

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет
 Факультет кібербезпеки, комп'ютерної та програмної інженерії
 Кафедра безпеки інформаційних технологій

УЗГОДЖЕНО
 Декан ФККПІ

Нестеренко К. Нестеренко

«09» 09 2022 р.

ЗАТВЕРДЖЕНО
 Проректор з навчальної роботи

А. Долухів
 «08» 09 2022 р.



Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Теоретико-множинне моделювання даних для вирішення задач
кібербезпеки/захисту інформації»

Освітньо-наукова програма
 Галузь знань
 Спеціальність:
 Статус дисципліни:
 Освітній ступінь:

«Кібербезпека»
 12 Інформаційні технології
 125 Кібербезпека
 обов'язковий компонент
 Доктор філософії

Форма навчання	Семестр	Усього (годин/кредитів ECTS)	Лекції	Практ. заняття	Лабор. заняття	Самостійна робота	Форма підсумк. контролю
Очна	3	180/6,0	24	36	-	120	Екзамен
Заочна	3	180/6,0	8	12	-	160	Екзамен

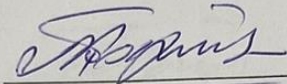
Індекс: РДФ - 4 - 125 / 22-2.1.3
 Індекс: РДФ - 4 - 125 / 22-2.1.3 (3)

СМЯ НАУ РПНД 07.01.07-01-2022

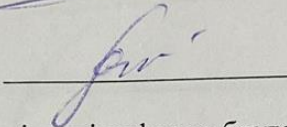


Робочу програму навчальної дисципліни «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації» розроблено на основі освітньо-наукової програми «Кібербезпека», навчальних (№ НДФ - 4 - 125 / 22, № НДФ - 4 - 125 / 22(3)) та робочих навчальних (РДФ - 4 - 125 / 22, РДФ - 4 - 125 / 22(3)) планів підготовки здобувачів ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Робочу програму розробили:
Завідувач кафедри

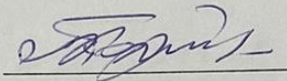
 О. Корченко

доцент кафедри безпеки
інформаційної безпеки

 Ю. Дрейс


Робочу програму обговорено та схвалено на засіданні кафедри безпеки інформаційних технологій, протокол №7 від 22.08.2022 р.

Завідувач кафедри

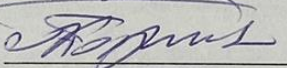
 О. Корченко

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-наукової програми підготовки докторів філософії «Кібербезпека», спеціальності 125 «Кібербезпека», кафедри безпеки інформаційних технологій, протокол №7 від 22.08.2022 р.

Завідувач кафедри

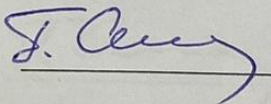
 О. Корченко

Гарант освітньо-наукової програми

 О. Корченко

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету кібербезпеки, комп'ютерної та програмної інженерії, протокол №19 від «06» вересня 2022р.

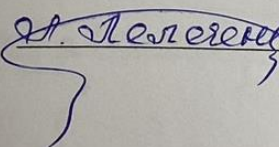
Голова НМРР

 С. Гнатюк

УЗГОДЖЕНО

Завідувач аспірантури та докторантури

« 07 » 09 2022 р.

 А. Лелеченко

Рівень документа – 3б

Плановий термін між ревізіями – 1 рік

Контрольний примірник



Система менеджменту якості.
Робоча програма навчальної дисципліни
«Методи ідентифікації аномальних станів
для системи виявлення вторгнень»

Шифр
документа

СМЯ НАУ
РПНД 07.01.07-01-2022

стор. 3 з 12

АРКУШ ПОГОДЖЕННЯ


Гарант освітньо-наукової
програми «Кібербезпека»

