КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

«ЗАТВЕРДЖЕНО»
Рішенням Вченої ради Київського
університету імені Бориса Грінченка
24 січня 2019 р., протокол № 1

Голова Вченої ради, ректор
Огнєв'юк Віктор Олександрович

ОСВІТНЬО-НАУКОВА ПРОГРАМА
«Інформаційна безпека держави»
третього (освітньо-наукового) рівня вищої освіти

Галузь знань:	12 Інформаційні технології
Спеціальність:	125 Кібербезпека
Кваліфікація:	доктор філософії з кібербезпеки

Введено в дію з «01» вересня 2019 р.
(наказ від 29.01.2019 р., № 37)

Київ – 2019

ЛИСТ ПОГОДЖЕННЯ
освітньо-наукової програми

Кафедра інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка
Протокол № 1 від "16" січня 2019 р.
Завідувач кафедри _____ В.Л.Бурячок

Вчена рада Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка
Протокол № 1 від "23" січня 2019 р.
Голова Вченої ради _____ А.В. Михацька

Завідувач аспірантури, докторантури
_____ О.В.Плющик
24.01.2019 р.

Проректор з наукової роботи
_____ Н.М. Віннікова
24.01.2019 р.

ПЕРЕДМОВА

Розроблено на основі Закону України від 01.07.2015 №1556-VII «Про вищу освіту» з урахуванням вимог проекту Стандарту вищої освіти з підготовки докторів філософії спеціальності 125 Кібербезпека робочою групою у складі:

Керівник робочої групи:
БУРЯЧОК Володимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка

Члени робочої групи:
БЕССАЛОВ Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка

СЕМКО Віктор Володимирович, доктор технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка

АНОСОВ Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка

Рецензенти:
1. ТОЛЮПА Сергій Васильович, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Т.Г.Шевченка, м. Київ

2. ЄРМОШИН Валерій Віталійович, кандидат технічних наук, директор Департаменту з інформаційної безпеки ДП «НЕК «Укренерго», м. Київ

Актуалізовано:

Дата перегляду ОНП/ внесення змін до ОНП			
Підпис			
ПІБ гаранта ОНП			

1. Профіль освітньо-наукової програми «Інформаційна безпека держави» зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський університет імені Бориса Грінченка Факультет інформаційних технологій та управління
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	доктор філософії, доктор філософії з кібернетичної безпеки
Офіційна назва освітньої-наукової програми	«Інформаційна безпека держави»
Тип диплому та обсяг освітньо-наукової програми	Диплом доктор філософії, одиничний, 60 кредитів ЄКТС (освітня складова – 60 кредитів). Термін навчання 4 роки
Наявність акредитації	Національне агентство забезпечення якості вищої освіти, Україна Термін подання програми на акредитацію – 2023 р.
Цикл/рівень	третій (освітньо-науковий) рівень FQ-EHEA – третій цикл, QF LLL – 8 рівень, НРК – 9 рівень
Передумови	Наявність ступеня магістра або освітньо-кваліфікаційного рівня спеціаліста
Мова(и) викладання	Українська
Інтернет-адреса постійного розміщення опису освітньої-наукової програми	http://kubg.edu.ua/
2 – Мета освітньо-наукової програми	
Забезпечити аспірантам фундаментальну теоретичну і практичну підготовку для організації захисту інформації, інформаційної та/або кібербезпеки на об'єктах інформаційної діяльності (ОІД), достатню для продукування нових ідей, розв'язання комплексних проблем у галузі професійної та/або дослідницько-інноваційної діяльності, оволодіння методологією наукової та педагогічної діяльності, а також проведення власного наукового дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.	
3 - Характеристика освітньо-наукової програми	
Предметна область	*Об'єкти професійної діяльності випускників:* – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. *Цілі навчання:* підготовка науковців, здатних 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 з питань інформаційної та/або кібербезпеки. *Теоретичний зміст предметної області.* Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення

	професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до ІР; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно комунікаційних технологій; – автоматизованих систем проектування. *Методи, методики та технології:* методи, методики та технології забезпечення інформаційної та/або кібербезпеки. *Інструменти та обладнання:* системи розробки, забезпечення, моніторингу та контролю інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інфокомунікаційних технологій. *Співвідношення обсягів загальної і професійної складових та вибіркової частини:* Обов'язкова частина – 41 кредит, 68%: дисципліни, спрямовані на формування загальних компетентностей – 20 кредитів, 33%; дисципліни, спрямовані на формування фахових компетентностей – 15 кредитів, 25%; практики (науково-викладацька, дослідницька) – 6 кредитів, 10%. Вибіркова частина – 19 кредитів (32%).
Орієнтація освітньої-наукової програми	Освітньо-наукова програма з прикладною спрямованістю на фундаментальні наукові дослідження в сфері захисту інформації, забезпечення безпеки інформаційних і комунікаційних систем, а також організації й забезпечення інформаційної та/або кібербезпеки об'єктів інформаційної діяльності, що підлягають захисту.
Основний фокус освітньої-наукової програми	Дослідження в області практики та науки захисту інформації, організації і забезпечення інформаційної та/або кібербезпеки об'єктів інформаційної діяльності, що підлягають захисту.
Особливості програми	З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання аспірантами освітньої кваліфікації доктор філософії з кібербезпеки, програма забезпечує підготовку професіоналів, здатних: – виявляти та оцінювати ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки; – організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізуємості та економічної доцільності, можливих внутрішніх і зовнішніх впливів, імовірних загроз та рівня розвитку технологій захисту інформації; – проводити дослідження у напрямах забезпечення інформаційної та/або кібербезпеки національних інтересів України й обґрунтовувати шляхи підвищення їх ефективності; – протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення

	кібернападів; – забезпечити криптозахист власного інформаційного ресурсу тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: – реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; – залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах ІТ-компаній Києва, України та Європейського Союзу у таких сферах діяльності: 1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 2) застосування засобів антивірусного захисту (ESET, McAfee, Zilly, etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3) створення технічної, проектної та експлуатаційної документації ІКС та систем захисту інформації (далі – СЗІ); 4) налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5) проведення моніторингу несанкціонованої активності в обчислювальних системах; 6) створення, впровадження та експлуатації КСЗІ, а також СЗІ в складі ІТС та обчислювальних систем; 7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками ІБ; 8) проведення розслідувань інцидентів та забезпечення аудиту процесів ІБ; 9) підтримка наукових досліджень, педагогічна діяльність тощо. Згідно з Національним класифікатором професій ДК 003:2010 фахівці, які здобули освіту за ОНП «Інформаційна безпека держави» можуть обіймати такі первинні посади, як: молодший науковий співробітник; науковий співробітник; науковий співробітник-консультант; директор технічний; (1210.1) керівник (директор, начальник та ін.) департаменту; (1231) начальник відділу; (1229.7) начальник (завідувач) підрозділу; (1229.1) начальник лабораторії науково-дослідної, дослідної та ін.; (1237.2) аналітик проекту; (1231) викладач вищих навчальних закладів тощо.
Подальше навчання	Докторантура за спеціальністю 125 Кібербезпека або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом

	доктора філософії.	
5 – Викладання та оцінювання		
Викладання та навчання	*Стиль навчання*: – поєднання репродуктивного та творчого стилів навчання як взаємодоповнюючих з домінуючим творчим компонентом; – емоційно-ціннісний стиль навчання з поєднанням емоційно-імпровізаційного та емоційно-методичного стилів; – проблемно-орієнтовані лекційні курси, семінари, групові та індивідуальні консультації, самопідготовка у бібліотеці та мережі Інтернет. *Методика навчання*: – узгодження декількох навчальних технологій - інформаційної, моделюючої, розвивальної та активізуючої технологій, технології виробничого, випереджаючого та дистанційного навчання; – інтерактивне співробітництво з науковим керівником, колегами із наукової групи та науково-педагогічними працівниками університету. *Організація навчального процесу*: – формування і дотримання дослідницького портфоліо.	
Оцінювання	Формувальне оцінювання, яке передбачає врахування динаміки освітніх та наукових досягнень здобувачів за усіма видами аудиторної та позааудиторної освітньої діяльності у вигляді проміжного та/або підсумкового (семестрового) контролю (іспити, заліки), захист звітів з усіх видів практик.	
6 – Програмні компетентності		
Інтегральна компетентність	Здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації до вимог зовнішнього середовищ, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сферах тощо.	
Загальні компетентності (ЗК)	**ЗК-1**	Здатність до оволодіння різними комунікаційними стилями спілкування (неофіційним, офіційним та науковим) державною та іноземною мовами
	ЗК-2	Здатність до накопичення нових професійно профільованих знань і практичних навичок та застосування їх в професійній діяльності
	ЗК-3	Здатність до виявлення проблемних аспектів у галузі забезпечення інформаційної та/або кібербезпеки, їх аналізу, оцінювання та вирішення
	ЗК-4	Здатність до синтезу нових ідей, проведення наукових досліджень та реалізації технічних розробок за професійним спрямуванням на відповідному рівні
Фахові компетентності спеціальності (ФК)	**ФК-1**	Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів
	ФК-2	Здатність застосовувати математичні навички, навички системного аналізу та синтезу для вирішення нагальних проблем в системах інформаційної та/або кібербезпеки і захисту інформації
	ФК-3	Здатність застосовувати сучасні IT технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації

