МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-НАУКОВА ПРОГРАМА "КІБЕРБЕЗПЕКА"

РІВЕНЬ ВИЩОЇ ОСВІТИ	третій (ДОКТОР ФІЛОСОФІЇ) рівень (назва рівня вищої освіти)
СТУПІНЬ ВИЩОЇ ОСВІТИ	ДОКТОР ФІЛОСОФІЇ (назва ступеня вищої освіти)
ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології (шифр та назва галузі знань)
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека (код та найменування спеціальності)

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ
Голова вченої ради
_____ В.В. Семенець
Протокол № 5 від 10.04.2018

Освітня програма
вводиться в дію з __.__.2018
наказом від 10.04.2018 № 5
Ректор
_____ В.В. Семенець

Харків 2018 р.

ЛИСТ ПОГОДЖЕННЯ

Проректор з НМР І.В. Рубан

Розглянуто на засіданні Вченої Ради
факультету КІУ
протокол № 7 від 27.03.2018р.
декан факультету КІУ

О.С. Ляшенко

Розглянуто на засіданні кафедри БІТ
протокол № 10 від 21.03.2018р.
Завідувач кафедри БІТ

Г.З. Халімов

Розглянуто на засіданні Вченої Ради
факультету ІРТЗІ
протокол № 7 від 02.04.2018р.
декан факультету ІРТЗІ

С.М. Сакало

Розглянуто на засіданні кафедри КРіСТЗІ
протокол № 7 від 29.03.2018р.
Завідувач кафедри КРіСТЗІ

І.Є. Антіпов

Розглянуто на засіданні кафедри РТІКС
протокол № 8 від 30.03.2018р.
Завідувач кафедри РТІКС

О.І. Цопа

Розглянуто на засіданні Вченої Ради
факультету ІК
протокол № 5 від 26.03.2018р.
декан факультету ІК

А.В. Снігуров

Розглянуто на засіданні кафедри ІКІ
протокол № 7 від 22.03.2018р.
В.о. Завідувача кафедри ІКІ

О.В. Лемешко

Начальник відділу ЛА та ВСЗЯО Л.С. Осьмачко

Розроблено членами проектної групи з кібербезпеки та науково-педагогічними працівниками кафедр ХНУРЕ.

РОЗРОБНИКИ

(прізвище, ім’я, по батькові, науковий ступінь та вчене звання, посада)

Халімов Геннадій Зайдулович	д.т.н., проф., зав. каф. БІТ, керівник проектної групи
Заболотний Володимир Ілліч	к.т.н., доц., проф. каф. БІТ, відповідальний виконавець
Цопа Олександр Іванович	д.т.н., проф., зав. каф. РТІКС, член проектної групи
Руженцев Віктор Ігорович	д.т.н., доц., доц. каф. БІТ, член проектної групи
Олейніков Анатолій Миколайович	к.т.н., доц., проф. каф. КРіСТЗІ, член проектної групи
Снігуров Аркадій Владиславович	к.т.н., доц., доц. каф. ІКІ, декан факультету ІК
Свид Ірина Вікторівна	к.т.н., доц., доц. каф. РТІКС

Загальна характеристика

Освітньо-наукова програма (далі – ОНП) зі спеціальності 125 «Кібербезпека» створена в Харківському національному університеті радіоелектроніки (далі – ХНУРЕ) згідно вимог чинного законодавства України, спрямована на підготовку фахівців з вищою освітою за третім рівнем вищої освіти та передбачає набуття здобувачами теоретичних знань, умінь, навичок та інших компетентностей, достатніх для продукування нових ідей та здатності розв'язання комплексних наукових проблем у галузі інформаційних технологій.

На навчання для здобуття ступеня доктора філософії приймаються особи, які здобули ступінь магістра або освітньо-кваліфікаційний рівень спеціаліста за спеціальністю 125 «Кібербезпека» або за напрямом 1701 «Інформаційна безпека».

