МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО – НАУКОВА ПРОГРАМА

«Кібербезпека»

третього (освітньо-наукового) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Кваліфікація: Доктор філософії з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Заступник голови Вченої ради_____ Олександр ФИЛИПЕНКО

(протокол від "_28_" _лютого_ 2023 р. № 2)

Освітня програма вводиться в дію з 02 березня 2023 р.

В.о. ректора_____ Ігор РУБАН

(наказ від "_02_" _березня_ 2023 р. № _34_)

Харків 2023 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-наукової програми
«Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації
третього (освітньо-наукового) рівня вищої освіти

УЗГОДЖЕНО

Перший проректор

_____ Ігор РУБАН

«_25» ___січня__ 20_23 р.

Начальник навчального відділу

_____ Аліна МІХНОВА

«_25_» __січня__ 2023 р.

Начальник відділу ЛА та ВСЗЯО

Сергій МАКАШЕВ

«_25_» ___січня__ 20_23 р.

Завідувач відділу аспірантури та докторантури

_____Володимир МАНАКОВ

«25» січня 2023 р.

Розглянуто на засіданні Вченої Ради
факультету КІУ
Протокол __від «25»_01.2023 р. №_6_ _
Декан факультету КІУ

_____ Олексій ЛЯШЕНКО

Розглянуто на засіданні кафедри БІТ
Протокол від «11» 01.2023 р. №_6_
Завідувач кафедри БІТ

_____ Геннадій ХАЛІМОВ

Розглянуто на засіданні Вченої Ради
факультету ІК
Протокол від «18»_01.2023 р. №_1_
Декан факультету ІК

_____ Аркадій СНІГУРОВ

Розглянуто на засіданні кафедри ІКІ
ім. В.В. Поповського
Протокол від «28» 12.2022 р. № 12___
Завідувач кафедри ІКІ ім. В.В. Поповського

_____ Олександр ЛЕМЕШКО

Представники роботодавців

Технічний директор приватного акціонерного товариства
«Інститут інформаційних технологій» _____ Олександр ШУМОВ

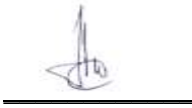
Генеральний директор товариства з
обмеженою відповідальністю «МНС ГРУП» _____ Григорій МАЗУР

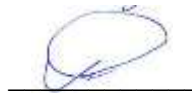
Представник ради молодих вчених
Наукового товариства молодих учених
В.о. голови Ради молодих вчених
к.т.н., доцент, доцент кафедри ЕОМ _____ Віталій ТКАЧОВ

РОЗРОБЛЕНО

Проєктна група:
керівник проєктної групи:
Халімов Геннадій Зайдулович,
д.т.н., професор, завідувач кафедри БІТ ХНУРЕ 

члени проєктної групи:
Сєвєрінов Олександр Васильович,
к.т.н., доцент, доцент кафедри БІТ ХНУРЕ 

Олейніков Анатолій Миколайович,
к.т.н., професор, професор кафедри КРіСТЗІ ХНУРЕ 

Снігуров Аркадій Владиславович,
к.т.н., доцент, декан факультету ІК ХНУРЕ 

ПЕРЕДМОВА

Розроблено проектною групою у складі:

Керівник проектної групи:

Халімов Геннадій Зайдулович, доктор технічних наук, професор, завідувач кафедри БІТ, факультету КІУ ХНУРЕ.

Члени проектної групи:

Сєвєрінов Олександр Васильович, кандидат технічних наук, доцент, доцент кафедри БІТ, факультету КІУ ХНУРЕ;

Олейніков Анатолій Миколайович, кандидат технічних наук, професор, професор кафедри КРіСТЗІ, факультету ІРТЗІ ХНУРЕ;

Снігуров Аркадій Владиславович, кандидат технічних наук, доцент, декан факультету ІК ХНУРЕ.

