МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ПРОЕКТ

ОСВІТНЬО-НАУКОВА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

третього (освітньо-наукового) рівня вищої освіти
за спеціальністю 125 Кібербезпека
галузі знань 12 Інформаційні технології

Тернопіль – 2024

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗІ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Західноукраїнський національний університет, кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії Доктор філософії з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії, одиничний, 240 кредитів ЄКТС, (термін навчання 4 роки), з них освітня складова 60 кредитів
Наявність акредитації	Первинна, 2024 р
Цикл/рівень	FQ-EHEA – третій цикл, EQF-LLL – 8 рівень, НРК України – 8 рівень
Передумови	Наявність ступеня вищої освіти магістр або освітньо-кваліфікаційного рівня спеціаліст
Мова(и) викладання	Українська
Термін дії освітньої програми	2021-2025 р.р.
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.wunu.edu.ua
2 – Мета освітньої програми	
Підготовка висококваліфікованих, конкурентоспроможних, інтегрованих у європейський та світовий науково-освітній простір фахівців із ступенем доктора філософії в галузі кібербезпеки здатних проводити наукові дослідження в галузі інформаційної безпеки та/або кібербезпеки, які мають теоретичні знання та сформоване критичне мислення достатні для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки; вміють безконфліктно та продуктивно працювати в командах щодо розв’язання проблем та прийняття рішень.	
3 - Характеристика освітньої програми	
Предметна область 125 Кібербезпека **Галузь знань**	**Об’єкти вивчення та діяльності:** інформаційні системи і технології, моделі, методи та механізми забезпечення кібербезпеки, захисту інформації в інформаційних і телекомунікаційних системах.

12 Інформаційні технології	**Цілі навчання**: здобуття наукового ступеня доктора філософії, формування у здобувачів теоретичних знань та підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області**: моделі і методи забезпечення кібербезпеки. **Методи, методики та технології**: математичні методи аналізу, розробки, оптимізації та застосування сучасних технологій та засобів забезпечення інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Програма зорієнтована на формування загальнонаукових, науково-дослідних, спеціальних та мовних компетенцій, що дадуть можливість аспірантам отримати концептуальні та методологічні знання в галузі інформаційної безпеки та/або кібербезпеки для започаткування, планування, коригування та реалізації ґрунтовного самостійного наукового дослідження та його успішного захисту у формі дисертаційної роботи.
Основний фокус освітньої програми	Підготовка фахівців для проведення досліджень та науково-технічних розробок у галузі інформаційної безпеки та\або кібербезпеки. Ключові слова: інформаційна безпека, кібербезпека, шифрування, криптоаналіз, безпека Інтернет речей та кіберфізичних систем.
Особливості програми	
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Робота на посадах, пов'язаних з науково-дослідною, викладацькою, експертною та прикладною діяльністю у сфері захисту кіберпростору. Професіонал підготовлений до роботи в галузі економіки за ДК 009: 2010: - Наукові дослідження та розробки (код 72). - Вища освіта (код 85.4). Професіонал здатний виконувати зазначену(і) професійну (і) роботу(и) за ДК 003:2010: 2310 Викладачі університетів та вищих навчальних закладів 2131.1 Наукові співробітники (обчислювальні системи) 2132.1 Наукові співробітники (програмування) 2139.1 Наукові співробітники (інші галузі обчислень) 2144.1 Наукові співробітники (електроніка, телекомунікації) 433.1 Наукові співробітники (інформаційна аналітика)
Подальше навчання	Може продовжувати наукову діяльність для здобуття наукового ступеня доктора наук
5 – Викладання та оцінювання	
Викладання та навчання	При викладанні навчальних дисциплін використовується студентоцентрований підхід організації навчання, коли аспіранти через стиль викладання, орієнтований на дослідження, залучаються до пізнавальної роботи, що дозволяє кожному з них не тільки набути концептуальні знання, але й критично сприймати їх, що, своєю