	ФК-4	Здатність проектувати, впроваджувати і застосовувати сучасні інформаційні та безпекові технології (комплексні системи криптографічного і технічного захисту інформації, системи соціотехнічної безпеки тощо)
	ФК-5	Здатність робити оцінки та в умовах припущень і обмежень знаходити відповідні рішення щодо систем інформаційної та/або кібербезпеки і захисту інформації
	ФК-6	Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації
	ФК-7	Здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов різних класів і походження.
7 – Програмні результати навчання		
Знання та розуміння	**ПРН-1**	– застосовувати знання державної та іноземних мов для забезпечення ефективності професійної комунікації;
	ПРН-2	– здійснювати інформаційний пошук; – аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки; – реалізовувати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, застосовуючи їх як в побуті, так і в професійній діяльності;
	ПРН-3	– виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією;
	ПРН-4	– забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; – здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; – проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; – обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; – використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів;
	ПРН-5	– розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних; – аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС; – проектувати та реалізувати комплексні системи КТЗІ в

		ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації; – вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань; – забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;
	ПРН-6	– розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки; – розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки; – здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування; – забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ; – забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф;
	ПРН-7	– вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; – володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.
8 – Ресурсне забезпечення реалізації програми		
Кадрове забезпечення		Кадрове забезпечення освітньо-наукової програми складається з науково-педагогічних працівників кафедри інформаційної та кібернетичної безпеки. До викладання окремих дисциплін відповідно до їх компетенції та досвіду залучений професорсько-викладацький склад: кафедри філософії Історико-філософського факультету, кафедри англійської мови Факультету права та міжнародних відносин, кафедри комп'ютерних наук і математики Факультету інформаційних технологій та управління. Наукова спрямованість освітньо-наукової програми передбачає широку участь інших фахівців, що відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної і практичної підготовки аспірантів. Керівник проектної групи та викладацький склад, який забезпечує її реалізацію, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності закладів освіти.
Матеріально-технічне забезпечення		Спеціально обладнані апаратно-програмним забезпеченням, наочними та методичними матеріалами центри розвитку компетентностей, а саме:

	1) «Центр дослідження технологій функціонування й захисту інформаційно-комунікаційних систем та мереж» з: навчальною «Лабораторією комп'ютерних мереж», навчальною «Лабораторією безпеки інформаційно-комунікаційних систем» та навчальною «Лабораторією антивірусного захисту»; 2) «Центр дослідження технологій захисту інформаційних ресурсів» з: навчальною «Лабораторією безпеки інформаційних активів» (навчальний кіберполігон) та навчальною «Лабораторією систем технічного та криптографічного захисту інформації»; 3) лабораторія вбудованих систем і 3Д моделювання тощо.
Інформаційне та навчально-методичне забезпечення	Бібліотечні електронні ресурси, електронні наукові видання, електронні навчальні курси із можливістю дистанційного навчання та самостійної роботи, хмарні сервіси Microsoft.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Київським університетом імені Бориса Грінченка та вищими навчальними закладами і науковими установами України.
Міжнародна кредитна мобільність	На основі укладених договорів, які передбачають академічну мобільність із закордонними університетами-партнерами та у рамках програми ЄС Еразмус+.
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови та на підставах, визначених чинним законодавством України.

2. Перелік компонент освітньо-наукової програми та їх логічна послідовність.

2.1. Перелік компонент ОНП

Код	Компоненти освітньо-наукової програми (навчальні дисципліни, практики)	Кількість кредитів	Форма підсумкового контролю
Обов'язкові компоненти ОНП			
Формування загальних компетентностей			
ОДЗ.01	**Філософія і методологія наукової діяльності**	**4**	екзамен
	Філософія науки	2	
	Загальнонаукова методологія	1	
	Наукова етика	1	
ОДЗ.02	**Стратегії наукових досліджень**	**6**	залік
	Нормативно-правова база наукових досліджень та наукової діяльності	1	
	Інтернаціоналізація науки	3	
	Сучасні технології інформаційної і кібербезпеки та захисту інформації	2	
ОДЗ.03	**Наукова комунікація іноземною мовою**	**10**	екзамен
	Всього	**20**	
Формування фахових компетентностей			
ОДС.01	**Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів**	**3**	залік
ОДС.02	**Прикладні аспекти створення та застосування систем технічного захисту**	**4**	залік
ОДС.03	**Прикладні аспекти створення та застосування систем криптографічного захисту**	**4**	залік
ОДС.04	**Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки**	**4**	залік
ВП.01	**Науково-викладацька практика**	**2**	залік
ВП.02	**Дослідницька практика**	**4**	залік
	Всього	**21**	
	Разом за обов'язковою частиною	**41**	
Вибіркова частина (Додаток 1)			
ВДК.01	**Системний аналіз та прийняття рішень в інформаційній і кібербезпеці**	4	залік
	Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності		
ВДК.02	**Проектування і впровадження захищених інформаційно-комунікаційних систем**	4	залік
	Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем		
ВДК.03	**Організація захисту розподілених інформаційних ресурсів**	4	залік
	Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем		
ВДК.04	**Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів**	4	екзамен
	Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури		
ВДК.05	**Технології безпеки складних соціотехнічних систем**	3	залік
	Прикладні аспекти протидії кібератакам в соціотехнічних системах		
	Всього	**19**	
	Разом за вибірковою частиною	**19**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ		**60**	