Гарант освітньої програми
«Кібербезпека»  Геннадій ХАЛІМОВ

1. Профіль освітньої програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки. Факультет комп'ютерної інженерії та управління (КІУ) Кафедра Безпеки інформаційних технологій (БІТ). Факультет інфокомунікацій Кафедра інфокомунікаційної інженерії ім. В.В. Поповського (ІКІ)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії Доктор філософії з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії (PhD), одиничний, 30 кредитів ЄКТС освітньої складової освітньо-наукової програми, термін освітньої складової освітньо-наукової програми – 1 рік термін навчання 4 роки
Наявність акредитації	Сертифікат про акредитацію освітньої програми від 29.03.2022 р. №3004 Строк дії сертифікату: до 01.07. 2027 р.
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Наявність ступеня магістра або ОКР спеціаліста
Мова(и) викладання	Українська мова, англійська мова
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	https://nure.ua/branch/viddil-aspiranturi-ta-doktoranturi/specialnosti-ta-osvitno-naukovi-programi/125-kiberbezpeka
2 - Мета освітньої програми	
Підготовка висококваліфікованих, інтегрованих у світовий простір фахівців, які володіють методами дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних з організацією, створенням методів і засобів забезпечення інформаційної та кібербезпеки з використанням сучасних математичних методів, інформаційних технологій і технічних засобів, проведення педагогічної, наукової та дослідницько-інноваційної діяльності, а також впровадження отриманих результатів.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології, 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-наукова програма Освітньо-наукова програма ґрунтується на результатах сучасних наукових досліджень у сфері кібербезпеки. Спрямована на актуальні аспекти спеціальності, в рамках якої можлива подальша наукова та викладацька кар'єра.

Основний фокус освітньої програми та спеціалізації	Формування необхідних дослідницьких навиків для наукової кар'єри та викладання спеціальних дисциплін в галузі інформаційної безпеки та кібербезпеки **Ключові слова:** кібербезпека, інформаційна безпека, захист інформації, криптографічний захист інформації, захист персональних даних, антивірусний захист, технічний захист інформації, захист від несанкціонованого доступу, управління інформаційною безпекою
Особливості програми	Підготовка докторів філософії за програмою відрізняється акцентом у програмах дисциплін на особливостях забезпечення інформаційної безпеки та кібербезпеки у постквантовий період. Наукова складова освітньо-наукової програми визначається індивідуальним навчальним планом підготовки доктора філософії.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування на посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти, інших посадах, що потребують кваліфікації доктора філософії з кібербезпеки, зокрема на посадах наукових консультантів, експертів, аналітиків у дослідницьких установах і підрозділах підприємств, установ, організацій. Назва професій (робіт) згідно з Національним класифікатором України «Класифікатор професій» (ДК 003:2010): 1226.2 Начальник відділення установи, організації (сфера захисту інформації); 1229.7 (99) Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної); 2149.2 Професіонал із організації інформаційної безпеки; 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2149.1 Наукові співробітники (інформаційна та кібербезпека); 2149.2 Фахівець (сфера захисту інформації); 2310 Викладачі університетів та вищих навчальних закладів; 2310.1 Докторант; 2310.1 Доцент.
Подальше навчання	Здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих
5 - Викладання та оцінювання	
Викладання та навчання	Для освітньої складової: лекції, практичні заняття, консультації, самостійна робота, педагогічна практика. Для наукової складової: проведення наукового дослідження, консультування з науковим керівником, оприлюднення результатів досліджень, спілкування з представниками наукової спільноти, підготовка та захист дисертації.
Оцінювання	Для освітньої складової – поточний та семестровий контроль. Оцінювання навчальних досягнень здобувачів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано), 100-бальною шкалою та шкалою ЄКТС (A, B, C, D, E, FX, F). Для наукової складової – проміжна та річна атестації у формі звітування на засіданні кафедри та Вченої ради факультету. Атестація здійснюється у формі публічного захисту дисертації

