(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державне некомерційне підприємство
«Державний університет «Київський авіаційний інститут»

ОСВІТНЬО-НАУКОВА ПРОГРАМА

«Кібербезпека»

третього (освітньо-наукового) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»

галузь знань F «Інформаційні технології»

СМЯ КАІ ОП ДФ ID65364 – 01 – 2025

Освітньо-наукова програма
Затверджена Вченою радою КАІ
протокол №___ від _____2025 р.

Вводиться в дію наказом в.о. президента

_____ Ксенія СЕМЕНОВА

Наказ №_____ від _____2025 р.

КИЇВ

Стандарт вищої освіти України: третій (освітньо-науковий) рівень, галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека та захист інформації».

Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від 29.10.2024 №1543.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-наукової програми

ПОГОДЖЕНО

Науково-методичною радою КАІ

Протокол №_____

від "___"_____2025 р.

Голова науково-методичної ради

_____ Анатолій ПОЛУХІН

ПОГОДЖЕНО

Вченою радою КАІ

Протокол №_____

від "____"_____2025 р.

Голова вченої ради

_____ Сергій ГНАТЮК

ПОГОДЖЕНО

Проректор з наукових досліджень та трансферу технологій

_____ Сергій ГНАТЮК

"____" _____2025 р.

ПОГОДЖЕНО

Завідувач аспірантури та докторантури

_____ Анжела ЛЕЛЕЧЕНКО

"____"_____2025 р

ПОГОДЖЕНО

Кафедрою кібербезпеки

Протокол №_____

від "___"_____2025 р.

Завідувач кафедри

_____Анна ІЛЬЄНКО

ПОГОДЖЕНО

Науковим товариством студентів, аспірантів, докторантів та молодих учених КАІ

Протокол №_____

від "____"_____2025 р.

Голова Наукового товариства студентів, аспірантів, докторантів та молодих учених КАІ

_____Роман ОДАРЧЕНКО

ПЕРЕДМОВА

Розроблено робочою групою освітньо-наукової програми (F5 «Кібербезпека та захист інформації») у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

Міщенко Андрій Віталійович	доктор технічних наук, доцент, професор кафедри міжнародних відносин та стратегічних студій	_____ підпис

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Гнатюк Сергій Олександрович	доктор технічних наук, професор, проректор з наукових технологій та трансферу технологій	_____ підпис
Ахрамович Володимир Миколайович	доктор технічних наук, професор, професор кафедри кібербезпеки	_____ підпис
Фесенко Андрій Олексійович	кандидат технічних наук, доцент, декан факультету комп'ютерних наук та технологій	_____ підпис
Ільєнко Анна Вадимівна	кандидат технічних наук, доцент, завідувач кафедри кібербезпеки	_____ підпис
Охріменко Тетяна Олександрівна	кандидат технічних наук, старший дослідник, заступник декана факультету комп'ютерних наук та технологій	_____ підпис
Аушев Єгор Володимирович	кандидат фізико-математичних наук, доцент кафедри кібербезпеки, CEO «Cyber Unit Technologies»	_____ підпис
Бондаровець Сергій Сергійович	здобувач вищої освіти (аспірант, спеціальність 125)	_____ підпис

ЗОВНІШНІ СТЕЙКХОЛДЕРИ:

Юдін Олексій Юрійович	кандидат технічних наук, заст. нач. ДержНДІ технологій кібербезпеки та захисту інформації	_____ підпис
Ковтун Владислав Юрійович	кандидат технічних наук, директор ТОВ «САЙФЕР ІТ»	_____ підпис
		_____ підпис

