ПРОЄКТ
(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

Другого (магістерського) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»

галузі знань F «Інформаційні технології»

СМЯ КАІ ОП М ID65512 – 01 – 2025

Освітньо-професійна програма
затверджена Вченою радою КАІ
протокол № _____ від _____ 2025 р.
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», спеціальності 125 «Кібербезпека».

Стандарт вищої освіти України 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,
проректор з навчальної роботи

_____ Анатолій ПОЛУХІН

ПОГОДЖЕНО
Вченою радою факультету комп'ютерних наук та технологій
протокол №_____
від «_____»_____2025 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
_____ _____

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (спеціальності F5 «Кібербезпека та захист інформації») у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ЛАЗАРЕНКО Сергій Володимирович - д.т.н., професор, професор кафедри технічного захисту інформації

_____
підпис гаранта

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ Валерій Валерійович - д.т.н., професор, завідувач кафедри технічного захисту інформації

_____
підпис члена робочої групи

ТЕМНІКОВ Володимир Олександрович - д.т.н., доцент, професор кафедри технічного захисту інформації

_____
підпис члена робочої групи

ШВЕЦЬ Валеріян Анатолійович - к.т.н., доцент, доцент кафедри технічного захисту інформації

_____
підпис члена робочої групи

_____
_____ - здобувач(ка) вищої освіти за
_____ освітньою програмою, група _____

_____
підпис здобувача вищої освіти

ЗОВНІШНІ СТЕЙКХОЛДЕРИ:

Савченко В.А. – д.т.н., професор, професор кафедри управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій

_____
(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 технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому, обсяг освітньо-професійної програми, форми здобуття освіти та розрахункові строки виконання освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС. Очна (денна), заочна форми здобуття освіти. Розрахункові строки виконання освітньої програми: - 1 рік 6 місяців (денна форма здобуття освіти); - 1 рік 6 місяців (заочна форма здобуття освіти).
1.5.	Акредитаційна інституція	Національне агентство із забезпечення якості вищої освіти. Дата видачі сертифіката про акредитацію освітньої програми 25.06.2024 № 8810
1.6.	Період акредитації	До 25.06.2025 р., чергова
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 (вимоги до освіти осіб, які можуть розпочати навчання за освітньою програмою)	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 F5 «Кібербезпека та захист інформації» 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.

1.9.	Форма навчання	Інституційна з елементами дистанційної: очна (денна), заочна, мережева.
1.10.	Мова(и) викладання	Українська
1.11.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://kai.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціллю освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» є підготовка висококваліфікованих, конкурентоспроможних фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями кібербезпеки та захисту інформації, здатних як розв'язувати задачі дослідницького та/або інноваційного характеру у сфері кібербезпеки та захисту інформації, так і опановувати специфічні знання особливостей професійної діяльності в авіаційному секторі. Забезпечення здобувачів вищої освіти фундаментальною підготовкою у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації, з метою позитивного внеску у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і практики.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1.	Предметна область (об'єкт діяльності, теоретичний зміст)	***Об'єкт діяльності*:** системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків). ***Об'єкти вивчення:*** - 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, 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

3.1.	Предметна область (об’єкт діяльності, теоретичний зміст)	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 кібербезпеки та захисту інформації. ***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 кібербезпеки та захисту інформації. 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 кібербезпеки та захисту інформації.

3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію. Освітньо-професійна програма базується на загальновідомих наукових результатах в галузі інформаційних технології, кібербезпеки та захисту інформації у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми	Загальна вища освіта та професійна підготовка в галузі «Інформаційні технології» за спеціальністю F5 «Кібербезпека та захист інформації». Освітньо-професійна програма спрямована на підготовку фахівців, здатних забезпечити захист інформації технічними засобами на об'єктах інформаційної діяльності та об'єктах авіаційної галузі України. Ключові слова: технічний захист інформації, автоматизовані системи захисту інформації, обробка інформації з обмеженим доступом.
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - методів та засобів організації і впровадження заходів щодо забезпечення кібербезпеки та захисту інформації; - автоматизованих систем обробки інформації з обмеженим доступом; - методів та засобів технічного захисту інформації тощо. На відміну від інших освітніх програм увага приділяється реалізації моделі підготовки фахівців в сфері систем технічного захисту інформації з урахуванням потреб ІТ ринку, а також авіаційної галузі України. У ОПП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Можливості працевлаштування	Випускники підготовлені до роботи у сфері кібербезпеки та захисту інформації в складі відповідних служб захисту інформації організацій, підприємств та банків; у сфері впровадження і експлуатації програмних та програмно-апаратних комплексів та засобів захисту інформації; в галузі кібербезпеки в складі правоохоронних органів; у сфері забезпечення кібербезпеки та захисту інформації в кіберпросторі (зокрема, на