6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати комплексні проблеми кібербезпеки у професійної та дослідницько-інноваційної діяльності, що передбачає глибоке переосмислення наявних та створення нових цілісних знань у галузі кібербезпеки та їх застосування у професійній практиці.
Загальні компетентності (ЗК)	ЗК01. Здатність сформувати системний науковий світогляд, опанувати принципи критичного мислення, основи професійної етики та загального культурного кругозору. ЗК02. Здатність демонструвати поведінку зрілої особистості, яка володіє цілісним та системним психолого-педагогічним та науковим світоглядом, розумінням завдань та методів викладання на сучасному етапі розвитку суспільства та освіти; опанувала базовими знаннями і уміннями наукового пошуку та вміннями використання його результатів в реальній практичній діяльності; застосовує прийоми ефективної комунікації в професійному середовищі. ЗК03. Здатність навчатися та самонавчатися, генерувати нові ідеї. ЗК04. Здатність до пошуку, оброблення та узагальнення науково-технічної інформації з різних джерел (у тому числі іншомовної літератури за фахом). ЗК05. Здатність вільно спілкуватися в усній та письмовій формі з питань, що стосуються сфери наукових досліджень, з колегами, науковою спільнотою, суспільством у цілому державною та іноземною мовами.
Фахові компетентності спеціальності (ФК)	СК01. Здатність застосовувати методологію та технології інтелектуального аналізу даних, реалізовувати його методи й алгоритми для дослідження складних об'єктів і систем, перевіряти отримані результати та інтерпретувати їх. СК02. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання і можуть бути опубліковані у провідних наукових виданнях. СК03. Здатність до продукування нових ідей і розв’язання комплексних проблем на основі застосування методології наукових досліджень та інструментів наукової діяльності. СК04. Здатність здійснювати педагогічну діяльність у вищому навчальному закладі у галузі інформаційної та кібербезпеки. СК05. Здатність використовувати сучасні досягнення науки, передові технології та математичні методи для розв’язування задач забезпечення інформаційної та кібербезпеки. СК06. Здатність аналізувати, використовувати, оцінювати ефективність та розробляти методи і засоби криптографічного та технічного захисту для забезпечення інформаційної та кібербезпеки в умовах сучасних загроз та викликів.
7 - Програмні результати навчання	
Програмні результати навчання (ПРН)	РН01. Володіти навичками критичного аналізу наукової інформації та результатів наукових досліджень, розуміти особливості взаємозв'язку наукових і технічних задач з сучасними соціальними та етичними проблемами, застосовувати отримані знання під час вирішення наукових проблем та прикладних проектів. РН02. Глибоко розуміти загальні принципи і методологію наукових досліджень, застосувати їх у власних дослідженнях та у викладацькій практиці.

	РН03. Використовувати знання про психологічно-педагогічні особливості науково-педагогічної діяльності в професійному освітньо-науковому процесі при розробці та викладанні спеціальних дисциплін. РН04. Застосовувати універсальні мовні навички дослідника, що дозволяють обирати оптимальні форми та жанри мовлення (в тому числі іноземною мовою) для подання наукової інформації у науковій та педагогічній діяльності. РН05. Застосовувати принципів підготовки та проголошення результатів дослідження за умов дотримання вимог академічної етики та доброчесності, використання відповідних засобів вираження наукової думки. РН06. Вміти написати наукову статтю (доповідь) державною та/або іноземною мовою з використанням наукової та навчальної літератури, довідників, словників, документів та іншої науково-технічної інформації з відповідної галузі знань з дотриманням норм авторського права. РН07. Знати та розуміти основні методи аналізу даних, вміти застосовувати інструменти та моделі аналізу даних (пакети прикладних програм, онлайн ресурси й відповідні технології) в дослідженні реальних систем та презентації результатів наукових досліджень у різних формах; здійснювати науково-педагогічну діяльності з використанням цих ресурсів. РН08. Планувати і виконувати експериментальні та/або теоретичні дослідження з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН09. Уміти застосовувати, удосконалювати та розробляти нові математичні моделі та методи забезпечення інформаційної та кібербезпеки, а також виконувати їх експериментальну перевірку з використанням сучасних інформаційних технологій. РН10. Застосовувати знання і розуміння фізико-математичних методів побудови систем захисту при проведенні досліджень, розробці нових методів й засобів забезпечення інформаційної та кібербезпеки, спираючись на сучасні досягнення світової науки.
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації (з науковим ступенем та вченим званням), які мають великий досвід науково-педагогічної, навчально-методичної, науково-дослідної роботи та відповідають кваліфікації згідно з ліцензійними умовами провадження освітньої діяльності. Науково-педагогічні працівники, які забезпечують реалізацію освітньої програми, є авторами навчальних посібників, наукових статей, монографій, беруть активну участь у науково-практичних заходах, мають свідоцтва про реєстрацію авторського права.
Матеріально-технічне забезпечення	Навчальний процес відбувається у аудиторіях та лабораторіях, обладнаних сучасними комп'ютерними та технічними засобами, в тому числі мультимедійними, а також спеціалізованим програмним забезпеченням.
Інформаційне та	1. Забезпеченість бібліотеки вітчизняними та закордонними