_____ О. Корченко



ЗМІСТ

Вступ	5
1. Пояснювальна записка	5
Мета та завдання навчальної дисципліни.....	5
Очікувані результати навчання	5
Передумови вивчення навчальної дисципліни.....	6
2. Зміст навчальної дисципліни.....	6
Програма навчальної дисципліни	6
Тематичний план навчальної дисципліни	8
Самостійна робота аспірантів.....	8
3. Навчально-методичні матеріали	9
Методи навчання	9
Рекомендована література (базова і допоміжна)	9
Інформаційні інтернет-ресурси.....	9
4. Система оцінювання результатів навчання	10
Засоби діагностики результатів навчальної діяльності	10
Форми контролю результатів навчання та їх оцінювання	10
Критерії оцінювання досягнень аспірантів.....	11

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методи ідентифікації аномальних станів для системи виявлення вторгнень»	Шифр документа	СМЯ НАУ РПНД 07.01.07-01-2022
		стор. 5 з 12	

ВСТУП

Робоча програма (РП) навчальної дисципліни «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації» розроблена на основі Методичних рекомендацій щодо розроблення робочих програм навчальних дисциплін з підготовки здобувачів ступеня доктора філософії у Національному авіаційному університеті, затверджених наказом ректора від 29.04.2021р. №249/од.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Мета та завдання навчальної дисципліни.

Дана навчальна дисципліна є однією з провідних в системі підготовки докторів філософії за ліцензованими в НАУ спеціальностями та спеціалізаціями, яка формує їх фаховий рівень та надає новітні методологічні основи з проведення наукових досліджень.

Мета та завдання є застосування сучасних методів теоретико-множинного моделювання даних для вирішення задач кібербезпеки/захисту інформації. Місце даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.

Завданнями вивчення навчальної дисципліни є:

- ознайомлення аспірантів з використанням методів фундаментальних наук для розв’язання загально інженерних, професійних та наукових задач;
- навчити аспірантів генерувати нові ідеї і варіанти розв’язання задач у галузі кібербезпеки;
- ознайомлення аспірантів з застосуванням сучасних методів теоретико-множинного моделювання даних для вирішення задач кібербезпеки/захисту інформації;
- навчання аспірантів основних принципів розробки та використання засобів, що розширюють функціональні можливості сучасних систем кібербезпеки та захисту інформації.

Очікувані результати навчання.

Навчальна дисципліна «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації» дає можливість досягти таких програмних результатів:

ПРН3. Уміння відслідковувати сучасні тенденції й нові напрямки розвитку захисту інформації, інформаційної та кібербезпеки, а також суміжних і прикладних областей


ПРН4. Здатність та уміння використовувати математичний апарат (теорії нечітких множин, математичної статистики, теорії імовірності тощо) для освоєння теоретичних основ, моделювання даних, практичного використання (обробки експериментальних даних), розробки нових та удосконалення існуючих методів, засобів та систем у сфері інформаційної та кібербезпеки.

ПРН5. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання ризиків інформаційної та/або кібербезпеки при побудові комплексних систем захисту інформації, систем управління інформаційною безпекою, аудит стану кібербезпеки.

ПРН6. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання негативних наслідків (шкоди) державі, суспільству, приватній чи юридичній особі у разі витоку державних інформаційних ресурсів, інформації з обмеженим доступом.

ПРН7. Здатність проводити дослідження, розвиток та удосконалення сучасних нейромережових моделей, методів, засобів та систем виявлення нових загроз, мережових кібератак, шкідливого програмного забезпечення, аналізу і оцінювання параметрів стану забезпечення активного захисту та кібербезпеки інформаційних (автоматизованих), інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури.

ПРН8. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем виявлення вторгнень, визначати їх базові характеристики, а також обґрунтовано обирати та застосовувати в практичній роботі при побудові систем кібербезпеки.

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методи ідентифікації аномальних станів для системи виявлення вторгнень»	Шифр документа	СМЯ НАУ РПНД 07.01.07-01-2022
		стор. 6 з 12	

ПРН9. Здатність продемонструвати знання та розуміння застосування методів, моделей та засобів ідентифікації аномальних станів для побудови систем виявлення вторгнень заснованих на теорії нечітких множин.

ПРН10. Вміти аналізувати, обґрунтовувати вибір та застосовувати методи фундаментальної та прикладної математики задля розв'язання задач аналізу, проектування і розробки елементів інтелектуальних систем кібербезпеки.