	чергою, дає можливість генерувати нові ідеї, гіпотези на емпірично їх перевіряти. Участь аспірантів у круглих столах, щорічних міжнародних науково-практичних конференціях факультету комп'ютерних інформаційних технологй, в рамках яких провідні професори проводять семінари щодо перспективних напрямків досліджень та підготовки наукових публікацій, дають можливість формувати вміння аргументовано презентувати свої ідеї, відстоювати їх в процесі дискусій. Навчання та викладання організовано у навчальних групах у системі: проблемна лекція – практичне заняття- дискусія, індивідуальні та групові завдання Освітньо-науковий процес здійснюється на засадах компетентнісного, системного, інтегративного підходів із застосуванням інноваційних технологій, елементів дистанційного навчання у системі Moodle, проходження науково-педагогічної практики, що визначає дослідницький характер навчання
Оцінювання	Поточні звіти, наукові дискусії у аудиторіях, презентації, усні презентації, усні та письмові екзамени, захист науково-педагогічної практики. Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність виявляти та розв'язувати комплексні проблеми в сфері інформаційної безпеки та\або кібербезпеки, досліджувати, формулювати, розв'язувати наукові та інноваційні проблеми в умовах комплексності та недостатньої визначеності умов, що передбачає глибоке переосмислення наявних і створення нових знань та/або професійної практики.
Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК3. Готовність до проблемно-орієнтованого професійного спілкування як українською так і іноземною мовою. ЗК4. Здатність проведення самостійних досліджень на сучасному рівні. ЗК5. Здатність здійснювати науково-педагогічну діяльність у вищій освіті. ЗК6. Здатність до розвитку та вдосконалення існуючих рішень, генерації нових ідей. ЗК7. Здатність дотримуватися етики досліджень, а також правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності.
Спеціальні компетентності (СК)	СК-1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі кібербезпеки. СК-2. Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок українською та англійською мовами, глибоке розуміння

	англомовних наукових текстів в галузі кібербезпеки та інформаційних технологій. СК-3. Здатність ефективно застосовувати методи аналізу, математичне моделювання, виконувати натурні та математичні експерименти при проведенні наукових досліджень. СК-4. Здатність інтегрувати знання з різних дисциплін, застосовувати системний підхід та враховувати нетехнічні аспекти при розв'язанні інженерних задач та проведенні досліджень. СК-5. Розуміння принципів функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації, а також систем управління інформаційною безпекою. СК-6. Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки, а також суміжних і прикладних областей. СК-7. Здатність використовувати методи фундаментальних і прикладних дисциплін для опрацювання, аналізу й синтезу результатів досліджень. СК-8. Здатність використовувати методи штучного інтелекту для задач кібербезпеки та глибоке розуміння їх математичного апарату.
7 – Програмні результати навчання	
	ПРН-1. Знати закономірності впливу прийнятих технічних рішень на функціонування соціальних, економічних та екологічних систем. ПРН-2. Знати сучасні методи проведення досліджень в галузі кібербезпеки. ПРН-3. Уміти вести дискусії і полеміки, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами. ПРН-4. Знати методи штучного інтелекту та вміння використовувати їх у задачах за фахом ПРН-5. Вміти ефективно здійснювати пошук та критичний аналіз інформації з різних джерел. ПРН-6. Вміти розв'язувати задачі синтезу та аналізу об'єктів професійної діяльності кібербезпеки. ПРН-7. Вміти досліджувати проблеми кібербезпеки критичної інфраструктури. ПРН-8. Вміти синтезувати науково обґрунтовані рішення по захисту інформації в кіберсистемах та кіберфізичних системах. ПРН-9. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей. ПРН-10. Вміти ефективно працювати як індивідуально, так і у складі команди. ПРН-11. Вміти ефективно поєднувати теорію і практику, задля вирішення науково-прикладних завдань в галузі кібербезпеки з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів. ПРН-12. Вміти самостійно проводити експериментальні дослідження в предметній області згідно обраної наукової тематики.

