ПРОЄКТ
(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи та технології кібербезпеки»

Другого (магістерського) рівня вищої освіти

за спеціальністю F5 Кібербезпека та захист інформації____

галузі знань F Інформаційні технології____

СМЯ КАІ ОП М ID65379 – 01– 2025

Освітньо-професійна програма
затверджена Вченою радою КАІ
протокол №____від_____2025р.
Вводиться в дію наказом в.о. президента КАІ
від_____2025 р. №_____

В.о. президента

_____ Ксенія СЕМЕНОВА

КИЇВ

Враховано Стандарт вищої освіти України: другого (магістерського) рівня, галузі знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека». Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою КАІ

протокол №_____

від "_____"_____2025 р.

Голова НМР КАІ

_____

ПОГОДЖЕНО

Вченою радою факультету комп'ютерних наук та технологій

протокол №_____

від "_____"_____2024 р.

Голова Вченої ради
факультету комп'ютерних наук та технологій

_____Андрій ФЕСЕНКО

ПОГОДЖЕНО

Кафедрою технічного захисту інформації

протокол засідання №_____

від "_____"_____2025 р.

Завідувач кафедри

_____Валерій КОЗЛОВСЬКИЙ

ПОГОДЖЕНО

Студентською радою факультету
комп'ютерних наук та технологій

протокол №_____

від "_____"_____2025 р.

Голова Студентської ради факультету

_____Власне ім'я ПРІЗВИЩЕ

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності F5 Кібербезпека та захист інформації у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ІВАНЧЕНКО Ігор Сергійович	*к.т.н., доц., доцент кафедри технічного захисту інформації*	_____ підпис
ЧЛЕНИ РОБОЧОЇ ГРУПИ:		
КОЗЛОВСЬКИЙ Валерій Валерійович	*д.т.н., проф., завідуючий кафедри технічного захисту інформації*	_____ підпис
ЗИБІН Сергій Вікторович	*проф., професор кафедри технічного захисту інформації*	_____ підпис
ПРИХОДЬКО Тетяна Юріївна	*к.т.н, доц., доцент кафедри технічно захисту інформації*	_____ підпис
	здобувач(ка) вищої освіти за освітньою програмою, група	_____ підпис
ЗОВНІШНІ СТЕЙКГОЛДЕРИ:		
ЛАХНО Валерій Анатолійович	*д.т.н., проф., професор кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України*	_____ підпис

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

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

Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Державний університет «Київський авіаційний інститут» Факультет комп'ютерних наук та технологій Кафедра технічного захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Освітній ступінь: магістр Освітня кваліфікація: магістр з кібербезпеки та захисту інформації
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Системи та технології кібербезпеки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, розрахункові строки виконання освітньої програми: 1 рік 6 місяців (денна форма здобуття освіти) 1 рік 6 місяці (заочна форма здобуття освіти)
1.5.	Акредитаційна інституція	Національне агентство із забезпечення якості вищої освіти
1.6.	Період акредитації	До 22.10.2025 р.
1.7.	Цикл/рівень	Другий (магістерський) рівень 7 рівень Національної рамки кваліфікацій України (НРК України), другий цикл Європейського простору вищої освіти (FQ-EHEA), 7 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Для здобуття освітнього рівня магістра можуть вступати особи, що здобули освітній рівень бакалавра. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти. Заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані за попередньою освітньою програмою підготовки магістра (спеціаліста) за іншою спеціальністю. Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми. Умови вступу регулюються Правилами прийому до КАІ.
1.9	Мова(и) викладання	Українська
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.kai.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Мета (цілі) освітньо-професійної програми		
2.1.	Мета (цілі) освітньо-професійної програми полягає у підготовці висококваліфікованих і конкурентоспроможних фахівців у сфері кібербезпеки, здатних розробляти, впроваджувати та управляти сучасними системами захисту інформації, що забезпечує формування необхідних компетентностей для оцінювання ризиків, впровадження політик інформаційної безпеки та використання новітніх технологій кіберзахисту, зокрема в критичних інформаційних інфраструктурах, у тому числі в авіаційній галузі; інтеграція теоретичних знань із практичними навичками, дозволяє випускникам ефективно працювати в умовах динамічного розвитку загроз та	