		об’єктах критичної інфраструктури, в службах та підрозділах авіаційної безпеки).
4.2.	Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Студентоцентрований підхід у навчанні, самонавчання, проблемно-орієнтоване навчання. Комбінація лекцій, лабораторних занять із розв’язанням ситуаційних завдань та з використанням кейс-методів, ділових ігор, міждисциплінарних тренінгів, що розвивають комунікативні та лідерські навички й уміння працювати в команді. Виконання проектів, дослідницькі лабораторні роботи, виробничі практики, курсових робіт (проєктів), підготовка магістерської кваліфікаційної роботи. ***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 систем технічного захисту, прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у напрямку кібербезпеки та захисту інформації. 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.*** Системи та комплекси виявлення каналів витоку інформації та технічного захисту інформації на об’єктах інформаційної діяльності. 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) при дослідженні та 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)	**ІК1.** 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

6.3.	Фахові компетентності (ФК)	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 аналізувати потреби та вимоги

6.3.	Фахові компетентності (ФК)	користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації. **ФК12.** Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз. (до Цілей сталого розвитку 9, 11 і 16). **ФК13.** Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності. **ФК14.** Здатність моделювати безпекові процеси в авіаційній галузі.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	**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.

7.1.	Програмні результати навчання (ПРН)	**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

7.1.	Програмні результати навчання (ПРН)	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

7.1.	Програмні результати навчання (ПРН)	інформації. ***Додаткові програмні результати навчання, пов'язані з особливостями освітньої програми:*** **ПРН24.** Розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, інформація з обмеженим доступом) **ПРН25.** Проводити спеціальні дослідження засобів обробки інформації, технічних засобів. **ПРН26.** Визначати показники захищеності інформації на об'єкті інформаційної діяльності та можливість (неможливість) створення на ОІД певних технічних каналів витоку інформації. **ПРН27.** Вирішувати задачі проектування та супроводу захищених інформаційних мереж та комплексів з використанням сучасних методів та технологій забезпечення інформаційної безпеки та/або кібербезпеки для забезпечення необхідного рівня захищеності на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь (відповідно до Цілей сталого розвитку 9, 11 і 16).
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Кадрове забезпечення відповідає ліцензійним вимогам. 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. В 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	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки КАІ.

8.3.	Інформаційне та навчально-методичне забезпечення	Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment). Офіційний веб-сайт www.kai.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. 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	Національна кредитна мобільність здобувачів вищої освіти, наукових і науково-педагогічних працівників, у т.ч. навчання, стажування, проведення наукових досліджень, викладання та підвищення кваліфікації організовується у рамках двосторонніх договорів між Державним університетом «Київський авіаційний інститут» та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Державним університетом «Київський авіаційний інститут» та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

2.1. Перелік компонентів

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
ОК1.	Ділова іноземна мова	3.5	Екзамен	1
ОК2.	Наукові комунікації у фаховій діяльності	3.5	Диферен-ційований залік	2