Для викладання дисциплін можливо використання дистанційних технологій.

Освітньо-наукова програма використовується під час:

– ліцензування та акредитації освітньо-наукової програми, інспектуванні освітньо-наукової діяльності за спеціальністю 125 «Кібербезпека»;

– розробки навчальних планів та формування індивідуальних планів здобувачів;

– формування програм навчальних дисциплін, практик, змісту індивідуальних завдань;

– розробки засобів діагностики системи внутрішнього забезпечення якості вищої освіти;

– визначення змісту навчання в системі перепідготовки та підвищення кваліфікації науково-педагогічних працівників;

– наукової орієнтації здобувачів ступеня докторів філософії;

– розробки Правил прийому до ХНУРЕ.

Користувачі освітньо-наукової програми:

– здобувачі ступеня доктора філосоії, які навчаються в ХНУРЕ;

– науково-педагогічні працівники ХНУРЕ, які здійснюють підготовку докторів філософії спеціальності 125 «Кібербезпека»;

– екзаменаційна комісія спеціальності 125 «Кібербезпека»";

– приймальна комісія ХНУРЕ.

Освітньо-наукова програма поширюється на кафедри ХНУРЕ, що здійснюють підготовку фахівців ступеня доктора філософії спеціальності 125 «Кібербезпека».

І. Профіль освітньої програми зі спеціальності № 125 "Кібербезпека"

1 ЗАГАЛЬНА ІНФОРМАЦІЯ

Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки. Кафедра Безпеки інформаційних технологій (БІТ) факультету комп'ютерної інженерії та управління (КІУ). Кафедра Комп'ютерної радіоінженерії та систем технічного захисту інформації (КРіСТЗІ), Кафедра радіотехнологій інформаційно-комуникаційних систем (РТІКС) факультету інформаційних радіотехнологій та технічного захисту інформації (ІРТЗІ). Кафедра Інфокомунікаційної інженерії (ІКІ) факультету інфокомунікацій (ІК)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	третій (освітньо-науковий) рівень доктор філософії з кібербезбеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії, одиничний, 40 кредитів ЄКТС освітньої складової освітньо-наукової програми, термін освітньої складової освітньо-наукової програми – 1 рік
Наявність акредитації	
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Наявність ступеня магістра або спеціаліста
Мова(и) викладання	Українська. За рішенням Вченої ради ХНУРЕ допускається викладання окремих дисциплін іноземною мовою
Термін дії освітньої програми	Програма впроваджується в 2018 році
Інтернет-адреса постійного розміщення опису освітньої програми	*https://uk.nure.info/universytet-xnure/specialnosti/66-specialnist-125-kiberbezpeka.html*

2 - Мета освітньої програми
Підготовка висококваліфікованих фахівців, які: володіють методами дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних з організацією, створенням методів і засобів забезпечення захисту інформації при її зберіганні, обробці та передачі з використанням сучасних математичних методів, інформаційних технологій і технічних засобів
3 – Характеристика освітньої програми

Предметна область (галузь знань, спеціальність)	12 Інформаційні технології, 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-наукова програма акцентована на розвиток здатності розв'язувати проводити наукові дослідження, вирішувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог, проведення педагогічної діяльності в ВНЗ за фахом.