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

1. Профіль освітньо-наукової програми

Розділ 1. Загальна інформація		
1.1	Повна назва закладу вищої освіти та структурного підрозділу	Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут» Факультет комп'ютерних наук та технологій Кафедра кібербезпеки
1.2	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії / Doctor of Philosophy (Ph.D) Доктор філософії з кібербезпеки та захисту інформації
1.3	Офіційна назва освітньо-наукової програми	Кібербезпека / Cybersecurity
1.4	Тип диплому та обсяг освітньо-наукової програми	Диплом доктора філософії, одиничний; перший науковий ступінь, що здобувається на третьому (освітньо-науковому) рівні вищої освіти; 4 академічних роки; освітня складова – 57 кредитів ЄКТС.
1.5	Акредитаційна інституція	Національне агентство забезпечення якості вищої освіти.
1.6	Період акредитації	Акредитація до 01.07.2029 (сертифікат №9998 від 30.12.2024).
1.7	Цикл / рівень	Третій (освітньо-науковий) рівень QF for EHEA – третій цикл, EQF for LLL – 8 рівень; НРК України –8 рівень.
1.8	Передумови	Для здобуття освітньо-наукового рівня доктора філософії зі спеціальності F5 «Кібербезпека та захист інформації» можуть вступати особи, що здобули освітній ступінь магістра. Програма фахових вступних випробувань повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 «Кібербезпека» (125 «Кібербезпека та захист інформації») галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти.
1.9	Форма навчання	Денна, вечірня, заочна.
1.10	Мови викладання	Українська та / або англійська.
1.11	Інтернет-адреса постійного розміщення опису освітньо-наукової програми	https://nau.edu.ua/ua/menu/quality/ects/zagalna-informatsiya/informatsiya-po-osvitnih-programah.html
Розділ 2. Ціль освітньо-наукової програми		
2.1	Ціллю освітньо-наукової програми є створення інтелектуального потенціалу держави шляхом підготовки висококваліфікованих на національному та міжнародному рівнях наукових кадрів з кібербезпеки та захисту інформації для критичної інфраструктури	

	держави (включаючи авіаційну галузь).	
Розділ 3. Характеристика освітньо-професійної (наукової) програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	Галузь знань – F «Інформаційні технології» Спеціальність (освітня) – F5 «Кібербезпека та захист інформації» Спеціальності (наукові): ▪ 05.13.21 – Системи захисту інформації; ▪ 21.05.01 – Інформаційна безпека держави. *Об'єкти вивчення та діяльності*: – інформаційні системи і технології на об'єктах інформаційної діяльності та критичної інфраструктури сфери кібербезпеки та захисту інформації; – новітні системи та комплексні створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків); – сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси); – програмне та програмне-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційної безпекою, кібербезпекою та захистом інформації; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. *Цілі навчання*: набуття здатності продукувати нові ідеї, розв'язувати комплексні проблеми професійної та дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, та здійснювати власні наукові дослідження, результати яких мають наукову новизну теоретичне та практичне значення. *Теоретичний зміст предметної області.* Принципи, концепції теорії захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. *Методи, методики та технології.* Сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, методи статистичного аналізу даних. *Інструменти та обладнання.* Програмно-апаратне та

		програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні технології, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображенню та захисту даних (інформаційних потоків).
3.2	Орієнтація освітньо-наукової програми	Академічна відповідно до Міжнародної стандартної класифікації освіти (ISCED 2011 / UNESCO)
3.3	Основний фокус освітньо-наукової програми	Підготовка конкурентоздатних фахівців міжнародного рівня для критичної інфраструктури держави, включаючи авіаційну галузь, що здатні розв'язувати складні наукоємні задачі в галузі кібербезпеки та захисту інформації та проводити дослідницьку і викладацьку діяльність з кібербезпеки та суміжних ІТ-спеціальностей.
3.4	Особливості освітньо-наукової програми	**1.** Організаційне забезпечення підготовки докторів філософії здійснюється через аспірантуру Київського авіаційного інституту. **2.** Організація освітньо-наукового процесу на основі системи методів проблемно-розвиваючого навчання та методології наукових досліджень, яка ґрунтується на принципах цілеспрямованості, бінарності (безпосередня взаємодія викладача та аспіранта, наукового керівника та аспіранта, наукового керівника та викладача для корекції процесу підготовки кожного аспіранта залежно від його індивідуальних потреб), показовому, діалогічному, евристичному, дослідницькому та програмованому методах. **3.** Диференціація років підготовки за спрямованістю: ▪ перший рік підготовки – домінування освітньої складової у поєднанні за науковою; ▪ другий, третій та четвертий роки підготовки – домінування наукової складової у поєднанні з освітньою (науково-педагогічною діяльністю). **4.** Можливість зарахування до 6 кредитів ЄКТС включно (10 % від загального обсягу програми) та результатів навчання, отриманих у неформальній освіті (наприклад, курси Coursera, Prometheus, Cisco, CompTIA, ISACA, CRDF, USAID тощо) за таких умов: ▪ зарахування кредитів для обов'язкових освітніх компонентів – не більше 50 % від обсягу кредитів для кожного окремого компонента (з метою досягнення компетентностей та програмних результатів навчання, які забезпечує цей компонент; пп. 4, 5 програми); ▪ результати навчання, отримані у неформальній освіті,