	технологічних викликів у сфері кібербезпеки, а опанування специфічних знань та особливостей професійної діяльності в авіаційному секторі, дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в даній галузі задля позитивного внеску у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей з урахуванням потреб ІТ ринку, а також авіаційної галузі України.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	*Об'єкт діяльності:* – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. *Цілі навчання:* Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. *Теоретичний зміст предметної області:* Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. *Методи, методики та технології:* Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів

		із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. *Інструменти та обладнання:* Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма має прикладну орієнтацію. Базується на загальновідомих положеннях, результатах сучасних наукових досліджень та нових знаннях у сфері систем та технологій кібербезпеки та акцентована на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності, а також на розвиток здатності розв'язувати складні задачі і проблеми в галузі інформаційних технологій, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта в галузі «Інформаційні технології», що забезпечує підготовку фахівців із поглибленою спеціалізацією в сфері кібербезпеки, включаючи моделювання, розробку, впровадження та управління системами кіберзахисту. Основний акцент зроблено на оцінюванні ризиків, впровадженні політик інформаційної безпеки та застосуванні сучасних технологій у критичних інформаційних інфраструктурах. Програма поєднує фундаментальні знання з інформаційних технологій, криптографії, аналізу кіберзагроз і управління безпекою, приділяючи особливу увагу практичній підготовці. Враховуючи авіаційну специфіку, програма спрямована на забезпечення безперервності бізнес-процесів, захист критичних систем та дотримання міжнародних стандартів авіаційної безпеки. **Ключові слова:** кібербезпека, інформаційна безпека, криптографічний захист, управління ризиками, авіаційна безпека, критична інформаційна інфраструктура, кіберзагрози, політики інформаційної безпеки, захист даних, системи управління безпекою.
3.4.	Особливості освітньо-професійної програми	Програма передбачає ґрунтовну теоретичну підготовку, поєднану з практичним застосуванням сучасних технологій кіберзахисту, орієнтованих на потреби галузі ІТ; поглиблене вивчення міжнародних стандартів, законодавчої та нормативно-правової бази України; методів управління ризиками; технічного та криптографічного захисту інформації; а також

		автоматизованих систем проєктування. Унікальність програми полягає в її галузевій спрямованості, що враховує специфіку авіаційної галузі, зокрема забезпечення кібербезпеки критичних інформаційних систем, які використовуються в транспортній інфраструктурі. Навчальний процес орієнтований на формування компетентностей, необхідних для оцінювання загроз, розробки політик безпеки та інтеграції інтелектуалізованих систем кіберзахисту. Відмінністю освітньо-професійної програми є підготовка фахівців у сфері кібербезпеки з урахуванням актуальних вимог IT-ринку та специфіки авіаційної галузі, що забезпечує їхню здатність ефективно захищати інформаційні та комунікаційні системи критичної інфраструктури.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники програми підготовлені до широкого спектра професійних ролей у сфері кібербезпеки та захисту інформації, відповідно до сучасних вимог IT-ринку та авіаційної галузі, зокрема можуть працювати в державних і комерційних установах, банках, підприємствах критичної інфраструктури, правоохоронних органах, кіберпідрозділах оборонного сектору, наукових та освітніх закладах. Вони здатні займатися розробкою, впровадженням та адмініструванням систем захисту інформації, аналізом кіберзагроз, тестуванням рівня безпеки, криптографічним і технічним захистом даних, розслідуванням кіберзлочинів та реагуванням на інциденти кібербезпеки.
4.2.	Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Базується на принципах студентоцентризму та індивідуального підходу, забезпечуючи навчання через дослідницьку діяльність, практичну спрямованість і творчий розвиток. Освітній процес поєднує лекції, практичні заняття, самостійну та науково-дослідницьку роботу, розв’язування реальних задач, виконання проєктів, проходження навчальних і виробничих практик, а також підготовку курсових і кваліфікаційних робіт. **Методи, методики та технології.** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані

		системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
5.2.	Оцінювання	Відповідно до Положення про організацію освітнього процесу в КАІ, рейтингової системи оцінювання набутих студентом знань та вмінь, визначеної для кожної навчальної дисципліни її робочою програмою, інших нормативних документів.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна Компетентність (ІК)	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
6.3.	Фахові компетентності (ФК)	ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

		ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. ***Додаткові компетентності, пов'язані з особливостями освітньої програми:*** ФК11. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. ФК12. Здатність організовувати роботу колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем захисту інформації. ФК13. Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень. ФК14. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації, а також застосовувати методи і засоби організаційного характеру щодо захисту інформації на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь. ФК15. Здатність розробляти та впроваджувати стратегії кіберстійкості систем та технологій кібербезпеки у межах концепції сталого розвитку, спрямованої на зменшення кіберризиків в контексті забезпечення захисту критичної інфраструктури та створення безпечного цифрового простору, а також формування компетентності для підтримки інновацій у сфері кібербезпеки (Ціль 9) та зміцнення інформаційної безпеки задля забезпечення довіри у кіберпросторі відповідно до принципів миру, правосуддя та ефективних інституцій (Ціль 16)
Розділ 7. Програмні результати навчання		
7.1.		ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або

		мультидисциплінарних контекстах. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або

		кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. ***Додаткові компетентності, пов'язані з особливостями освітньої програми*** ПРН24. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки, в тому числі в галузі авіаційної безпеки. ПРН25. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки, що дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в тому числі і в сфері авіаційної безпеки.

		ПРН26. Розробляти та впроваджувати стратегії кіберстійкості систем та технологій кібербезпеки, спрямовані на захист критичної цифрової інфраструктури, підвищення стійкості інформаційних систем до атак, мінімізацію кіберризиків та розвиток ефективних механізмів реагування на кіберзагрози, необхідні для забезпечення безпечного цифрового середовища, розвитку інновацій у сфері кібербезпеки (Ціль 9), підвищення рівня захищеності міських цифрових екосистем (Ціль 11) та зміцнення інституційних механізмів протидії кіберзлочинності відповідно до принципів миру, правосуддя та ефективного управління (Ціль 16).
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. У процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне Забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
8.3	Інформаційне та навчально-методичне Забезпечення	Офіційний веб-сайт www.kai.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/14303 Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	У рамках двосторонніх договорів між ДНП ДУ Київський авіаційний інститут та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між ДНП ДУ Київський авіаційний інститут та навчальними закладами ЄС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

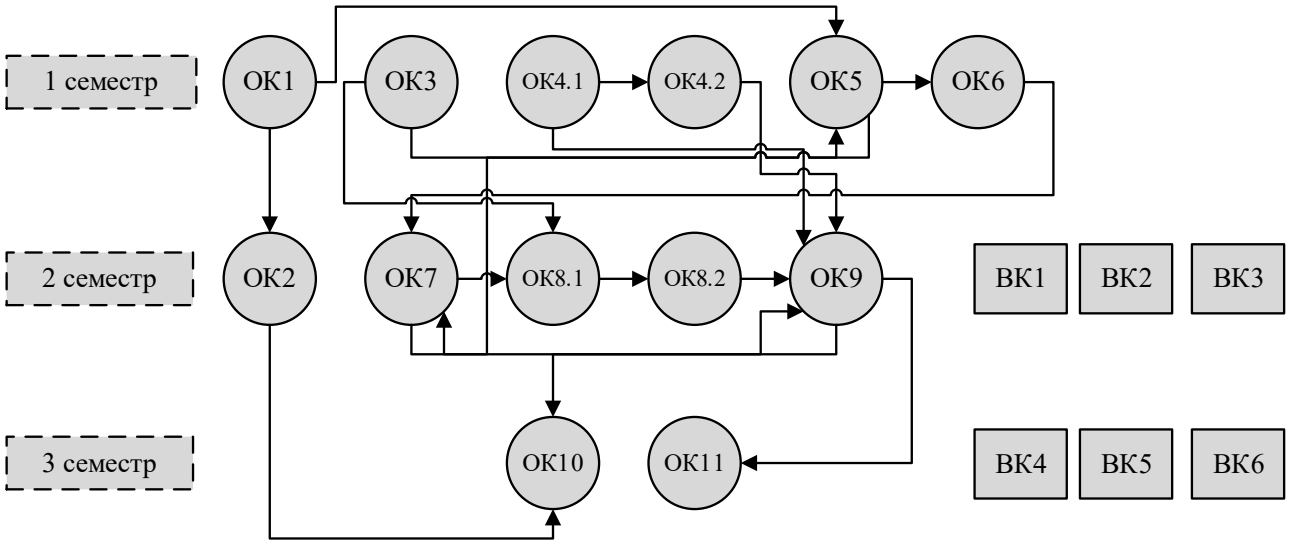
2. Перелік освітніх компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонентів

