інциденти. Поглиблений аналіз інцидентів та зворотній зв’язок. Стратегії впровадження корпоративної безпеки. Визначення стратегій корпоративної безпеки. Важливість розвитку культури безпеки в організації. Впровадження безпекових політик в компанії.

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**
Змістовний модуль 1. Основи корпоративної безпеки електронно-комунікаційних мереж та правові аспекти						
Тема 1. Огляд політик та стандартів корпоративної	12	2	2			8

безпеки електронно-комунікаційних мереж.						
Тема 2. Архітектура безпеки в корпоративних системах	10	2				8
Тема 3. Основи управління ризиками в корпоративній безпеці	12	2	2			8
Тема 4. Захист даних та управління доступом	12	2	2			8
Тема 5. Інформаційна безпека та кіберзахист	10	2				8
Тема 6. Приватність та конфіденційність даних	10	2				8
Тема 7. Безпека комунікацій та передачі даних	12	2	2			8
Тема 8. Системи моніторингу та реагування на інциденти безпеки	12	2				10
Усього годин	**90**	**16**	**8**			**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**
Змістовний модуль 1. Основи корпоративної безпеки електронно-комунікаційних мереж та правові аспекти						
Тема 1. Огляд політик та стандартів корпоративної безпеки електронно-комунікаційних мереж.	14	2	2			10
Тема 2. Архітектура безпеки в корпоративних системах	10					10
Тема 3. Основи управління ризиками в корпоративній безпеці	10					10
Тема 4. Захист даних та управління доступом	14	2	2			10
Тема 5. Інформаційна безпека та кіберзахист	12					12
Тема 6. Приватність та конфіденційність даних	10					10
Тема 7. Безпека комунікацій та передачі даних	10					10
Тема 8. Системи моніторингу та реагування на інциденти безпеки	10					10
Усього годин	**90**	**4**	**4**			**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	*0*	*0*

10. Перелік питань для практичних занять

№ заняття	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
1	Визначення основних загроз в корпоративних системах Оцінка безпеки в корпоративних мережах	*2*	*2*
2	Налаштування політики доступу Шифрування та захист переданих даних	*2*	*2*
3	Аудит систем безпеки Ідентифікація та аутентифікація користувачів	*2*	
4	Використання інструментів для моніторингу безпеки Реагування на інциденти безпеки	*2*	
Разом		***8***	***4***

11. Перелік питань для лабораторних занять

№ заняття	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
	Лабораторні заняття не передбачені	*0*	*0*

12. Самостійна робота

Метою самостійної роботи здобувачів вищої освіти є: 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 здобувача вищої освіти:

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

Питання для самостійного вивчення здобувачами вищої освіти

№ з/п	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
1	*Тема 1. Огляд політик та стандартів корпоративної безпеки електронно-комунікаційних мереж*. Корпоративна безпека та її основні цілі. Основні типи загроз для корпоративної безпеки. Основні принципи побудови стратегії корпоративної безпеки. Управління ризиками в корпоративній безпеці. Методи оцінки ризиків для корпоративної безпеки. Правові вимоги до корпоративної безпеки в Україні.	*8*	*10*
2	*Тема 2. Архітектура безпеки в корпоративних системах.* Міжнародні стандарти та регламенти у сфері корпоративної безпеки. Вплив законодавства на зберігання та обробку персональних даних в корпоративному середовищі. Що таке політики безпеки та як їх розробляти для підприємства?	*8*	*10*
3	*Тема 3. Основи управління ризиками в корпоративній безпеці.* Що таке шифрування та як воно використовується для захисту даних. Види загроз для інформаційної безпеки в корпоративному середовищі. Політика доступу до корпоративної інформації. Стандарти для захисту персональних даних в корпоративній безпеці	*8*	*10*
4	*Тема 4. Захист даних та управління доступом.* Що таке GDPR і як він впливає на корпоративну безпеку та обробку персональних даних. Порядок здійснення контролю доступу до конфіденційної інформації в організаціях. Використання NIST Privacy Framework для забезпечення безпеки даних в організації. Методи анонімізації та псевдонімізації даних.	*8*	*10*
5	*Тема 5. Інформаційна безпека та кіберзахист.* Управління інцидентами в корпоративній безпеці. Класифікація інцидентів безпеки. Методи їх усунення. Розробка плану реагування на інциденти. План безперервності бізнесу та як він створюється.	*8*	*12*

6	*Тема 6. Приватність та конфіденційність даних.* Оцінка ризиків постачальників у контексті корпоративної безпеки. Система управління безпекою інформації (ISMS) і як її впровадити в компанії. Стандарт ISO/IEC 27001. Стандарт ISO 27005.	*8*	*10*
7	*Тема 7. Безпека комунікацій та передачі даних.* Як побудувати систему контролю доступу до інформаційних систем? Які методи моніторингу безпеки інформаційних систем застосовуються в корпоративному середовищі? Які сучасні інструменти використовуються для захисту від кіберзагроз в корпоративному середовищі?	*8*	*10*
8	*Тема 8. Системи моніторингу та реагування на інциденти безпеки.* Як здійснюється впровадження антивірусного захисту в організації? Які основні етапи проведення аудиту інформаційної безпеки? Як проводиться тестування на проникнення (pen-test) в корпоративних системах?	*10*	*10*
	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 навчання, які дозволяють формувати Soft skills: Experiential Learning, PBL.

15. Методи контролю

Поточний контроль успішності засвоєнням здобувачами вищої освіти навчального матеріалу здійснюється шляхом опитування й оцінювання знань здобувачамів вищої освіти під час практичних занять, оцінювання виконання здобувачами вищої освіти самостійної роботи, тестування або в ході індивідуальних співбесід зі здобувачами вищої освіти під час консультацій. Вибір конкретних форм і методів поточного контролю знань здобувачів вищої освіти залежить від викладача і доводиться до їхнього відома на першому практичному занятті.