ПРН11. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем кібербезпеки в умовах неповної визначеності.

Навчальна дисципліна «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації» дає можливість здобути такі компетентності:

ЗК1. Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності.

ФК3. Здатність та уміння проводити дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації та/або кібербезпеки при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.

ФК4. Здатність та уміння проводити дослідження проблеми забезпечення інформаційної безпеки національних інтересів України, вивчати і обґрунтовувати форми та методи захисту людини, суспільства й держави від зовнішніх і внутрішніх загроз в інформаційній сфері, а також шляхи підвищення ефективності функціонування інформаційних систем держави в сучасних умовах.

ФК5. Уміння застосовувати та розробляти сучасні технології, системи, технічні засоби, методи та моделі, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій, освітній та професійній діяльності;

ФК7. Здатність та уміння проводити дослідження проблеми забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів, інформаційні ресурси різних класів на об'єктах інформаційної діяльності та критичної інфраструктури, системи управління, на основі технологій, методів, моделей та засобів у сфері інформаційної безпеки та/або кібербезпеки.

Передумови вивчення навчальної дисципліни.

Навчальна дисципліна «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації» базується на знаннях таких дисциплін, як: «Інноваційні методи прийняття рішень в соціотехнічних та соціокультурних системах», «Правове, економічне та інформаційне забезпечення наукових досліджень», «Методологія наукових досліджень у сфері кібербезпеки», «Наукові розробки та дослідження у сфері інформаційної безпеки та кібербезпеки (у т.ч. наукової школи «Кібербезпеки» НАУ)», «Англійська мова наукового спрямування», а результати навчання даного курсу можуть бути використані під час написання кандидатської дисертації.

2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програма навчальної дисципліни.

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля, який є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни.

Модуль №1 «Побудова систем кібербезпеки та захисту інформації на нечітких множинах».

Тема 1.1. Основи організації систем кібербезпеки та захисту інформації.

Базові поняття та визначення. Основні вимоги і класифікації. Стандарти інформаційної безпеки. Сучасні методи та засоби оцінювання стану захисту інформації та кібербезпеки.



Тема 1.2. Методологічний базис нечітких множин для вирішення задач кібербезпеки\захисту інформації.

Базові поняття та засоби нечітких множин. Узагальнена класифікація нечітких чисел. Методи побудови функцій приналежності нечітких множин. Методи реалізації операцій нечіткої арифметики. Методи порівняння нечітких чисел.

Тема 1.3. Логіко-лінгвістичні технології організації моделей кібербезпеки\захисту інформації.

Логіко-лінгвістичний підхід до оцінювання рівня стану кібербезпеки\захисту інформації. Організація нечітких моделей оцінки рівня захищеності.

Тема 1.4. Синтез обчислювальних структур для реалізації моделей систем кібербезпеки\захисту інформації.

Організація паралельних обчислювальних структур нечіткої арифметики. Синтез комбінаційних обчислювальних елементів. Побудова швидкодіючих криптографічних обчислювачів.


Тема 1.5. Організація систем захисту на основі засобів з нечіткою логікою.

Методологія синтезу систем оцінки рівня захищеності інформаційних ресурсів. Система оцінки стану захищеності на лінгвістичних і варіативних бальних шкалах. Методологія синтезу систем оцінки рівня гарантій. Системи оцінки для проведення експертиз технічного захисту інформації.

Тема 1.6. Реалізовані системи оцінки ризиків інформаційної безпеки та нанесеної шкоди у разі витоку інформації з обмеженим доступом.

Тематичний план навчальної дисципліни.