Основний фокус освітньої програми та спеціалізації	Формування необхідних дослідницьких навиків для наукової кар'єри та викладання спеціальних дисциплін в галузі інформаційної та кібербезпеки Ключові слова: КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ, АНТІВІРУСНИЙ ЗАХИСТ, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ
Особливості програми	Наукова складова освітньо-наукової програми визначається індивідуальним навчальним планом підготовки доктора філософії.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 1210.1 Керівник підприємства (установи, організації) (сфера захисту інформації); 1226.2 Керівник структурного підрозділу (сфера захисту інформації); 1226.2 Начальник відділення (сфера захисту інформації); 1229.7 (99) Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної); 1495 Менеджер (управитель) систем з інформаційної безпеки. 2149.2 Професіонал із організації інформаційної безпеки. 2149.2 Професіонал із організації захисту інформації з обмеженим доступом. 2149.2 Фахівець (сфера захисту інформації). 2310 Викладачі університетів та вищих навчальних закладів. 2310.1 Докторант. 2310.1 Доцент.
Подальше навчання	Здобуття другого наукового ступеня (доктор наук). Післядипломна освіта здійснюється відповідно до чинних вимог в залежності від сфери діяльності.
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, самостійна науково-навчальна робота на основі науково-технічної навчальної літератури та публікацій у фахових періодичних виданнях, консультування із науковим керівником, науково-педагогічною спільнотою, проведення наукового дослідження, підготовка та захист дисертаційної роботи.
Оцінювання	Форми семестрового оцінювання: поточний контроль, екзамени, заліки. Підсумкова атестація здійснюється у формі публічного захисту дисертаційної роботи.
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики
Загальні компетентності (ЗК)	ЗК-1. Здатність спілкуватися другою (іноземною) мовою. ЗК-2. Здатність навчатися та самонавчатися. ЗК-3. Здатність до усного та письмового спілкування рідною мовою.

	ЗК-4. Здатність бути критичним та самокритичним. ЗК-5. Здатність генерувати нові ідеї (креативність). ЗК-6. Здатність знаходити, обробляти та аналізувати інформацію з різних джерел. ЗК-7. Здатність працювати автономно. ЗК-8. Здатність виявляти, ставити і вирішувати проблеми. ЗК-9. Здатність приймати обґрунтовані рішення. ЗК-10. Здатність проведення досліджень на відповідному рівні. ЗК-11. Знання і розуміння предметної області та розуміння професії. ЗК-12. Здатність до абстрактного та аналітичного мислення й генерування ідей. ЗК-13. Здатність оцінювати і підтримувати якість роботи. ЗК-14. Здатність використовувати інформаційні та комунікаційні технології.
Фахові компетентності спеціальності (ФК)	ФК-1. Здатність будувати та розвивати логічні аргументи обчислювального характеру з чітким визначенням припущень та висновків. ФК-2. Можливість здійснювати програмне моделювання ситуації з реального світу та трансформувати інформаційну експертизу, що не відображається в контексті інформаційних технологій. ФК-3. Можливість отримувати якісну інформацію з кількісних даних для проведення наукових експериментів. ФК-4. Можливість використовувати обчислювальні інструменти числових та символьних обчислень для постановки та вирішення проблем інформаційної та кібербезпеки. ФК-5. Здатність виконувати абстракцію досліджуваної наукової проблеми, включаючи логічний розвиток формальних теорій та відношень між ними. ФК-6. Здатність представляти числові аргументи та висновки з них з ясністю та точністю і в таких формах, що підходять для аудиторії як у вербальній, так і в письмовій формі. ФК-7. Здатність складати математичний опис задачі прийняття рішень як оптимізаційної задачі на основі змістовного опису, обирати метод її розв’язання, виходячи з її властивостей. ФК-8. Знання історичного розвитку інформаційних технологій та їх культурний вплив на розвиток науково-технічного мислення. ФК-9. Здатність та готовність вирішувати нові проблеми галузі інформаційної та кібербезпеки. ФК-10. Знання сучасних інформаційних технологій та програмного забезпечення для вирішення актуальних проблем інформаційної та кібербезпеки. ФК-11. Можливість планування та проведення експериментальних та спостережних досліджень, а також аналізу даних та обробки інформації; набуття практичних навичок використання програмних засобів інтелектуального аналізу даних, отриманих за результатами досліджень. ФК-12. Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї інформаційної та кібербезпеки. ФК-13. Здатність оцінювати ступінь обґрунтованості застосування специфікацій, стандартів, правил і рекомендацій в професійній галузі та дотримуватися їх при реалізації процесів життєвого циклу ззасобів і систем інформаційної та кібербезпеки. ФК-14. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної та кібербезпеки. ФК-15. Здатність застосовувати і розвивати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань засобів і систем