		повинні співпадати або бути близькими за змістом до програмних результатів навчання (п. 5 програми), які забезпечує компонент, за яким зараховуються кредити, отримані у неформальній освіті; ▪ зарахування кредитів для вибіркових освітніх компонентів – додаткові обмеження та умови відсутні. **5.** Освітньо-наукова програма реалізує фахову профілюючу підготовку через сертифікатні освітні програми. **6.** Освітньо-наукова програма є синтезом кращих світових теорій та практик у галузі кібербезпеки та захисту інформації (як результат аналізу проєктною групою відповідних програм США, ЄС та вітчизняних ЗВО). **7.** Освітньо-наукова програма дає реальну можливість здобувачам брати участь в наукових дослідженнях на базі вітчизняних і закордонних установ-партнерів університету (зокрема, в авіаційній галузі та інших секторах критичної інфраструктури держави).
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1	Придатність до працевлаштування	Працевлаштування на посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти, посадах працівників найвищої кваліфікації у дослідницьких, проектних, конструкторських й т.п. установах і підрозділах підприємств.
4.2	Подальше навчання	Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.
Розділ 5. Викладання та оцінювання		
5.1	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	**1.** Проведення наукових досліджень з урахуванням тем дисертаційних робіт та наукових інтересів здобувачів. **2.** Синергетичне поєднання освітньої та наукової складових під час підготовки аспірантів. **3.** Проблемно-орієнтований стиль викладання, що реалізується через систему методів проблемно-розвиваючого навчання (показового, діалогічного, евристичного, дослідницького, програмованого); інтерактивних методів навчання (метод групової роботи, синектика, дискусії, рольові ігри, кейс-метод, метод проєктів), які сприяють розвитку дослідницької, творчої та пізнавальної діяльності аспірантів; методик тренінгового навчання у вигляді виконання пошукових, розрахункових та творчих завдань з використанням сучасних інформаційних технологій, роботи з базами бібліографічних, статистичних та інших видів даних, проходження науково-педагогічної практики, апробація результатів самостійного наукового дослідження (наукові конференції, семінари тощо). **4.** Використання матеріально-технічної бази факультету

		комп'ютерних наук та технологій, науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі https://cyberlab.nau.edu.ua, CyberRange UA. **5.** Тематика наукових досліджень (теми дисертацій) аспірантів повинна безпосередньо відповідати хоча б одному освітньому компонентові освітньо-наукової програми. Дисертація має розв'язувати значущі задачі у сфері комп'ютерних наук або на її межі з іншими спеціальностями галузі знань F «Інформаційні технології», що передбачає розширення та переоцінку вже існуючих і створення нових знань і професійних практик.
5.2	Оцінювання	Система оцінювання знань включає поточний і підсумковий контроль: • поточний контроль здійснюється шляхом оцінки роботи здобувача на практичних заняттях, підготовлених наукових статей, виступів на наукових конференціях та інших публічних заходах, виконання науково-дослідницьких завдань тощо; • підсумковий контроль здійснюється у формі екзамену або заліку з урахуванням накопичених балів поточного контролю. Здобувач вважається допущеним до підсумкового контролю з дисципліни у разі виконання всіх видів робіт, передбачених робочою програмою навчальної дисципліни. Виконання дисертаційного дослідження щорічно обговорюється на засіданні кафедри, за якою закріплено здобувача, виходячи з тематики дисертації. Оцінювання дисертації здійснюється за підсумками публічного захисту у разових радах із захисту дисертацій.
Розділ 6. Програмні компетентності		
6.1	Інтегральна компетентність (ІК)	Здатність продукувати нові ідеї, розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
6.2	Загальні компетентності (ЗК)	**ЗК1.** Здатність до абстрактного мислення, аналізу і синтезу. **ЗК2.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК3.** Здатність працювати в міжнародному контексті. **ЗК4.** Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

6.3	Спеціальні (фахові) компетентності (СК)	**СК1.** Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. **СК2.** Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації **СК3.** Здатність розв'язувати значущі проблеми в сфері кібербезпеки та захисту інформації., розширювати та переоцінювати наявні знання і професійні практики. **СК4.** Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації. **СК5.** Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. **СК6.** Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому українською та англійською мовами. **СК7.** Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищій освіті. **СК8**. Здатність до застосування сучасних технологій машинного навчання, штучного інтелекту, обробки великих даних, нейронних мереж, високопродуктивних обчислень для їх оптимізації та синтезу їх нових функціональних можливостей у концепції сталого розвитку.
Розділ 7. Програмні результати навчання		
7.1	Програмні результати навчання (ПР)	**РН1.** Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. **РН2.** Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.

		РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблем. **РН4.** Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці. **РН5.** Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. **РН6.** Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях. **РН7.** Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації. **РН8.** Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах. **РН9.** Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи. **РН10.** Організовувати і здійснювати освітній процес у сфері інформаційних технологій, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти. **ПР11**. Глибокі знання й розуміння сучасних технологій машинного навчання, штучного інтелекту, обробки великих даних, нейронних мереж, Інтернету речей, високопродуктивних обчислень у концепції сталого розвитку.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1	Кадрове забезпечення	**1.** Наукове керівництво аспірантом здійснюється активним

		дослідником (що має науковий ступінь та/або вчене звання), який має публікації по темі, що відповідає темі дисертаційного дослідження аспіранта, результати наукової роботи керівника публікуються чи практично впроваджуються не рідше, ніж раз на два роки. **2.** До наукового керівництва аспірантами не допускаються особи, які були притягнуті до відповідальності за порушення академічної доброчесності. **3.** До додаткового наукового консультування аспірантів за необхідності (відповідно до їх потреб) може бути залучений будь-який науково-педагогічний чи науковий працівник факультету комп'ютерних наук та технологій КАІ (структурний підрозділ, який забезпечує реалізацію освітньо-наукової програми відповідно до п. 1.1) та / або фахівці інших вітчизняних чи закордонних ЗВО або наукових установ (у рамках чинних угод про наукове співробітництво) з організаційним забезпеченням такого залучення з боку гаранта освітньо-наукової програми та декана зазначеного факультету. **4.** Навчальні дисципліни та інші освітні компоненти освітньо-наукової програми викладаються та забезпечуються науково-педагогічними та науковими працівниками, наукова діяльність яких (публікації, НДР, гранти, стажування тощо) відповідає змісту зазначених навчальних дисциплін та інших освітніх компонентів, які ними викладаються та / або забезпечуються. **5.** Представники академічної та наукової спільноти, зокрема, міжнародної, а також роботодавці залучаються до організації та реалізації освітнього процесу та / або наукового консультування аспірантів. **6.** Ураховуються вимоги пп. 35-38 Ліцензійних умов провадження освітньої діяльності (Постанова КМУ № 1187 від 30.12.2015 із змінами, внесеними згідно з Постановами КМУ № 347 від 10.05.2018, № 180 від 03.03.2020 № 365 від 24.03.2021).
8.2	Матеріально-технічне забезпечення	Для реалізації освітньої діяльності за освітньо-науковою програмою та здійснення наукових досліджень може бути залучене за необхідності (відповідно до потреб аспірантів та потреб реалізації освітніх компонентів) будь-яке обладнання та програмне забезпечення лабораторій та аудиторний фонд випускової кафедри кібербезпеки, науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі https://cyberlab.nau.edu.ua, CyberRange UA, які входять до складу Факультету комп'ютерних наук та технологій КАІ (структурний підрозділ, який забезпечує реалізацію освітньо-наукової програми відповідно до п. 1.1). В університеті наявна вся необхідна соціально-побутова

		інфраструктура (гуртожитки, їдальня, спортивні зали та спортивні майданчики, тренажерні зали, медичний комплекс), кількість місць в гуртожитках відповідає вимогам.
8.3	Інформаційне та навчально-методичне забезпечення	На сайті випускової кафедри розміщено основні інформаційні матеріали (програми вступних випробувань, силабуси, навчальні програми та плани) для вступників та аспірантів http://kszi.nau.edu.ua/ Навчально-методичні матеріали навчальних дисциплін (конспекти лекцій, лабораторні практикуми тощо), репозитарій КАІ (https://er.nau.edu.ua), ресурси Науково-технічної бібліотеки КАІ (http://www.lib.nau.edu.ua), безоплатні з локальної мережі університету доступ до повнотекстових ресурсів видавництва Springer, а також повнофункціональний доступ до наукометричних баз даних Scopus та Web of Science; для публікації та апробації результатів наукових досліджень аспірантів – фахові наукові журнали КАІ (http://jrnl.nau.edu.ua), зокрема видання базового факультету (наукові журнали «Безпека інформації» та «Захист інформації») і видавництва MECS Press (Hong Kong) http://www.mecs-press.org (у рамках діючої угоди про співпрацю), а також низка конференцій, співорганізатором яких є КАІ та публікації в яких індексуються науко-метричними базами даних Scopus / Web of Science: ▪ International Conference on Computer Science, Engineering and Education Applications (ICCSEEA); ▪ International Conference on Cyber Hygiene & Conflict Management in Global Information Networks; ▪ International Symposium on Network Security and Communications (ISNSC); ▪ International Conference on Next Generation Cybersecurity Systems and Applications (NGSEC).
Розділ 9. Академічна мобільність		
9.1	Національна кредитна мобільність	Відповідно до Постанови Кабінету Міністрів України «Про затвердження Порядку реалізації права на академічну мобільність» від 12.08.2015 № 579 (із змінами). Програми міжнародної академічної мобільності Erasmus+, Mevlana та інші (згідно міжнародних угод).
9.2	Міжнародна кредитна мобільність	
9.3	Навчання іноземних здобувачів вищої освіти	Реалізація освітньої та наукових складових освітньо-наукової програми англійською мовою для іноземців та осіб без громадянства (за потреби), врахування особливостей передумов, викладених у п. 1.8, умови вступу для іноземців та осіб без громадянства регулюються Правилами прийому до аспірантури та докторантури КАІ .

