МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО – НАУКОВА ПРОГРАМА

«Кібербезпека»

третього освітньо–наукового рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Доктор філософії, Кібербезпека

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол від "21" 02 2020 р. № 2)

Освітня програма вводиться в дію з ____2020 р.

Ректор_____ / В.В. Семенець /

(наказ від "27" 02 2020 р. № 117)

Харків 2020 р.

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

УЗГОДЖЕНО

Перший проректор
_____ (підпис) І.В. Рубан
«___» _____ 20__ р.

Начальник навчального відділу
_____ (підпис) А.В. Міхнова
«25» 02 2020 р.

Начальник відділу ЛА та ВСЗЯО
_____ (підпис) Ю.Б. Корнілова
«25» 02 2020 р.

Завідувач відділу аспірантури та докторантури
_____ (підпис) В.П. Манаков
«25» 02 2020 р.

Розглянуто на засіданні
Вченої Ради факультету КІУ
Протокол № 7 від 20.02.2020 р.
Декан факультету КІУ
_____ О.С. Ляшенко

Розглянуто на засіданні
кафедри БІТ
Протокол № 6 від 20.01.2020 р.
Завідувач кафедри БІТ
_____ Г.З. Халімов

Розглянуто на засіданні
Вченої Ради факультету ІРТЗІ
протокол № 2 від 10.02.2020 р.
декан факультету ІРТЗІ
_____ С.М. Сакало

Розглянуто на засіданні
кафедри РТІКС
Протокол № 8 від 20.01.2020 р.
Завідувач кафедри РТІКС
_____ О.І. Цопа

Розглянуто на засіданні
кафедри КРіСТЗІ
Протокол № 6 від 20.01.2020 р.
Завідувач кафедри КРіСТЗІ
_____ І.Є. Антіпов

Розглянуто на засіданні
Вченої Ради факультету ІК
Протокол № 4 від 10.02.2020 р.
Декан факультету ІК
_____ А.В. Снігуров

Розглянуто на засіданні
кафедри ІКІ ім. В.В. Поповського
Протокол № 6 від 29.01.2020 р.
Завідувач кафедри ІКІ
ім. В.В. Поповського
_____ О.В. Лемешко

Представники роботодавців

Приватне акціонерне товариство «Інститут інформаційних технологій»
Технічний директор АТ «ІІТ» _____ О.І. Шумов
(підпис) (ІБП)

Товариство з обмеженою відповідальністю «НВК Автоматизовані системи
Директор _____ А.І. Роговий
(підпис) (ІБП)

Товариство з обмеженою відповідальністю «МНС ГРУП»
Генеральний директор _____ Г.В.Мазур
(підпис) (ІБП)

Представники студентського самоврядування

Голова Ради молодих вчених
Наукового товариства молодих учених _____ О.С. Єременко
(підпис) (ІБП)

РОЗРОБЛЕНО

Проєктна група:

керівник проєктної групи:
Халімов Г.З., д.т.н.,
професор, завідувач кафедри БІТ ХНУРЕ _____ Г.З. Халімов

члени проєктної групи:
Цопа О.І., д.т.н.,
професор, завідувач кафедри РТІКС ХНУРЕ _____ О.І. Цопа

Олейніков А.М., к.т.н.,
професор, професор кафедри КРіСТЗІ ХНУРЕ _____ А.М. Олейніков

Руженцев В.І., д.т.н.,
доцент, професор кафедри БІТ ХНУРЕ _____ В.І. Руженцев

ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Освітньо-наукова програма (далі – ОНП) «Кібербезпека» 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 (освітньо-науковим) 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.

Для викладання дисциплін можливо використання дистанційних технологій.

Освітньо-наукова програма використовується під час:

– 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.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Халімов Геннадій Зайдулович (керівник проєктної групи)	– д.т.н., професор, завідувач кафедри БІТ Харківського національного університету радіоелектроніки
2. Заболотний Володимир Ілліч	- к.т.н., доцент, професор кафедри БІТ Харківського національного університету радіоелектроніки
3. Сєвєрінов Олександр Васильович	- к.т.н., доцент, доцент кафедри БІТ Харківського національного університету радіоелектроніки
4. Лемешко Олександр Віталійович	- д.т.н., професор, завідувач кафедри ІКІ ім. В.В. Поповського Харківського національного університету радіоелектроніки
5. Антіпов Іван Євгенійович	– д.т.н., професор, завідувач кафедри КРіСТЗІ Харківського національного університету радіоелектроніки
6. Цопа Олександр Іванович	– д.т.н., професор, завідувач кафедри РТІКС Харківського національного університету радіоелектроніки