	інформаційної та кібербезпеки. ФК-16. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження засобів і систем інформаційної та кібербезпеки, визнання важливості навчання протягом всього життя. ФК-17. Дослідження складних міждисциплінарних проблем різної природи на основі системного аналізу, формалізація системних задач, що мають суперечливі цілі, невизначеності та ризики. ФК-18. Здатність продемонструвати знання і розуміння наукових та математичних принципів, що лежать в основі інформаційної та кібербезпеки. ФК-19. Здатність застосовувати отримані знання для аналізу інженерних об'єктів, процесів і методів. ФК-20. Здатність до пошуку та аналізу науково-технічної, природничо-наукової та загальнонаукової інформації ФК-21. Здатність продемонструвати розуміння методології проектування засобів і систем інформаційної та кібербезпеки. ФК-22. Здатність розуміти та застосовувати в дослідницькій та прикладної діяльності сучасний математичний апарат теорії оптимізації при розв'язанні задач інженерії програмного забезпечення. ФК-23. Здатність обирати моделі та методи, розробляти алгоритми розв'язання задач управління та проектування систем інформаційної та кібербезпеки. ФК-24. Здатність використовувати концепції, методи та теоретичні положення автоматизації складно формалізованих задач вибору рішень, методи прийняття рішень в антагоністичних та конфліктних ситуаціях, умовах ймовірнісної та нечіткої невизначеності.
7 - Програмні результати навчання	
Шифр	Зміст
Програмні результати навчання (ПР)	*Когнітивна сфера (знання з предметної області, уміння та навички)* ПР-1. На основі знань загальнонаукових методів вміти застосовувати методи емпіричного та теоретичного дослідження. Вивчаючи зміст прогностичної функції філософського знання визначати основні типи та методи прогнозування. ПР-2. Знати основні класи моделей і методів моделювання систем та принципи побудови моделей процесів функціонування засобів і систем інформаційної та кібербезпеки, методи їх формалізації та алгоритмізації. ПР-3. Знати можливості реалізації моделей із використанням сучасних програмно-технічних засобів. ПР-4. Застосовувати методологію наукової діяльності, організовувати дослідницьку діяльність, структурувати вміст наукових праць та правильно подавати результати досліджень. ПР-5. Уміти використовувати математичні і програмні засоби системного моделювання засобів і систем інформаційної та кібербезпеки та розробляти схеми моделювальних алгоритмів. ПР-6. Уміти проводити планування машинних експериментів, дослідження, обробку та аналіз результатів моделювання засобів і систем інформаційної та кібербезпеки з використанням сучасних програмних і технічних засобів. ПР-7. Уміти виконувати дослідження та проектування засобів і систем інформаційної та кібербезпеки. ПР-8. Знати основні класи сучасних методів аналізу даних, зокрема інтелектуального аналізу, та принципи пошуку неявних закономірностей та практично корисних і доступних інтерпретації знань необхідних для