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

2.1. Перелік компонент

Код н/д	Компоненти освітньо-наукової програми	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
1.1	***Цикл дисциплін з оволодіння загальнонауковими (філософськими) компетентностями***			
ОК1.1.1	Філософія науки	3	Екзамен	1
1.2	***Цикл дисциплін із набуття універсальних навичок дослідника та викладача***			
ОК1.2.1	Правове забезпечення наукових досліджень	3	Диф. залік	1
ОК1.2.2	Економічне забезпечення наукових досліджень	3	Диф. залік	1
ОК1.2.3	Інформаційне забезпечення наукових досліджень	3	Диф. залік	1
ОК1.2.4	Андрагогіка та інноваційні освітні технології вищої освіти	3	Диф. залік	1
1.3	***Цикл дисциплін із оволодіння глибинними знаннями зі спеціальності***			
ОК1.3.1	Методологія наукових досліджень у сфері кібербезпеки та захисту інформації	3	Диф. залік	1
ОК1.3.2	Статегія та тактика кібервійни	3	Диф. залік	2
ОК1.3.3	Технології захисту критичної інформаційної інфраструктури	3	Екзамен	2
ОК1.3.4	Цифрова криміналістика (Digital forensic)	3	Екзамен	2
ОК1.3.5	Стандартизація та сертифікація в галузі кібербезпеки та захисту інформації	3	Екзамен	2
1.4	***Цикл дисциплін зі здобуття мовних компетентностей***			
ОК1.4.1	Англійська мова наукового спрямування	3	Екзамен	1
ОК1.4.2	Академічне письмо англійською мовою (English academic writing)	3	Диф. Залік	2
1.5	***Цикл практичної підготовки***			
ОК1.5.1	Фахова науково-педагогічна практика	6	Диф. Залік	1
	Дисертаційна робота доктора філософії		Захист	8
Загальний обсяг обов'язкових компонентів:		**42 кредити ЄКТС**		

1	2	3	4	5
Вибіркові компоненти				
Вибір дисциплін				
ВК1	Загальноуніверситетський вибір	5	Диф. Залік	2
ВК2	Фаховий вибір*	5	Диф. Залік	2

ВК3	Фаховий вибір*	5	Диф. Залік	2
Загальний обсяг вибіркових компонент 15 кредитів ЄКТС				
Загальний обсяг освітньої складової освітньо-наукової програми 57 кредитів ЄКТС				

** У Додатку 1*

2.2. Структурно-логічна схема освітньої програми

1 семестр							
ОК 1.1.1	**ОК 1.2.1**	**ОК 1.2.2**	**ОК 1.2.3**	**ОК 1.2.4**	**ОК 1.3.1**	**ОК 1.4.1**	**ОК 1.5.1**
2 семестр							
ОК 1.3.2	**ОК 1.3.3**	**ОК 1.3.4**	**ОК 1.3.5**	**ОК 1.4.2**	*ВК 1*	*ВК 2*	*ВК 3*
3-8 семестр							