2.2 Структурно-логічна схема ОНП

<table>
<tr><th colspan="2">1 курс</th><th colspan="2">2 курс</th><th colspan="2">3 курс</th><th colspan="2">4 курс</th></tr>
<tr><th>1 семестр</th><th>2 семестр</th><th>3 семестр</th><th>4 семестр</th><th>5 семестр</th><th>6 семестр</th><th>7 семестр</th><th>8 семестр</th></tr>
<tr><td colspan="2">Наукова комунікація іноземною мовою,
4+4+2= 10 кр., каф. ІМ</td><td colspan="2" rowspan="2">Прикладні аспекти теорії ризиків, конфліктів і катастроф в системах безпеки.
4 кр., каф. ІКБ</td><td colspan="2" rowspan="3">Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів
4 кр., каф. ІКБ</td><td rowspan="6"></td><td rowspan="6"></td></tr>
<tr><td colspan="2">Стратегії наукових досліджень,
1+3+2= 6 кр., каф. ІКБ</td></tr>
<tr><td colspan="2">Філософія і методологія наукової діяльності
4 кр. каф.</td><td rowspan="2">Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів
3 кр., каф. ІКБ</td></tr>
<tr><td rowspan="3" colspan="2">Системний аналіз та прийняття рішень в інформаційній і кібербезпеці
4 кр., каф. ІКБ</td><td rowspan="2">Прикладні аспекти створення та застосування систем технічного захисту
4 кр., каф. ІКБ</td><td>Проектування і впровадження захищених інформаційно-комунікаційних систем
4 кр., каф. ІКБ</td></tr>
<tr><td rowspan="2">Технології безпеки складних соціотехнічних систем,
3 кр., каф. ІКБ</td><td rowspan="2">Прикладні аспекти створення та застосування систем криптографічного захисту
4 кр. каф. ІКБ</td><td colspan="2">Організація захисту розподілених інформаційних ресурсів,
4 кр., каф. ІКБ</td></tr>
<tr><td>Науково-викладацька практика
2 кр.</td><td>Науково-дослідницька практика
4 кр.</td></tr>
<tr><td colspan="6">60 кр.</td><td colspan="2"></td></tr>
</table>

Наукова складова освітньо-наукової програми

Освітньо-наукова програма та навчальний план аспірантури є основою для формування аспірантом індивідуального навчального плану та індивідуального плану наукової роботи.

Наукова складова освітньо-наукової програми передбачає проведення 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 зі спеціальності 125 Кібербезпека, результати якого характеризуються науковою новизною та практичною цінністю, становлять оригінальний внесок у суму знань відповідної галузі та 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.

Індивідуальний план наукової роботи є обов'язковим до виконання здобувачем відповідного ступеня і використовується для оцінювання успішності запланованої наукової роботи.

3. Форма атестації здобувачів вищої освіти

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

Стан готовності дисертації аспіранта 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 освітньо-наукової програми

	ЗК1	ЗК2	ЗК3	ЗК4	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7
ОДЗ.01				+	+						
ОДЗ.02		+	+	+	+						
ОДЗ.03	+										
ОДС.01				+		+		+			
ОДС.02							+		+	+	
ОДС.03							+		+	+	
ОДС.04							+			+	
ВП.01	+	+									
ВП.02	+	+	+	+	+	+	+	+	+	+	+
ВДК.01			+	+		+		+			
ВДК.02							+		+	+	
ВДК.03						+					+
ВДК.04								+			+
ВДК.05									+	+	+

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-наукової програми

	ПРН1	ПРН2	ПРН3	ПРН4	ПРН5	ПРН6	ПРН7
ОДЗ.01		+	+	+			
ОДЗ.02		+	+	+			
ОДЗ.03	+		+				
ОДС.01			+	+			
ОДС.02				+	+	+	
ОДС.03				+	+	+	
ОДС.04						+	
ВП.01	+	+	+	+			
ВП.02	+	+	+	+			
ВДК.01				+			
ВДК.02				+	+	+	
ВДК.03				+			+
ВДК.04				+			+
ВДК.05					+	+	+