№ п/п	Назва теми	Обсяг навчальних занять (год.)								
		Очна форма навчання				Заочна форма навчання				
		Усього	Лекції	Практ./лабо р. заняття (семінари)	СР	Усього	Лекції	Практ./лабо р. заняття (семінари)	СР	
1	2	3	4	5	6	7	8	9	10	
Модуль №1 «Побудова систем кібербезпеки та захисту інформації на нечітких множинах»										
1.1	Основи організації систем кібербезпеки та захисту інформації	3 семестр				3 семестр				
		27	4	3	20	23	1	2	20	
1.2	Методологічний базис нечітких множин для вирішення задач кібербезпеки\захисту інформації	28	4	4	20	23	1	2	20	
1.3	Логіко-лінгвістичні технології організації моделей кібербезпеки\захисту інформації	28	4	6	18	23	1	2	20	
1.4	Синтез обчислювальних структур для реалізації моделей систем кібербезпеки\ захисту інформації.	32	4	8	20	40	2	2	36	
1.5	Організація систем захисту на основі засобів з нечіткою логікою	32	4	8	20	41	1	2	38	
1.6	Реалізовані системи оцінки ризиків інформаційної безпеки та нанесеної шкоди у разі витоку інформації з обмеженим доступом		4	6	20		2	2	26	
1.7.	Модульна контрольна робота №1	3	-	1	2	-	-	-	-	
Усього за модулем №1		180	24	36	120	180	8	12	160	
Усього за навчальною дисципліною		180	24	36	120	180	8	12	160	

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методи ідентифікації аномальних станів для системи виявлення вторгнень»	Шифр документа	СМЯ НАУ РПНД 07.01.07-01-2022
		стор. 8 з 12	

Лекційні заняття, їх тематика і обсяг

№ п/п	Назва теми	Обсяг навчальних занять (год.)			
		Очна форма навчання		Заочна форма навчання	
		Лекції	СРС	Лекції	СРС
1	2	3	4	5	6
1.1	Основи організації систем кібербезпеки та захисту інформації	3 семестр		3 семестр	
		4	10	1	10
1.2	Методологічний базис нечітких множин для вирішення задач кібербезпеки\захисту інформації	4	10	1	10
1.3	Логіко-лінгвістичні технології організації моделей кібербезпеки\захисту інформації	4	10	1	10
1.4	Синтез обчислювальних структур для реалізації моделей систем кібербезпеки\ захисту інформації.	4	10	2	18
1.5	Організація систем захисту на основі засобів з нечіткою логікою	4	10	1	19
1.6	Реалізовані системи оцінки ризиків інформаційної безпеки та нанесеної шкоди у разі витоку інформації з обмеженим доступом	4	10	2	13
	Модульна контрольна робота №1				
Усього за модулем №1		24	60	6	80
Усього за навчальною дисципліною		24	60	6	80

Самостійна робота аспірантів

Самостійна робота з дисципліни складається з таких видів роботи:

- 1). опрацювання лекційного матеріалу;
- 2). підготовка до практичних занять;
- 3). підготовка до модульних контрольних робіт.

Завдання 1) виконується з метою поглиблення знань з лекційного матеріалу та полягає в опануванні більш широкого кола питань за тематикою лекцій.

Завдання 2) виконується з метою надбання практичних навичок з розробки та застосування методів теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації, які розширюють функціональні можливості сучасних побудови систем.

Завдання 3) виконується з метою підготовки до продуктивної праці над тематикою модульної контрольної роботи та полягає у вивченні контрольних питань із затвердженого на засіданні кафедри переліку питань для підготовки до модульної контрольної роботи.


3. НАВЧАЛЬНО – МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання:

- пояснювально-ілюстративний метод;
- метод проблемного викладу;
- репродуктивний метод;
- дослідницький метод.

Реалізація цих методів здійснюється при проведенні лекцій, демонстрацій, самостійному

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методи ідентифікації аномальних станів для системи виявлення вторгнень»	Шифр документа	СМЯ НАУ РПНД 07.01.07-01-2022
		стор. 9 з 12	

вирішенні задач, роботі з навчальною літературою, аналізі та вирішенні задач з розробки та застосування методів виявлення аномальних станів породжених кібератаками. У процесі проведення лекційних занять використовуються мультимедійні технології та пояснювально-ілюстративні методи навчання. Практичні заняття проводяться з використанням прикладного програмного забезпечення, роботи в групах та дослідницьких методів та методів проблемного викладення.

Рекомендована література

Базова література.