	прийняття рішень. ПР-9. Знати методи побудови моделей та аналізу залежностей у великих масивах даних та критерії порівняння моделей і методів сучасного аналізу даних ПР-10. Знати основні сучасні програмні засоби інтелектуального аналізу даних, їх порівняльні переваги і недоліки. ПР-11. Уміти обґрунтовувати й аналізувати вибір конкретного типу моделі та методу аналізу даних при вирішенні відповідних практичних задач. ПР-12. Уміти використовувати сучасні математичні і програмні засоби для досліджень та інтелектуального аналізу даних. ПР-13. Уміти інтерпретувати результати аналізу даних при вирішенні практичних задач та формалізувати їх з метою прийняття рішень. ПР-14. Уміти розвивати нові та удосконалювати існуючі методи математичного та чисельного моделювання засобів і систем інформаційної та кібербезпеки. ПР-15. Уміти конструювати програмні архітектури, які суттєво відрізняються від типових рішень та враховують актуальні тренди у галузі розробки засобів і систем інформаційної та кібербезпеки та актуальні технології розробки. ПР-16. Уміти розвивати нові та удосконалювати існуючі засобів і систем інформаційної та кібербезпеки. ПР-17. Уміти виконувати дослідження властивостей засобів і систем інформаційної та кібербезпеки та проектувати додаткові компоненти на етапі супроводу. ПР-18. Уміти обирати відповідний (найкращий за якимось критерієм) метод розв'язання задачі. ПР-19. Знати особливості філософсько-світоглядних засад, сучасних тенденцій, напрямків і закономірностей розвитку вітчизняної науки в умовах глобалізації й інтернаціоналізації. *Ціннісно-мотиваційна сфера* ПР-20. Виявляти здатність до самонавчання та продовження професійного розвитку. ПР-21. Здатність написати наукову статтю (доповідь) на державній та/або іноземній мові з використанням наукової та навчальної літератури, довідників, словників, документів та іншої науково-технічної інформації, з дотриманням норм авторського права. ПР-22. Ефективно спілкуватися з питань інформаційної та кібербезпеки, ідей, проблем та рішень зі спеціалістами та суспільством загалом. ПР-23. Демонструвати навички професійного спілкування, включаючи усну та письмову комунікацію українською мовою та принаймні ще однією з поширених європейських мов. ПР-24. Здатність виконувати навчальну та методичну роботу зі своєї навчальної дисципліни, керуючись нормативними документами та психолого-педагогічними вимогами до навчального процесу. ПР-25. Оформляти результати досліджень у вигляді наукових звітів, доповідей, презентацій та статей.
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Згідно ліцензійних умов для кадрового забезпечення підготовки магістрів: - наявність у складі підрозділу чи кафедри, відповідальних за підготовку здобувачів вищої освіти, тимчасової робочої групи (проектної групи) з науково-педагогічних працівників, на яку покладено відповідальність за підготовку здобувачів вищої освіти за спеціальністю трьох осіб, що мають

	науковий ступінь та вчене звання, з них не менше двох докторів наук; - наявність у керівника проектної групи (гаранта освітньої програми): наукового ступеня та вченого звання за відповідною або спорідненою спеціальністю та - стажу науково-педагогічної та/або наукової роботи не менш як 10 років.
Матеріально-технічне забезпечення	Засоби обчислювальної техніки з відповідним програмним забезпеченням, спеціальні радіовимірювальні прилади, засоби ТЗІ, апаратно-програмні комплекси.
Інформаційне та навчально-методичне забезпечення	Сайт ХНУРЕ http://nure.ua/ Сайт наукової бібліотеки ХНУРЕ http://lib.nure.ua Електронний архів відкритого доступу Харківського національного університету радіоелектроніки http://openarchive.nure.ua/ Наукова бібліотека ХНУРЕ та фонд кафедри програмної інженерії 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 вищими навчальними закладами зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів між Харківським національним університетом радіоелектроніки і вищими навчальними закладами країн-партнерів.

2. Перелік компонент освітньо-наукової програми та їх логічна послідовність викладена у навчальному плані підготовки доктора філософії