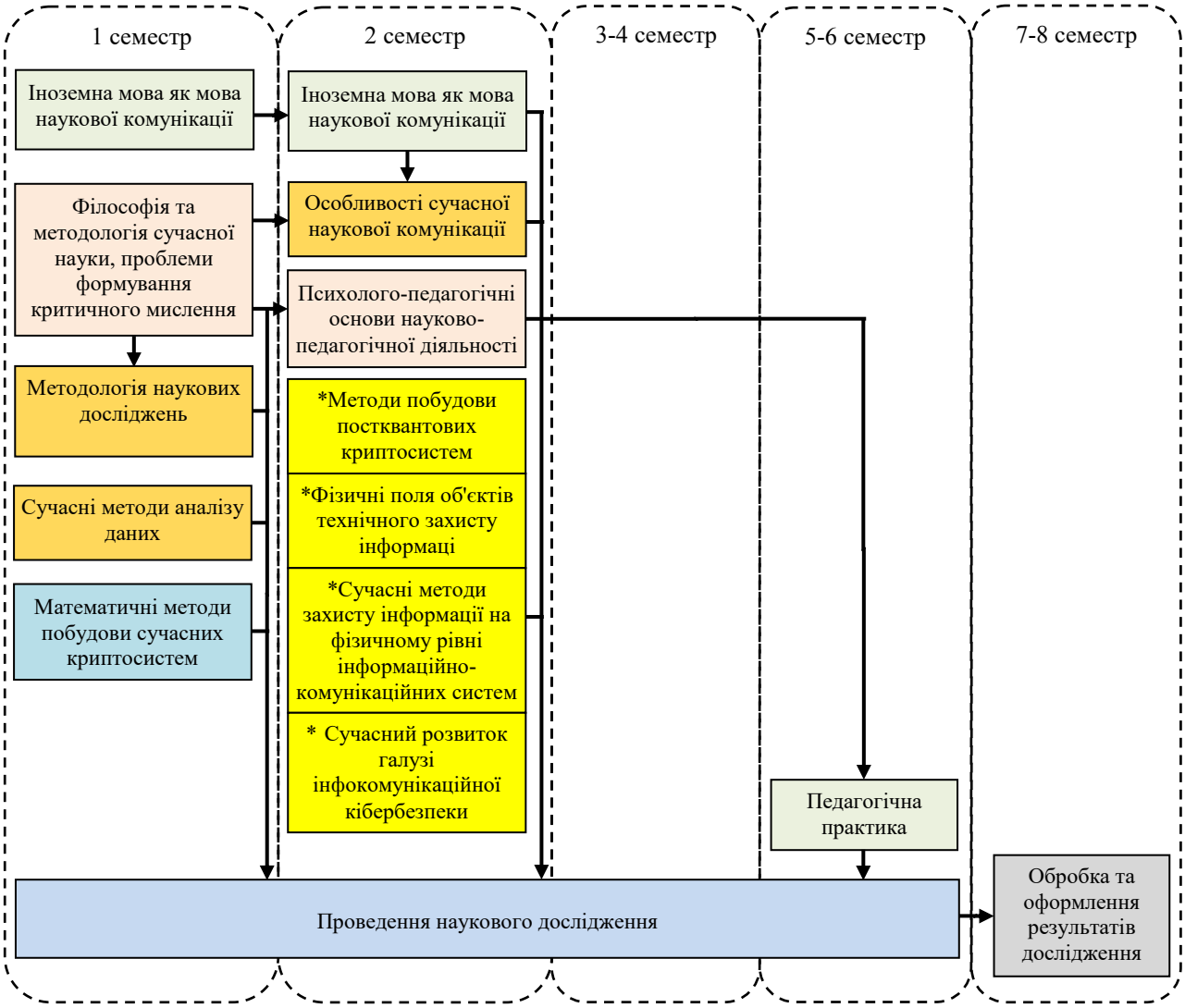
навчально-методичне забезпечення	фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. Сайт наукової бібліотеки ХНУРЕ http://lib.nure.ua. Електронний архів відкритого доступу Харківського національного університету радіоелектроніки http://openarchive.nure.ua. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Сайт ХНУРЕ http://nure.ua. 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання. Наукова бібліотека ХНУРЕ та фонди кафедр БІТ, ІКІ ім. В.В. Поповського, КРіСТЗІ, РТІКС, ІМ, філософії, ІУС, українознавства, ПМ ХНУРЕ.
9 — Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів між Харківським національним університетом радіоелектроніки і закладами вищої освіти країн-партнерів.