1. Профіль освітньої програми «Кібербезпека» зі спеціальності 125 Кібербезпека

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). Кафедра інфокомунікаційної інженерії ім. В.В. Поповського (ІКІ) Кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації (КРіСТЗІ) Кафедра радіотехнологій інформаційно-комунікаційних систем (РТІКС)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії Доктор філософії, Кібербезпека
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії, одиничний, 30 кредитів ЄКТС освітньої складової освітньо-наукової програми, термін освітньої складової освітньо-наукової програми – 1 рік
Наявність акредитації	
Цикл/рівень	НРК України – 9 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	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 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 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 безпеки 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, 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. Знання історичного розвитку інформаційних технологій та їх культурний вплив на розвиток науково-технічного мислення. ФК-8. Здатність та готовність вирішувати нові проблеми галузі інформаційної та кібербезпеки. ФК-9. Знання сучасних інформаційних технологій та програмного забезпечення для вирішення актуальних проблем інформаційної та кібербезпеки. ФК-10. 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-11. Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї інформаційної та кібербезпеки. ФК-12. 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-13. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної та кібербезпеки. ФК-14. Здатність застосовувати і розвивати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань засобів і систем інформаційної та кібербезпеки. ФК-15. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження засобів і систем

	інформаційної та кібербезпеки, визнання важливості навчання протягом всього життя. ФК-16. Дослідження складних міждисциплінарних проблем різної природи на основі системного аналізу, формалізація системних задач, що мають суперечливі цілі, невизначеності та ризики. ФК-17. Здатність продемонструвати знання і розуміння наукових та математичних принципів, що лежать в основі інформаційної та кібербезпеки. ФК-18. Здатність застосовувати отримані знання для аналізу інженерних об'єктів, процесів і методів. ФК-19. Здатність до пошуку та аналізу науково-технічної, природничо-наукової та загальнонаукової інформації ФК-20. Здатність продемонструвати розуміння методології проектування засобів і систем інформаційної та кібербезпеки.
7 - Програмні результати навчання	
Програмні результати навчання (ПРН)	***Когнітивна сфера (знання з предметної області, уміння та навички)*** ПРН-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. ПРН-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. ПРН-3. Знати можливості реалізації моделей із використанням сучасних програмно-технічних засобів. ПРН-4. Застосовувати методологію наукової діяльності, організовувати дослідницьку діяльність, структурувати вміст наукових праць та правильно подавати результати досліджень. ПРН-5. Уміти використовувати математичні і програмні засоби системного моделювання засобів і систем інформаційної та кібербезпеки та розробляти схеми моделювальних алгоритмів. ПРН-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. ПРН-7. Уміти виконувати дослідження та проектування засобів і систем інформаційної та кібербезпеки. ПРН-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. ПРН-9. Знати методи побудови моделей та аналізу залежностей у великих масивах даних та критерії порівняння моделей і методів сучасного аналізу даних ПРН-10. Знати основні сучасні програмні засоби інтелектуального аналізу даних, їх порівняльні переваги і недоліки. ПРН-11. Уміти обґрунтовувати й аналізувати вибір конкретного типу моделі та методу аналізу даних при вирішенні відповідних практичних задач. ПРН-12. Уміти використовувати сучасні математичні і програмні