- 3.2.1. *Корченко О.Г.*, Системи захисту інформації. Монографія, К.: НАУ – 2004. – 264 с.
- 3.2.2. Безпека авіації. Монографія, *Бабак В.П., Корченко О.Г., Харченко В.П., Максимов В.О.* та ін., К.: Техніка, 2004. – 584 с.: іл. – Бібліогр.: 560–583 с.
- 3.2.4. *Корченко А.Г.* Побудова систем захисту інформації на нечітких множинах. Теорія і практичні рішення. Монографія, К.: МК-Пресс.- 2006. – 320 с.
- 3.2.5. Quantum Secure Telecommunication Systems / Telecommunications Networks: Current Status and Future Trends., *A. Korchenko, P. Vorobiyenko, M. Lutskiy, Y. Vasiliu, S. Gnatyuk*, Edited by Jesus Hamilton Ortiz. – Rijeka, Croatia : InTech, 2012. – P. 211-236. ISBN978- 953-51-0341-7 (монографія).
- 3.2.6. Аналіз і оцінювання ризиків інформаційної безпеки. Монографія, *Корченко О.Г., О.Є.Архипов, С.В. Казмирчук*, К.: ООО «Лазурит Поліграф», 2013. – 275 с.
- 3.2.7. Системи аналізу і оцінювання ризиків інформаційної безпеки. Монографія, *Корченко О.Г., С.В.Казмирчук, О.Є.Архипов, Саарбрюккен* (Германія): Palmarium Academic Publishing, 2013 -316 с.
- 3.2.8. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці. Монографія, *Корченко О.Г., Архипов ОЄ., Дрейс Ю.О.*, К.: наук. – вид. центр НА СБ України, 2014 –332 с.
- 3.2.9. Immune and defensive corporate systems with intellectual identification of threats, *Oleksandr Korchenko, Oleksandr Petrov, Bohdan Borowik, Mykola Karpinsky y, Valery Lakhno, Pszczyna* : Śląska Oficyna Drukarska, 2016 – 222 s. : il. pISBN: 978-83-62674-68-8.
- 3.2.10. Методологія розроблення нейромережових засобів інформаційної безпеки Інтернеторієнтованих інформаційних систем. Монографія, *Корченко О.Г., Терейковський І.А., Білощицький А.О.*, К.: ТОВ «Наш формат». – 2016. – 249 с.
- 3.2.11. Методи перехоплення інформації в інформаційно-комунікаційних системах на основі квантових технологій. Монографія, *Корченко О.Г., Є.В. Василю, С.О. Гнатюк, Т.О. Жмурко.* – Х.: Цифрова друкарня №1, 2013. – С. 98-111.

Допоміжна література.

- 3.2.5. *Корченко О.Г.*, Авіаційна безпека. Збірник документів, *Корченко О.Г., Бабак Н.В., Карпенко С.В., Пацюра Є.В., Шевчук В.О.*, К.: НАУ, 2003. - 235 с.
- 3.2.6. *Корченко О.Г.*, Інформаційна безпека та сучасні мережеві технології. Англоукраїнсько-російський словник термінів, *Бабак В.П., Корченко О.Г.*, Київ: НАУ.- 2003. - 670 с.

3.3. Інформаційні ресурси в Інтернет.

- 3.3.1. <https://nau.edu.ua/> - сайт Національного авіаційного університету.
- 3.3.2. <http://bit.nau.edu.ua/> - сайт кафедри безпеки інформаційних технологій НАУ.
- 3.3.3. <http://www.kdpu-nt.gov.ua/> - Комітет Державних премій України.
- 3.3.4. <https://mon.gov.ua/ua> - сайт Міністерства освіти і науки України.
- 3.3.5. <http://nfvy.ukrintei.ua/> - Реєстр наукових видань України.

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методи ідентифікації аномальних станів для системи виявлення вторгнень»	Шифр документа	СМЯ НАУ РПНД 07.01.07-01-2022
		стор. 10 з 12	

4. СИСТЕМА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання результатів навчальної діяльності.