	ПРН-13. Вміти обґрунтовувати вибір методів розв'язання науково-прикладних задач та критично оцінювати отримані результати, аргументовано захищаючи прийняті рішення. ПРН-14. Вміти аналізувати та впроваджувати у власну діяльність теоретично обґрунтовані положення сучасного педагогічного досвіду. ПРН-15. Уміти визначати основні параметри інформаційних ресурсів наукового дослідження (навчального процесу), планувати структуру, зміст та процес організації його проведення (лекцій та практичних занять). ПРН-16. Уміти приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, залучені до реалізації освітньо-наукової програми мають науковий ступінь і/або вчене звання та підтверджений рівень наукової і професійної активності, що відповідає вимогам ліцензійних умов. Науково-педагогічні працівники, що забезпечують освітньо-наукову програму, мають показники академічної та професійної кваліфікації відповідно до дисципліни, викладання якої вони забезпечують. Підготовку фахівців здійснюють спеціалізовані кафедри університету. У процесі організації освітнього процесу залучаються професіонали з досвідом управлінської та фахової діяльностей.
Матеріально-технічне забезпечення	Освітній процес здійснюється в спеціально обладнаних аудиторіях і лабораторіях, які відповідають санітарно-технічним нормам і оснащених сучасним навчальним обладнанням, мультимедійною, комп'ютерною технікою та спеціалізованим програмним забезпеченням, з можливістю постійного доступу до мережі Internet та внутрішньої мережі ЗУНУ. Комп'ютерна лабораторія обладнана наступним устаткуванням: проектор мультимедійний BenQ TH671ST (1 шт.); комп'ютери на базі процесора Intel Xeon W3550, (10 шт): системний блок Precsion T3500 Westmere. N-serie; монітор Dell E2211H 21.5in.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт http://www.wunu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньо-наукової програми викладені в інституційному репозитарії бібліотеки ЗУНУ ім. Л. Каніщенка: http://library.wunu.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Усі ресурси бібліотеки доступні через сайту університету: http://www.wunu.edu.ua
9 – Академічна мобільність	

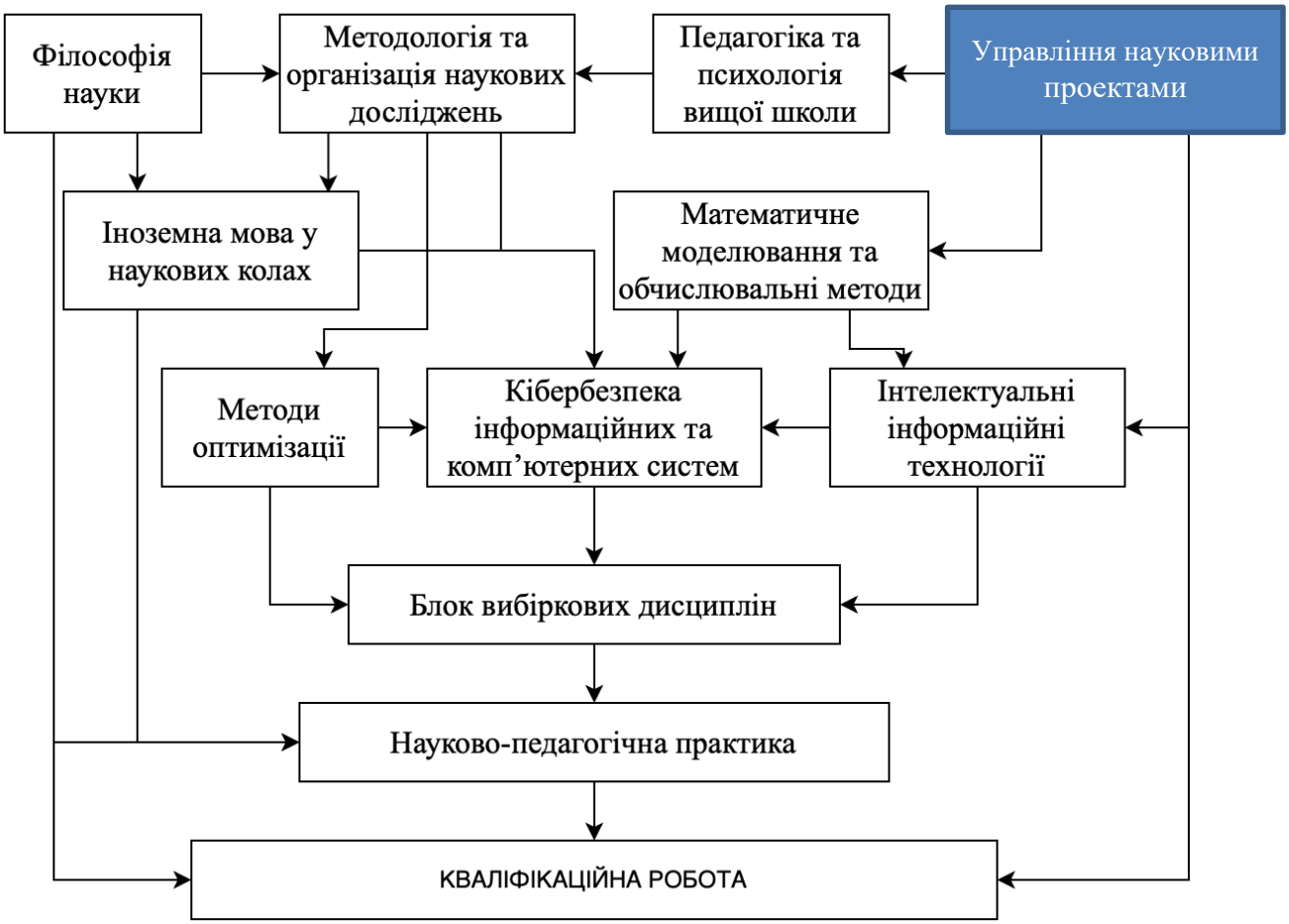
Національна кредитна мобільність	Відповідно до угод Університету.
Міжнародна кредитна мобільність	Відповідно до угод Університету та угод про міжнародну академічну мобільність (Еразмус+ К1)
Навчання іноземних здобувачів вищої освіти	Відповідно до нормативно-правових документів.