	засоби для досліджень та інтелектуального аналізу даних. ПРН-13. Уміти інтерпретувати результати аналізу даних при вирішенні практичних задач та формалізувати їх з метою прийняття рішень. ПРН-14. Уміти розвивати нові та удосконалювати існуючі методи математичного та чисельного моделювання засобів і систем інформаційної та кібербезпеки. ПРН-15. Уміти розвивати нові та удосконалювати існуючі засоби і системи інформаційної та кібербезпеки. ПРН-16. Уміти виконувати дослідження властивостей засобів і систем інформаційної та кібербезпеки та проектувати додаткові компоненти на етапі супроводу. ПРН-17. Уміти обирати відповідний (найкращий за якимось критерієм) метод розв'язання задачі. ПРН-18. Знати особливості філософсько-світоглядних засад, сучасних тенденцій, напрямків і закономірностей розвитку вітчизняної науки в умовах глобалізації й інтернаціоналізації. ***Ціннісно-мотиваційна сфера*** ПРН-19. Виявляти здатність до самонавчання та продовження професійного розвитку. ПРН-20. 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. ПРН-21. Ефективно спілкуватися з питань інформаційної та кібербезпеки, ідей, проблем та рішень зі спеціалістами та суспільством загалом. ПРН-22. Демонструвати навички професійного спілкування, включаючи усну та письмову комунікацію українською мовою та принаймні ще однією з поширених європейських мов. ПРН-23. Здатність виконувати навчальну та методичну роботу зі своєї навчальної дисципліни, керуючись нормативними документами та психолого-педагогічними вимогами до навчального процесу. ПРН-24. Оформляти результати досліджень у вигляді наукових звітів, доповідей, презентацій та статей.
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної, управлінської та інноваційної роботи за фахом. Викладачі є авторами навчальних посібників, монографій та статей, учасниками вітчизняних та міжнародних наукових конференцій.
Матеріально-технічне забезпечення	Навчальний процес відбувається у аудиторіях та лабораторіях, обладнаних сучасними комп'ютерними та технічними засобами, в тому числі мультимедійними, та спеціалізованим програмним забезпеченням.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 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). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання.
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

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
1. ОСВІТНЯ СКЛАДОВА			
Цикл 1. Соціально-гуманітарні дисципліни			
ОК 1.1.	Іноземна мова як мова наукової комунікації	5	залік
ОК 1.2.	Філософія та методологія сучасної науки, проблеми формування критичного мислення	2	залік
ОК 1.3.	Психолого-педагогічні основи науково-педагогічної діяльності	2	залік
ОК 1.4.	Особливості сучасної наукової комунікації	2	залік
Загальний обсяг		**11**	
Цикл 2. Дисципліни науково-професійної та практичної підготовки			
ОК 2.1.	Сучасні методи аналізу даних	3	залік
ОК 2.2.	Методологія наукових досліджень	3	залік
Загальний обсяг		**6**	
Цикл 1.3. Дисципліни за спеціальністю (вибіркові)			
ВБ 1.1.	Математичне моделювання процесів та систем	5	залік
ВБ 1.2.	Сучасні інформаційні технології	5	залік
ВБ 1.3.	Методи побудови криптосистем стійких до квантових обчислень	4	залік
ВБ 1.4.	Методи побудови криптосистем на групах	4	залік
ВБ 1.5.	Технічний захист інформації в каналах зв’язку	4	залік
ВБ 1.6.	Фізичні поля об'єктів технічного захисту інформації	4	залік
ВБ 1.7.	Сучасні методи захисту інформації на фізичному рівні інформаційно-комунікаційних систем	8	залік
ВБ 1.8.	Новітні технології забезпечення мережної безпеки в інфокомунікаціях	8	залік
Загальний обсяг		**13**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**30**	

2.1. Структурно-логічна схема ОП

1 семестр	2 семестр
ОК 1.1.	ОК 1.1.
ОК 1.2.	ОК 1.3.
ОК 2.1.	ОК 1.4.
ОК 2.2.	ВБ 1.1., ВБ 1.2.
ВБ 1.3., ВБ 1.5., ВБ 1.7., ВБ 1.8	ВБ 1.4., ВБ 1.6., ВБ 1.7., ВБ 1.8.

3. Форма атестації здобувачів вищої освіти

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.

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.

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	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 1.6	ВБ 1.7	ВБ 1.8
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					+	+	+		+					+
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						+			+				+	+

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

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 2.1	ОК 2.2	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 1.6	ВБ 1.7	ВБ 1.8
ПРН-1		+				+	+							
ПРН-2				+			+							
ПРН-3					+	+	+							
ПРН-4			+			+								
ПРН-5					+		+							
ПРН-6						+	+							
ПРН-7						+	+	+	+	+			+	+
ПРН-8					+									
ПРН-9					+		+							
ПРН-10					+									
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	+		+	+		+		+						

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:

- 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 захист;

- методи та засоби вимірювання й обчислення параметрів небезпечних сигналів;
- моделі та методи забезпечення мережної безпеки;
- методи та засоби автентифікації користувачів мережі;
- методи виявлення та протидії атакам в мережах;
- моделі та методи оцінки ризиків інформаційної безпеки.