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти ОПП				
ОК1	Ділова іноземна мова	3,5	Екзамен	1
ОК2	Наукові комунікації у фаховій діяльності	3,5	Диф. Залік	2
ОК3	Методи побудови та аналізу криптосистем	6,0	Екзамен	1
ОК4.1	Методологія прикладних досліджень у сфері кібербезпеки	6,5	Диф. Залік	1
ОК4.2	Курсовий проєкт з дисципліни «Методологія прикладних досліджень у сфері кібербезпеки»	1,5	Захист	1
ОК5	Моделювання та оптимізація безпекових процесів авіаційної галузі	6,0	Екзамен	1
ОК6	Організаційні моделі кібербезпеки	6,5	Диф. Залік	1
ОК7	Аудит інформаційної безпеки	3,5	Екзамен	2
ОК8.1	Інтелектуалізовані системи інформаційної безпеки	4,0	Екзамен	2
ОК8.2	Курсова робота з дисципліни «Інтелектуалізовані системи інформаційної безпеки»	1,0	Захист	2
ОК9	Науково-дослідна практика в області систем та технологій кібербезпеки	6,0	Диф. Залік	2
ОК10	Переддипломна практика	9,0	Диф. Залік	3
ОК11	Кваліфікаційна робота	9,0	Захист	3
Загальний обсяг обов'язкових компонентів:		**66 кредитів ЄКТС**		
Вибіркові компоненти *				
ВК 1	Дисципліна 1	4,0	Диф. Залік	2
ВК 2	Дисципліна 2	4,0	Диф. Залік	2
ВК 3	Дисципліна 3	4,0	Диф. Залік	2
ВК 4	Дисципліна 4	4,0	Диф. Залік	3
ВК 5	Дисципліна 5	4,0	Диф. Залік	3
ВК 6	Дисципліна 6	4,0	Диф. Залік	3
Загальний обсяг вибіркових компонентів		**24 кредитів ЄКТС**		
Загальний обсяг освітньо-професійної програми		**90 кредитів ЄКТС**		

**Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується Законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ. Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	**Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.**
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв’язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.
Вимоги до публічного захисту (демонстрації)	Захист кваліфікаційних робіт проводиться шляхом публічного захисту на відкритому засіданні ЕК.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК1	ОК2	ОК3	ОК4.1	ОК4.2	ОК5	ОК6	ОК7	ОК8.1	ОК8.2	ОК9	ОК10	ОК11	ВК1	ВК2	…	ВКn
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК1		+	+			+	+	+	+	+	+	+	+				
ЗК2	+	+	+		+	+	+	+	+	+		+	+				
ЗК3		+		+		+		+					+				
ЗК4		+		+	+	+	+	+				+	+				
ЗК5	+	+								+	+	+	+				
ФК1				+				+					+				
ФК2	+	+		+	+	+	+				+	+	+				
ФК3			+	+	+	+	+		+	+			+				
ФК4						+	+	+	+				+				
ФК5					+	+		+					+				
ФК6			+			+		+		+			+				
ФК7				+	+	+	+		+				+				
ФК8			+					+					+				
ФК9				+		+	+		+	+		+	+				
ФК10		+		+					+	+		+	+				
ФК11	+	+		+					+	+	+	+	+				
ФК12		+		+					+	+	+	+	+				
ФК13		+			+		+		+	+		+	+				
ФК14		+		+		+		+			+		+				
ФК15			+	+	+	+	+	+	+	+	+	+	+				