Діагностика навчальних досягнень аспірантів здійснюється шляхом обов'язкового виконання аспірантами таких видів навчальної діяльності:

- робота на практичному занятті;
- ділова гра;
- виконання модульної контрольної роботи.

Форми контролю результатів навчання та їх оцінювання

Оцінювання навчальної роботи аспіранта здійснюється в балах відповідно до табл. 4.1.

Таблиця 4.1


Вид навчальної діяльності	Максимальна кількість балів	
	Очна форма навчання	Заочна форма навчання
Модуль № 1 «»		
Діяльність 1	106 x 5 = 50	256 x 2 = 50
Діяльність 2	20	20
Модульна контрольна робота №1	30	x
Підсумкова контрольна робота	x	30
Поточна модульна оцінка №1	100	x
Всього за модулем № 1	100	100
Диференційований залік (за наявності)	100	
Підсумкова рейтингова оцінка	100	

Переведення підсумкової рейтингової оцінки в балах в оцінки за національною шкалою та шкалою ECTS здійснюється відповідно до табл. 4.2.

Таблиця 4.2.

Відповідність підсумкової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	Відмінно	A	Відмінно (відмінне виконання лише з незначною кількістю помилок)
82-89	Добре	B	Дуже добре (вище середнього рівня з кількома помилками)
75-81		C	Добре (в загальному вірне виконання з певною кількістю суттєвих помилок)
67-74	Задовільно	D	Задовільно (непогано, але зі значною кількістю недоліків)
60-66		E	Достатньо (виконання задовольняє мінімальним критеріям)
35-59	Незадовільно	FX	Незадовільно (з можливістю повторного складання)
1-34		F	Незадовільно (з обов'язковим повторним курсом)

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методи ідентифікації аномальних станів для системи виявлення вторгнень»	Шифр документа	СМЯ НАУ РПНД 07.01.07-01-2022
		стор. 11 з 12	

Підсумкова рейтингова оцінка з дисципліни заноситься до заліково-екзаменаційної відомості, індивідуального навчального плану аспіранта та до академічної довідки про виконання освітньо-наукової програми.

Критерії оцінювання досягнень аспірантів.

Критерієм успішного проходження аспірантом оцінювання є досягнення ним мінімальних рівнів оцінок за кожним запланованим видом навчальної діяльності.

Виконані види навчальної роботи зараховуються аспіранту, якщо він отримав за них позитивну оцінку (за національною шкалою) відповідно до даних табл. 4.3.

Таблиця 4.3.

Відповідність рейтингових оцінок за окремими видами навчальної роботи в балах оцінкам за національною шкалою⁵

Рейтингова оцінка в балах				Оцінка за національною шкалою
Оцінка за діяльність 1 (очна/заочна)	Оцінка за діяльність 2	Модульна (підсумкова) контрольна оцінка	Поточна модульна оцінка	
9-10 / 23-25	18-20	23-30	90-100	Відмінно
8 / 19-22	15-17	21-27	75-89	Добре
6-7 / 15-18	12-14	19-23	60-74	Задовільно
менше 6 / 15	менше 12	менше 19	менше 60	Незадовільно

Аспірант допускається до виконання модульної контрольної роботи за умови наявності у нього поточної модульної рейтингової оцінки величиною не менше 60% максимальної поточної модульної рейтингової оцінки.

Слід мати на увазі, що отримання аспірантом лише мінімальних оцінок за виконання окремих видів навчальної роботи з певного модуля може виявитися недостатнім для отримання допуску до виконання модульної контрольної роботи та потребуватиме виконання ним додаткового індивідуального завдання, захистити його з позитивною оцінкою в балах, яка буде додана до поточної модульної рейтингової оцінки.

До екзамену аспірант допускається за умови отримання позитивних (за національною шкалою) контрольних модульних рейтингових оцінок.

У разі отримання незадовільних контрольної модульної чи екзаменаційної рейтингових оцінок аспірант повинен повторно пройти відповідний контроль в установленому порядку. При повторному його проходженні максимальна величина рейтингової оцінки в балах не повинна перевищувати максимальне значення оцінки «Добре» за національною шкалою.



(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайомлення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульованого			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				