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ

2.1. Перелік компонент ОНП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ДИСЦИПЛІНИ ЗАГАЛЬНОНАУКОВОЇ (ФІЛОСОФСЬКОЇ) ПІДГОТОВКИ			
ОК 1.	Філософія науки	4	екзамен
ОК 2.	Педагогіка та психологія вищої школи	4	залік
ДИСЦИПЛІНИ МОВНОЇ ПІДГОТОВКИ			
ОК 3.	Іноземна мова у наукових колах	6	екзамен
ДИСЦИПЛІНИ НАУКОВО-ДОСЛІДНОЇ ПІДГОТОВКИ			
ОК 4.	Методологія та організація наукових досліджень	4	залік
ОК 5.	Управління науковими проектами	5	залік
ОК 6.	Математичне моделювання та обчислювальні методи	5	залік
ОК 7.	Науково-педагогічна практика	5	залік
ДИСЦИПЛІНИ ПІДГОТОВКИ ЗІ СПЕЦІАЛЬНОСТІ			
ОК 8.	Методи оптимізації	4	екзамен
ОК 9.	Інтелектуальні інформаційні технології	4	екзамен
ОК 10.	Кібербезпека інформаційних та комп’ютерних систем	4	екзамен
ДИСЦИПЛІНИ ЗА ВИБОРОМ АСПІРАНТА			
	Дисципліна за вибором 1	5	залік
	Дисципліна за вибором 2	5	залік
	Дисципліна за вибором 3	5	залік
Загальний обсяг обов’язкових компонентів:		**45**	
Загальний обсяг вибіркових компонентів:		**15**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**60**	

2.2. Структурно-логічна схема освітньо-професійної програми «Кібербезпека»



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена у репозитарії ЗУНУ. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	**ОК 2**	**ОК 3**	**ОК 4**	**ОК 5**	**ОК6**	**ОК 7**	**ОК 8**	**ОК 9**	**ОК 10**
ЗК-1	•			•						
ЗК-2				•	•					
ЗК-3			•							
ЗК-4				•						
ЗК-5		•					•			
ЗК 6						•		•		
ЗК 7					•					
ФК 1				•						•
ФК 2			•							•
ФК 3						•		•		
ФК 4							•	•		
ФК 5							•			•
ФК 6									•	•
ФК 7						•		•		
ФК 8						•			•	

5. Матриця забезпечення програмних результатів навчання (РН) відповідними компонентами освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК6	ОК 7	ОК 8	ОК 9	ОК 10
РН 1	•			•						
РН 2				•			•			
РН 3		•	•				•			
РН 4									•	
РН 5					•	•				
РН 6						•		•		•
РН 7							•			•
РН 8				•						•
РН 9		•		•	•					
РН 10		•		•						
РН 11							•			•
РН 12				•						
РН 13						•		•		
РН 14		•								
РН 15					•		•			
РН 16					•			•		