2.1 Перелік компонент освітньо-наукової програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
Обов'язкові компоненти ОП			
1. ОСВІТНЯ СКЛАДОВА. ОБОВ'ЯЗКОВІ (НОРМАТИВНІ) НАВЧАЛЬНІ ДИСЦИПЛІНИ			
Цикл 1.1. Дисципліни гуманітарної та соціально-економічної підготовки			
ОК 1.1.	Іноземна мова як мова наукової комунікації	6	залік
ОК 1.2.	Філософія та методологія сучасної науки. Проблеми формування критичного мислення	3	залік
ОК 1.3.	Психолого-педагогічні основи науково-педагогічної діяльності	2	залік
ОК 1.4.	Особливості наукової української мови	3	залік
Цикл 1.2. Дисципліни природничо-наукової (фундаментальної) підготовки			
ОК 2.1.	Математичне моделювання процесів та систем	6	залік
ОК 2.2.	Сучасні методи аналізу даних	6	залік
Цикл 1.3. Дисципліни професійної та практичної підготовки			
ОК 3.1.	Методологія наукових досліджень	4	залік
Загальний обсяг обов'язкових компонент:		30	

Вибіркові компоненти ОП			
2. ОСВІТНЯ СКЛАДОВА. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ			
Цикл 2.1 Дисципліни професійної та практичної підготовки			
ВБ 1.1.	Згідно навчального плану підготовки доктора філософії на відповідний навчальний період	10	залік
ВБ 1.2.	Згідно навчального плану підготовки доктора філософії на відповідний навчальний період	10	залік
Загальний обсяг вибіркових компонент:		10	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		40	

2.1. Структурно-логічна схема ОП

1 семестр	2 семестр
ОК 1.1. ОК 1.2. ОК 2.1. ОК 3.1. ВБ 1.1., ВБ 1.2.	ОК 1.1. ОК 1.3. ОК 1.4. ОК 2.2. ВБ 1.1., ВБ 1.2.

3. Форма атестації здобувачів вищої освіти

Атестація здійснюється спеціалізованою вченою радою, (зокрема К 64.052.05 у ХНУРЕ) за спеціальністю 05.13.21 – системи захисту інформації, після представлення і захисту дисертаційної роботи (опублікованої монографії) та завершується видачею диплома встановленого зразка.

Дисертаційна робота має відповідати вимогам, передбаченими постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 про Порядок присудження наукових ступенів.

Дисертація на здобуття наукового ступеня є кваліфікаційною науковою працею, виконаною особисто здобувачем у вигляді спеціально підготовленого рукопису або опублікованої монографії. Підготовлена до захисту дисертація повинна містити висунуті здобувачем науково обґрунтовані теоретичні або експериментальні результати, наукові положення, а також характеризуватися єдністю змісту і свідчити про особистий внесок здобувача в науку.

До дисертації, що містить науково-прикладні результати, повинні додаватися документи, що підтверджують практичне використання отриманих здобувачем результатів - впровадження у виробництво, достатню дослідно-виробничу перевірку, отримання нових кількісних і якісних показників, суттєві переваги запропонованих технологій, зразків продукції, матеріалів тощо, а до дисертації, що містить теоретичні наукові результати, - рекомендації щодо їх використання.

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.

Прилюдний захист дисертації проводиться на засіданні спеціалізованої вченої ради, яке вважається правоможним у разі, коли в його проведенні взяло участь не менш як дві третини складу, а також не менш три доктори наук із спеціальності кандидатської дисертації. Рішення спеціалізованої вченої ради про присудження наукового ступеня вважається позитивним, якщо за нього проголосувало не менш як три чверті членів ради, які брали участь у засіданні.

2.1. Вимоги до кваліфікаційної роботи

Наукова складова освітньо-наукової програми передбачає проведення власного розгорнутого наукового дослідження, результати якого мають наукову новизну, теоретичне та практичне значення, під керівництвом одного або двох наукових керівників та оформлення його результатів у вигляді дисертації. Результати досліджень повинні оприлюднюватись у публікаціях, проходити апробацію на наукових семінарах та конференціях.

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

Стан готовності дисертації аспіранта (ад'юнкта) до захисту визначається науковим керівником (або консенсусним рішенням двох керівників).

За всі відомості, викладені в дисертації, порядок використання фактичного матеріалу та іншої інформації під час її написання, обґрунтованість висновків та положень, які в ній захищаються, несе відповідальність безпосередньо аспірант (ад'юнкта) – автор дисертації.

