МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ПРОЄКТ

ОСВІТНЬО-НАУКОВА ПРОГРАМА
«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

третього (освітньо-наукового) рівня вищої освіти
за спеціальністю F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Тернопіль – 2025

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗІ СПЕЦІАЛЬНОСТІ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

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 та захисту інформації
Офіційна назва освітньої програми	Кібербезпека та захист інформації
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, 2026 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	2025-2029 рр.
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 F5 Кібербезпека та захист інформації	**Об’єкти вивчення та діяльності:** – інформаційні системи і технології на об'єктах інформаційної діяльності та критичної інфраструктури сфери кібербезпеки та захисту інформації;

Галузь знань F Інформаційні технології	– новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків); – сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою та захистом інформації; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. **Цілі навчання**: набуття здатності продукувати нові ідеї, розв'язувати комплексні проблеми професійної та дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, та здійснювати власні наукові дослідження, результати яких мають наукову новизну, теоретичне та практичне значення. **Теоретичний зміст предметної області.** Принципи, концепції, теорії захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології.** Сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, методи статистичного аналізу даних. **Інструменти та обладнання.** Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та система автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні, технології, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплексу проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків).
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, децентралізовані та кіберфізичні системи.
Особливості програми	Освітня програма орієнтована на розробку та дослідження криптосистем на основі системи залишкових класів, дослідження їх криптостійкості.
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 технологій, 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 продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу і синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК3. Здатність працювати в міжнародному контексті. ЗК4. Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.
Спеціальні (фахові, предметні) компетентності (СК)	СК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації. СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики. СК4. Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації. СК5. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. СК6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому українською та англійською мовами. СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.
7 – Програмні результати навчання	
	РН1. Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і

	прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. РН2. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики. РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН4. Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці. РН5. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. РН6. Вільно презентувати та обговорювати з фахівцями і не фахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях. РН7. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації. РН8. Розробляти та досліджувати концептуальні, математичні і комп’ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах. РН9. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи. РН10. Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.
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 КОМПОНЕНТ ОСВІТНЬО-НАУКОВОЇ 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 дослідженнях	6	екзамен
ДИСЦИПЛІНИ НАУКОВО-ДОСЛІДНОЇ ПІДГОТОВКИ			
ОК 4.	Методологія та організація наукових досліджень	4	залік
ОК 5.	Управління науковими проєктами	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 шифрування в системі залишкових класів	4	екзамен
ОК 9.	Оцінка складності алгоритмів шифрування	4	екзамен
ОК 10.	Криптографія в децентралізованих системах	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 компонент:		**45**	
Загальний обсяг вибіркових компонент:		**15**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**60**	

2.2. Структурно-логічна схема освітньо-наукової програми «Кібербезпека та захист інформації»

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів освітнього рівня доктора філософії здійснюється у формі публічного захисту дисертації.
Вимоги до кваліфікаційної роботи	Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання комплексної проблеми в сфері кібербезпеки та захисту інформації, результати якого мають наукову новизну, теоретичне та практичне значення. Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації. Дисертація має бути розміщена у репозитарії ЗУНУ.

4. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програмитьб

	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						+				
СК 1								+	+	+
СК 2					+				+	
СК 3						+				+
СК 4						+			+	
СК 5				+				+		
СК 6			+				+			
СК 7		+			+		+			

5. Матриця забезпечення програмних результатів навчання (РН) відповідними компонентами освітньо-наукової 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				+	+		+			