2. Перелік компонентів освітньої програми та їх логічна послідовність

2.1. Перелік компонентів ОП

Код	Компоненти освітньої програми	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
ОСВІТНЯ СКЛАДОВА			
Обов'язкові компоненти ОП			
1.Загальнонаукові (філософські) дисципліни			
ОК 1.1	Філософія та методологія сучасної науки, проблеми формування критичного мислення	3	залік
ОК 1.2	Психолого-педагогічні основи науково-педагогічної діяльності	2	залік
2.Дисципліни, що формують універсальні навички дослідника			
ОК 2.1	Методологія наукових досліджень	3	залік
ОК 2.2	Особливості сучасної наукової комунікації	2	залік
ОК 2.3	Сучасні методи аналізу даних	2	залік
3.Дисципліни, що формують мовні компетентності			
ОК 3.1	Іноземна мова як мова наукової комунікації	6	залік
4.Дисципліни зі спеціальності			
ОК 4.1	Математичні методи побудови сучасних криптосистем	4	залік
Загальний обсяг обов'язкових компонентів:		**22**	
Вибіркові компоненти ОП			
Дисципліни зі спеціальності (вибіркові)			
ВБ 1.1	Методи побудови постквантових криптосистем	8	залік
ВБ 1.2	Фізичні поля об'єктів технічного захисту інформації	8	залік
ВБ 1.3	Сучасні методи захисту інформації на фізичному рівні інформаційно-комунікаційних систем	8	залік
ВБ 1.4	Сучасний розвиток галузі інфокомунікаційної кібербезпеки	8	залік
Загальний обсяг вибіркових компонентів:		**8**	
ПП	**Педагогічна практика**	**2**	залік
Загальний обсяг освітньої складової		**32**	
НАУКОВА СКЛАДОВА			
Наукові дослідження		**148**	
Робота над дисертацією		**60**	
Загальний обсяг наукової складової		**208**	
УСЬОГО ПІДГОТОВКА ДОКТОРА ФІЛОСОФІЇ		**240**	

2.1. Структурно-логічна схема ОП



*Дисципліни зі спеціальності (вибіркові)

3. Форма атестації здобувачів вищої освіти

Проміжна атестація здобувачів вищої освіти ступеня доктора філософії спеціальності 125 Кібербезпека та захист інформації проводиться два рази на рік протягом навчання (піврічна проміжна та щорічна). Метою проміжних звітів є контроль за виконанням індивідуального плану аспіранта за всіма складовими, передбаченими навчальним планом.