3. Наукова складова

Рік підготовки	Зміст наукової роботи здобувача вищої освіти	Форма контролю
Перший рік	Вибір теми дисертаційного дослідження аспіранта, формування індивідуального плану роботи здобувача вищої освіти; виконання дисертаційної роботи під керівництвом наукового керівника; підготовка та подання до друку не менше однієї публікації за темою дисертації та участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей	Затвердження на вченій раді факультету / інституту, звітування двічі на рік про виконання індивідуального плану аспіранта
Другий рік	Виконання під керівництвом наукового керівника дисертаційного дослідження; підготовка та подання до друку не менше однієї публікації за темою дисертації відповідно чинних вимог; участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей	Звітування про хід виконання індивідуального плану аспіранта двічі на рік
Третій рік	Виконання під керівництвом наукового керівника дисертаційної роботи; підготовка та подання до друку не менше двох публікації за темою дисертації відповідно чинних вимог; участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей	Звітування про хід виконання індивідуального плану аспіранта двічі на рік
Четвертий рік	Завершення та оформлення дисертаційної роботи, підведення підсумків щодо повноти висвітлення результатів дисертації у наукових статтях відповідно чинних вимог; подання документів на попередню експертизу дисертації; підготовка наукової доповіді для підсумкової атестації (захисту дисертації) Звітування про хід виконання індивідуального плану аспіранта двічі на рік.	Надання висновку про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження

4. Форма атестації здобувачів вищої освіти

Підсумкова атестація здобувачів вищої освіти за освітньо-науковою програмою «Кібербезпека» галузі знань F «Інформаційні технології» проводиться у формі публічного захисту дисертаційної роботи у разовій спеціалізованій вченій раді та завершується видачею документа встановленого зразка про присудження йому наукового ступеня доктора філософії з присвоєнням кваліфікації «Доктор філософії з комп'ютерних наук» («Doctor of Philosophy (Ph.D) in Cybersecurity»).

Відповідно до «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженого Постановою КМУ № 261 від 23.03.2016 (із змінами, внесеними згідно з Постановами КМУ № 283 від 03.04.2019, № 502 від 19.05.2023): протягом строку навчання в аспірантурі (ад'юнктурі) аспірант (ад'юнкт) повинен виконати освітню і наукову складові освітньо-наукової програми, зокрема здобути теоретичні знання, уміння, навички та інші компетентності, достатні для продукування нових ідей, розв'язання комплексних проблем у галузі професійної та/або дослідницько-інноваційної діяльності, оволодіти методологією наукової та педагогічної діяльності, а також провести власне наукове дослідження, результати якого мають наукову новизну, теоретичне та/або практичне значення, опублікувати наукові публікації за темою дисертації, підготувати дисертацію та пройти процедуру атестації разовою спеціалізованою вченою радою на підставі публічного захисту наукових досягнень у формі дисертації.

5. Вимоги до кваліфікаційної роботи (дисертації)

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим науковим дослідженням, що має розв'язувати комплексну проблему у сфері комп'ютерних наук або на її межі з іншими спеціальностями, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.

Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації.

Дисертація має бути розміщена на сайті закладу вищої освіти (наукової установи)

6. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

	ОК 1.1.1	ОК 1.2.1	ОК 1.2.2	ОК 1.2.3	ОК 1.2.4	ОК 1.3.1	ОК 1.3.2	ОК 1.3.3	ОК 1.3.4	ОК 1.3.5	ОК 1.4.1	ОК 1.4.2	ОК 1.5.1
ЗК01	+	+	+	+	+	+							
ЗК02				+							+	+	
ЗК03											+	+	
ЗК04	+						+						+
СК01				+		+	+						
СК02											+	+	
СК03		+		+		+							
СК04					+								
СК05			+			+							
СК06							+	+	+	+	+		+
СК07					+		+						
СК08						+		+	+	+			

7. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК 1.1.1	ОК 1.2.1	ОК 1.2.2	ОК 1.2.3	ОК 1.2.4	ОК 1.3.1	ОК 1.3.2	ОК 1.3.3	ОК 1.3.4	ОК 1.3.5	ОК 1.4.1	ОК 1.4.2	ОК 1.5.1
ПР01		+	+			+	+						
ПР02				+			+				+	+	+
ПР03						+	+						
ПР04						+							
ПР05				+		+	+						
ПР06				+		+				+			
ПР07	+	+	+	+									
ПР08					+		+	+	+	+			+
ПР09	+				+								+
ПР10							+						
ПР11		+	+		+	+							

(Ф 03.02 - 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 - 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище, ім’я, побатькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 - 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	зміненого	заміненого	нового	анульованого			

(Ф 03.02 - 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЙ

№ пор.	Прізвище, ім’я, по батькові	Дата ревізії	Підпис	Висновок щодо адекватності