Оформлення дисертації має відповідати діючим вимогам.

Експертна комісія установи, де виконувалась дисертація, вивчає питання про наявність або відсутність у ній текстових запозичень, використання ідей, наукових результатів і матеріалів інших авторів без посилання на джерело.

Робота, автореферат та відзиви офіційних опонентів має бути оприлюднена(-ні) згідно з вимогами ВНЗ в електронному інформаційному просторі на сайті вченої ради.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 2.1	ОК 2.2	ОК 3.1	ВБ 1.1	ВБ 1.2
ЗК 1	+								
ЗК 2		+	+				+		
ЗК 3				+					
ЗК 4		+	+						
ЗК 5		+	+				+	+	
ЗК 6	+			+			+		+
ЗК 7		+					+		
ЗК 8		+	+				+	+	+
ЗК 9		+					+	+	+
ЗК 10					+		+	+	+
ЗК 11					+	+		+	+
ЗК 12		+			+	+	+		
ЗК 13							+	+	+
ЗК 14			+		+	+		+	+
ФК 1		+			+	+			
ФК 2		+			+	+	+		+
ФК 3		+			+		+		

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 2.1	ОК 2.2	ОК 3.1	ВБ 1.1	ВБ 1.2
ФК 4					+	+		+	
ФК 5		+			+		+		
ФК 6					+	+	+		
ФК 7		+			+	+	+		
ФК 8		+			+	+	+		
ФК 9		+			+	+	+	+	+
ФК 10		+			+	+	+	+	+
ФК 11		+			+	+			
ФК 12					+	+	+	+	+
ФК 13					+	+	+	+	
ФК 14		+	+				+	+	
ФК 15	+	+	+		+	+	+	+	+
ФК 16					+	+	+	+	
ФК 17	+	+	+		+	+	+	+	+
ФК 18					+	+	+	+	+
ФК 19								+	+
ФК 20	+	+	+		+	+	+		
ФК 21					+	+	+	+	+
ФК 22					+	+			
ФК 23					+	+	+	+	+
ФК 24		+			+	+	+	+	+

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

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 2.1	ОК 2.2	ОК 3.1	ВБ 1.1	ВБ 1.2
ПРН 1		+			+				
ПРН 2					+				
ПРН 3					+				
ПРН 4					+	+			
ПРН 5						+			
ПРН 6						+			
ПРН 7						+			
ПРН 8						+			
ПРН 9						+			
ПРН 10						+			

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 2.1	ОК 2.2	ОК 3.1	ВБ 1.1	ВБ 1.2
ПРН 11						+			
ПРН 12						+			
ПРН 13						+			
ПРН 14						+			
ПРН 15						+			
ПРН 16						+			
ПРН 17						+			
ПРН 18						+			
ПРН 19	+								
ПРН 20		+	+						
ПРН 21	+			+					
ПРН 22	+			+			+		
ПРН 23	+			+	+	+	+	+	+
ПРН 24			+				+		
ПРН 25			+		+	+	+		

6. Наукова (дослідницька) компонента ОНП

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

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 і оприлюднені у відповідних публікаціях.

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

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, КРіСТЗІ, РТІКС та ІКІ ХНУРЕ та спрямована на формування компетенцій проведення наукових досліджень у галузі інформаційної та кібербезпеки.

Основні напрямки досліджень (згідно паспорту спеціальності 05.13.21 - системи захисту інформації):

- 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;
- організація, архітектура, методологія проектування, технологія функціонування КСЗІ;
- шифри, шифросистеми, 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;
- 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;
- технічні канали витоку інформації та їх моделі, нові технології та засоби захисту інформації від витоку технічними каналами;
- моделювання процесів атак на інформацію та її захисту;
- методи та засоби вимірювання й обчислення параметрів небезпечних сигналів.

Гарант освітньо-наукової програми,
керівник проектної групи
д.т.н. професор Г.З. Халімов