Підсумковий контроль за дисциплінами навчального плану підготовки аспірантів здійснюється профільними кафедрами.

Під час атестації аспіранта враховується виконання освітньої і наукової складових освітньо-наукової програми 125 «Кібербезпека».

Аспіранти, що успішно пройшли щорічну атестацію, переводяться на наступний рік навчання. Аспіранти, які не пройшли атестацію, підлягають відрахуванню.

Стан готовності дисертації здобувача вищої освіти ступеня доктора філософії до захисту визначається науковим керівником (або консенсусним рішенням двох керівників).

Обов’язковою умовою допуску до захисту є успішне виконання аспірантом його індивідуального навчального плану.

Підсумкова атестація здобувачів вищої освіти ступеня доктора філософії спеціальності 125 Кібербезпека здійснюється спеціалізованою вченою радою, постійно діючою або утвореною для проведення разового захисту, на підставі публічного захисту наукових досягнень у формі дисертації.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1.1	ОК 1.2	ОК 2.1	ОК 2.2	ОК 2.3	ОК 3.1	ОК 4.1	ПП
ЗК 1	+							
ЗК 2		+						+
ЗК 3	+	+	+					
ЗК 4			+	+		+		
ЗК 5				+		+		+
ФК 1					+			
ФК 2			+				+	
ФК 3			+		+			
ФК 4		+						+
ФК 5							+	
ФК 6							+	

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

	ОК 1.1	ОК 1.2	ОК 2.1	ОК 2.2	ОК 2.3	ОК 3.1	ОК 4.1	ПП
ПРН-1	+							
ПРН-2	+	+	+					+
ПРН-3		+						+
ПРН-4				+		+		+
ПРН-5				+		+		
ПРН-6				+		+		
ПРН-7					+			
ПРН-8			+		+			
ПРН-9							+	
ПРН-10							+	

6. Матриця відповідності визначених стандартом компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	**Знання** **Зн1** Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності.	**Уміння** **Ум1** Спеціалізовані уміння/навички і методи, необхідні для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики. **Ум2** Започаткування, планування, реалізація та коригування послідовного процесу ґрунтовного наукового дослідження з дотриманням належної академічної доброчесності. **Ум3** Критичний аналіз, оцінка і синтез нових та комплексних ідей.	**Комунікація** **К1** Вільне спілкування з питань, що стосуються сфери наукових та експертних знань, з колегами, широкою науковою спільнотою, суспільством у цілому. **К2** Використання академічної української та іноземної мови у професійній діяльності та дослідженнях.	**Автономія та відповідальність** **АВ1** Демонстрація значної авторитетності, інноваційність, високий ступінь самостійності, академічна та професійна доброчесність, постійна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності. **АВ2** Здатність до безперервного саморозвитку та самовдосконалення.
Загальні компетенції				
ЗК1	**Зн1**	**Ум2, Ум3**	**К1**	**АВ1**
ЗК2	**Зн1**	**Ум1**	**К1, К2**	**АВ1, АВ2**
ЗК3	**Зн1**	**Ум1, Ум3**	**К2**	**АВ1, АВ2**
ЗК4	**Зн1**	**Ум1, Ум3**	**К2**	**АВ1, АВ2**
ЗК5	**Зн1**	**Ум1, Ум3**	**К1, К2**	**АВ1**
Фахові компетенції				
ФК1	**Зн1**	**Ум1, Ум2, Ум3**	**К1**	**АВ1, АВ2**
ФК2	**Зн1**	**Ум1, Ум2, Ум3**	**К1**	**АВ1, АВ2**
ФК3	**Зн1**	**Ум1, Ум2, Ум3**	**К1**	**АВ1, АВ2**
ФК4	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1, АВ2**
ФК5	**Зн1**	**Ум1, Ум2, Ум3**	**К1**	**АВ1, АВ2**
ФК6	**Зн1**	**Ум1, Ум2, Ум3**	**К1, К2**	**АВ1, АВ2**

7. Наукова та педагогічна компоненти ОНП

Наукова складова освітньо-наукової програми передбачає проведення аспірантами власного наукового дослідження під керівництвом наукових керівників (одного або двох) та оформлення їх результатів у вигляді дисертації.