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

Компоненти / Програмні результати навчання	ОК1	ОК2	ОК3	ОК4.1	ОК4.2	ОК5	ОК6	ОК7	ОК8.1	ОК8.2	ОК9	ОК10	ОК11	ВК1	ВК2	…	ВКn
ПРН1	+								+	+	+	+	+				
ПРН2		+		+		+			+	+	+	+	+				
ПРН3		+	+	+	+	+							+				
ПРН4			+			+	+	+	+	+		+	+				
ПРН5	+	+		+	+	+	+					+	+				
ПРН6			+		+	+		+					+				
ПРН7				+	+		+						+				
ПРН8				+		+	+					+	+				
ПРН9			+	+	+			+					+				
ПРН10					+	+	+						+				
ПРН11		+		+	+	+			+	+	+	+	+				
ПРН12						+	+						+				
ПРН13			+	+	+	+	+					+	+				
ПРН14						+		+	+	+	+	+	+				
ПРН15		+		+	+	+			+	+	+	+	+				
ПРН16				+		+	+						+				
ПРН17		+				+			+	+	+	+	+				
ПРН18		+		+	+				+	+		+	+				
ПРН19			+	+		+	+					+	+				
ПРН20		+		+								+	+				
ПРН21						+		+					+				
ПРН22									+	+	+	+	+				
ПРН23			+	+				+					+				
ПРН24				+		+	+	+			+	+	+				
ПРН25				+	+			+	+	+			+				
ПРН26			+	+	+	+	+	+	+	+	+	+	+				

6. Система внутрішнього забезпечення якості вищої освіти КАІ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та діяльністю КАІ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності, затвердженим рішенням Вченої ради університету від 28.11.2018 (протокол №8), та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 №1556-VII (зі змінами; розділ V «Забезпечення якості вищої освіти», стаття 16).

7. Перелік нормативних документів, на яких базується освітньо-професійна програма

1. Закон України «Про освіту» від 05.09.2017 № 2145-VIII (із змінами) [Електронний ресурс]. – режим доступу: http://zakon.rada.gov.ua/laws/show/2145-19
2. Закон України «Про вищу освіту» від 01.07.2014 № 1556-VII (із змінами) [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18
3. Постанова Кабінету Міністрів України від 23.11.2011 № 1341 «Про затвердження Національної рамки кваліфікацій» (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/1341-2011-п
4. Постанова Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/266-2015-п
5. Національний класифікатор України. Класифікація видів економічної діяльності: ДК 009:2010, затверджений наказом Держспоживстандарту України від 11.10.2010 № 457 (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/vb457609-10
6. Національний класифікатор України. Класифікатор професій ДК 003:2010, затверджений наказом Держспоживстандарту України від 28.07.2010 № 327 (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10.
7. Стандарт вищої освіти зі спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 18.03.2021 № 332.
8. Професійний стандарт «Аудитор інформаційних технологій (з кібербезпеки)», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.
9. Професійний стандарт «Фахівець з підтримки інфраструктури кіберзахисту», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.
10. Професійний стандарт «Фахівець з реагування на інциденти кіберезпеки», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.
11. Професійний стандарт «Фахівець з кібердосліджень та розробок систем безпеки», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.
12. Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20/ed20240101
13. Annex 17 «The Convention on International Civil Aviation. Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference. International Civil Aviation Organization» (12 видання, липень 2022 року) [Електронний ресурс]. – режим доступу: https://www.icao.int/Documents/annexes_booklet.pdf»

(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 по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 - 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЙ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(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 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				