Підсумковий контроль здійснюється у формі ***диференційованого заліку.***

16. Розподіл балів, які отримують здобувачі вищої освіти

Схема нарахування балів* для денної форми здобуття освіти з навчальної дисципліни «Корпоративна безпека електронно-комунікаційних мереж» за видами робіт

Види робіт/контролю	***Перелік тем***							
	Тема 1	*Тема 2*	*Тема 3*	*Тема 4*	*Тема 5*	*Тема 6*	*Тема 7*	*Тема 8*
	Практичне заняття							
	1		*2*	*3*			*4*	
Виконання практичних завдань	***9***		***9***	***9***			***9***	
Тестування			***9***				***9***	
Виконання завдань самостійної роботи	***2***	***2***	***2***	***2***	***2***	***2***	***2***	***2***
Всього	***11***	***2***	***20***	***11***	***2***	***2***	***20***	***2***
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 «Корпоративна безпека електронно-комунікаційних мереж» 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				***4***				
Виконання завдань самостійної роботи	***6***	***6***	***6***	***6***	***6***	***6***	***6***	***6***
Всього	***15***	***6***	***6***	***19***	***6***	***6***	***6***	***6***
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 заочної форми здобуття освіти

№	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 денної форми навчання

№	Завдання	Бали	Критерії оцінювання
1	Тестування	0-9	Кожна правильна відповідь оцінюється у фіксовану кількість балів (0,36×25=9), 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 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 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 семестровому контролі у вигляді диференційованого заліку на поточний контроль відведено 70 балів (для допуску до диференційованого заліку необхідно мати не менше 35 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, захист практичних робіт, а в разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних занять) – до 70 балів.

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

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

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

17. Методичне забезпечення

1. Живило Є.О. Конспект лекцій з дисципліни «Корпоративна безпека електронно-комунікаційних мереж» для здобувачів вищої освіти спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка». - Полтава : НУ «Полтавська політехніка імені Юрія Кондратюка», 2025. - 61 с.

2. Живило Є.О. Методичні вказівки для проведення практичних занять з дисципліни «Корпоративна безпека електронно-комунікаційних мереж» для здобувачів вищої освіти спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка». - Полтава : НУ «Полтавська політехніка імені Юрія Кондратюка», 2026. - 38 с.

18. Рекомендована література

Базова

1. Живило, Є.О. Корпоративна безпека: [навч. посіб.]. - П.: НУ “Полтавська політехніка імені Юрія Кондратюка”, 2025. – 157 с.

2. Живило, Є.О. Тестування на проникнення [навч. посіб.] . Ч. 1. / Є.О. Живило; за ред. Є.О. Живило.- Полтава : НУ “Полтавська політехніка імені Юрія Кондратюка”, 2024.- 134 с.

3. Живило, Є.О. Тестування на проникнення [навч. посіб.] . Ч. 2. / Є.О. Живило; за ред. Є.О. Живило.- Полтава : НУ “Полтавська політехніка імені Юрія Кондратюка”, 2024.- 239 с.

4. Живило, Є.О. Захист інформації та кібербезпека в електронних комунікаційних мережах : навч. посіб. / Є.О. Живило.- Полтава : НУ “Полтавська політехніка імені Юрія Кондратюка”, 2023.- 188 с.

5. Корпоративні інформаційні системи та безпека електронних комунікацій : навч. посіб. / О. В. Кузнецов, В. М. Левикін, О. В. Смирнов та ін. — Харків : ХНУРЕ, 2021. — 312 с.

6. Основи кібербезпеки та захисту корпоративних мереж : підручник / О. Г. Корченко, Ю. О. Дрейс, І. В. Олексієнко. — Київ : НАУ, 2022. — 400 с.

7. Моніторинг та забезпечення безпеки корпоративних телекомунікаційних мереж : навч. посіб. / В. А. Хорошко, О. О. Алімурадов, С. В. Голуб. — Київ : Вид-во «Центр учбової літератури», 2021. — 264 с.

Допоміжна

1. Kurose, J. F., Ross, K. W. Computer Networking: A Top-Down Approach / J. F. Kurose, K. W. Ross. — 8th ed. — Hoboken : Pearson, 2021. — 800 p.

2. Ciampa, M. Security+ Guide to Network Security Fundamentals / M. Ciampa. — 7th ed. — Boston : Cengage Learning, 2021. — 672 p.

3. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163- 19#Text;

4. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 р. URL : https://zakon.rada.gov.ua/laws/show/3475-15#top;

5. Про захист персональних даних : Закон України від 01.06.2010 р. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text;

6. Про інформацію: закон України від 02.10.1992 р. URL : https://zakon.rada.gov.ua/laws/main/2657-12#Text;

7. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України» : указ Президента України від 26.08.2021 р. URL : https://zakon.rada.gov.ua/laws/ show/447/2021#n12;

8. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show /685/2021#n14;

19. Інтернет-ресурси

1. Дистанційний курс з дисципліни «Корпоративна безпека електронно-комунікаційних мереж» URL: https://dist.nupp.edu.ua/course/view.php?id=8082.

2. Діяльність Адміністрації Держспецзв’язку у сфері кіберзахисту URL:https://cip.gov.ua/ua/statics/cyber-protection.

3. Перелік документів нормативно-правової бази, що забезпечує надання відповідних видів послуг у галузі технічного захисту інформації URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-normativno-pravovoyi-bazi-sho-zabezpechuye-nadannya-vidpovidnikh-vidiv-poslug-u-galuzi-tekhnichnogo-zakhistu-informaciyi.