Педагогічна складова забезпечує підготовку здобувачів до можливої подальшої викладацької діяльності в ЗВО.

7.1. Наукова компонента ОНП

Наукова складова освітньо-наукової програми оформляється у вигляді індивідуального плану наукової роботи аспіранта і є невід'ємною частиною навчального плану аспірантури.

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання актуального наукового завдання за спеціальністю 125 Кібербезпека, результати якого характеризуються науковою новизною та практичною цінністю.

Невід'ємною частиною наукової складової освітньо-наукової програми аспірантури є підготовка та публікація наукових статей, виступи на наукових конференціях, наукових фахових семінарах, круглих столах, симпозіумах.

Науково-дослідна тематика дисертаційних робіт пов'язана з науковою проблематикою кафедр БІТ та ІКІ ХНУРЕ та спрямована на формування компетенцій проведення наукових досліджень у галузі інформаційної та кібербезпеки.

Основні напрямки досліджень:

- теоретичні, методологічні, технічні, технологічні та організаційні основи створення комплексних систем захисту інформації (КСЗІ), зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах;
- дослідження та розробка методичних основ, та концептуальних положень процесного підходу до захисту інформації;
- організація, архітектура, методологія проектування, технологія функціонування КСЗІ;
- технічні канали витоку інформації та їх моделі, нові технології та засоби захисту інформації від витоку технічними каналами;
- дослідження та обґрунтування вимог, проектування, створення методів блокового симетричного шифрування, гешування та направленого шифрування інформації, дослідження ефективності та криптографічної стійкості;
- криптографічні протоколи та способи вибору систем криптозахисту, адекватних прийнятій політиці безпеки інформації;
- методологія криптографічного аналізу та побудови оцінок криптографічної стійкості шифросистем, методи викриття механізмів

криптоперетворень, зокрема дешифрування;

- методи побудови криптографічних систем на основі обчислень над функціональними полями проективних різноманіть та оцінка їх стійкості;

- математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем і криптографічних протоколів;

- математичні та обчислювальні методи розрахунку надійності криптосистем, прогнозування оцінок криптографічної стійкості, вирішення задач криптографічного аналізу та синтезу шифросистем і криптографічних протоколів;

− методи забезпечення інформаційної безпеки в інфокомунікаційних системах;

- моделі та методи оцінки ризиків інформаційної безпеки;

− моделі та методи забезпечення інформаційної та мережної безпеки, розробка систем оцінки ризиків, пошуку вразливостей та виявлення атак в мережах;

− інформаційна безпека інфокомунікаційних і хмарних технологій;

− розслідування інцидентів порушень інформаційної безпеки, розробка пропозицій щодо мінімізації ризиків і загроз;

− аналіз інформаційної безпеки і прогнозування стану елементів мережі і сегмента мережі в цілому;

- методи та засоби автентифікації користувачів мережі.

7.2. Педагогічна практика

Педагогічна практика є невід’ємною складовою програми підготовки здобувачів і призначена для набуття компетентностей щодо здійснення освітнього процесу, навчання, розвитку і професійної підготовки студентів до певного виду професійно-орієнтованої діяльності.

Метою практики є формування та розвиток професійно-педагогічних компетентностей, знань, навичок та умінь викладача вищої школи з питань організації і форм здійснення освітнього процесу в сучасних умовах.

Педагогічна практика полягає в участі аспіранта у забезпеченні освітнього процесу кафедри та реалізується у вивченні досвіду викладацької діяльності провідних викладачів, роботі з вивчення дисциплін, проведенні занять, що відповідають науково-дослідній роботі здобувача та навчальним планам підготовки студентів першого та другого освітнього рівня вищої освіти, забезпеченні виробничої, професійної та науково-дослідної практик студентів, участі в розробці навчально-методичного забезпечення викладання дисциплін кафедр за спеціальністю 125 Кібербезпека.