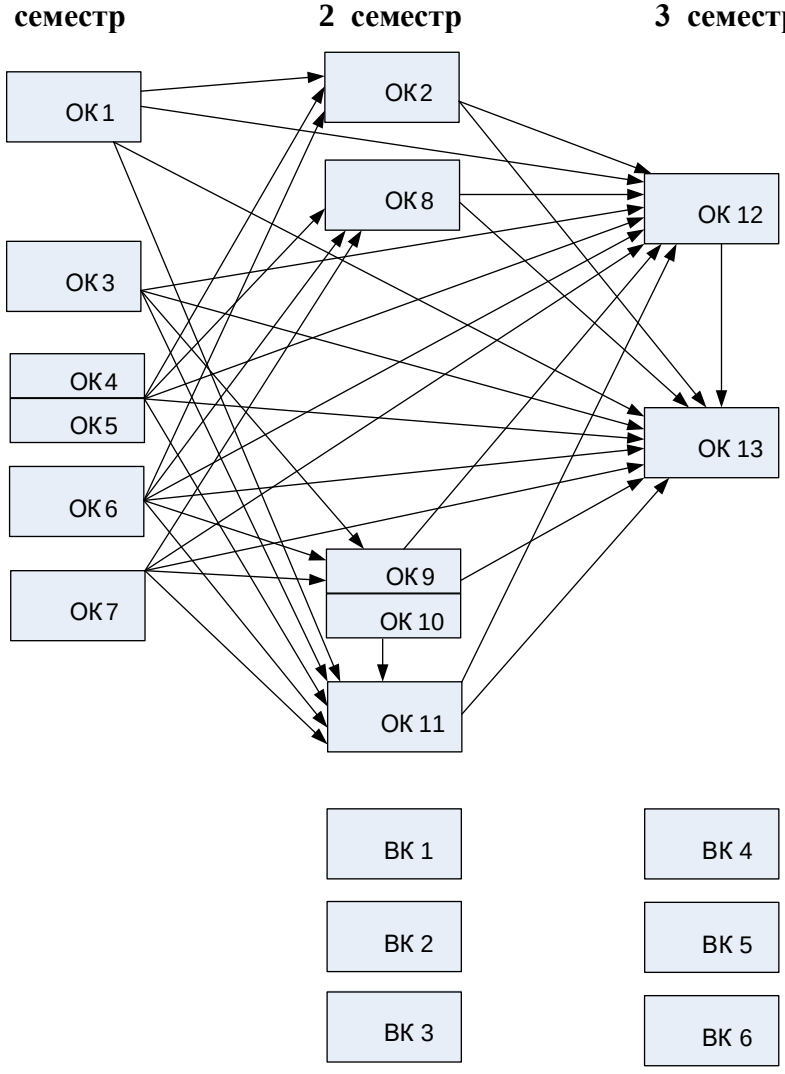
1	2	3	4	5
ОК3.	Методи побудови та аналізу криптосистем	6.0	Екзамен	1
ОК4.	Методологія прикладних досліджень у сфері кібербезпеки	6.5	Диферен-ційований залік	1
ОК5.	Курсовий проєкт з навчальної дисципліни «Методологія прикладних досліджень у сфері кібербезпеки»	1.5	Захист	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	6.0	Екзамен	1
ОК7.	Безпека в кібернетичному просторі	6.5	Диферен-ційований залік	1
ОК8.	Спеціальні вимірювання	3.5	Екзамен	2
ОК9.	Автоматизація обробки інформації з обмеженим доступом	4.0	Екзамен	2
ОК10.	Курсова робота з навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом»	1.0	Захист	2
ОК11.	Науково-дослідна практика у сфері систем технічного захисту інформації, автоматизації її обробки	6.0	Диферен-ційований залік	2
ОК12.	Переддипломна практика	9.0	Диферен-ційований залік	3
ОК13.	Кваліфікаційна робота	9.0	Захист	3
Загальний обсяг обов'язкових компонентів:		66 кредитів ЄКТС		
Вибіркові компоненти*				
ВК1.	Дисципліна 1	4.0	Диферен-ційований залік	2
ВК2.	Дисципліна 2	4.0	Диферен-ційований залік	2
ВК3.	Дисципліна 3	4.0	Диферен-ційований залік	2
ВК4.	Дисципліна 4	4.0	Диферен-ційований залік	3

1	2	3	4	5
ВК5.	Дисципліна 5	4.0	Диферен-ційований залік	3
ВК6.	Дисципліна 6	4.0	Диферен-ційований залік	3
Загальний обсяг вибіркових компонентів*		24 кредити 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 ДУ «КАІ».*

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 здобувачів освітнього ступеня «Магістр» здійснюється у формі публічного захисту кваліфікаційної роботи і завершується видачою документу встановленого зразку про присудження їм освітнього ступеня «Магістр» із присвоєнням освітньої кваліфікації: «Магістр з кібербезпеки та захисту інформації», за спеціальністю F5 «Кібербезпека та захист інформації».
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки та захисту інформації, передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) Державного університету «Київський авіаційний інститут» або його структурного підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.
Вимоги до публічного захисту (демонстрації)	Публічний захист кваліфікаційної магістерської роботи відбувається на засіданні екзаменаційної комісії. Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	**ОК1**	**ОК2**	**ОК3**	**ОК4**	**ОК5**	**ОК6**	**ОК7**	**ОК8**	**ОК9**	**ОК10**	**ОК11**	**ОК12**	**ОК13**	**ВК1**	**ВК2**	**ВК3**	**ВК4**	**ВК5**	**ВК6**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ІК1	+	+	+	+	+	+	+	+	+	+	+	+	+						
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+						
ЗК2	+	+	+	+	+	+	+	+			+	+	+						
ЗК3		+	+	+	+	+	+				+	+	+						
ЗК4		+		+	+	+	+	+	+	+	+	+	+						
ЗК5	+	+				+	+	+	+	+	+	+	+						
ФК1	+	+	+			+	+				+	+	+						
ФК2	+		+	+	+	+	+	+	+	+	+	+	+						

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ФК3			+	+	+	+	+	+			+	+	+						
ФК4	+					+	+		+	+	+	+	+						
ФК5		+				+	+	+			+	+	+						
ФК6			+			+	+		+	+	+	+	+						
ФК7						+	+	+			+	+	+						
ФК8			+					+			+	+	+						
ФК9						+	+				+	+	+						
ФК10	+	+		+	+	+	+	+	+	+	+	+	+						
ФК11						+	+				+	+	+						
ФК12						+	+				+	+	+						
ФК13							+	+			+	+	+						
ФК14						+	+				+	+	+						

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

Компоненти / Програмні результати навчання	**ОК1**	**ОК2**	**ОК3**	**ОК4**	**ОК5**	**ОК6**	**ОК7**	**ОК8**	**ОК9**	**ОК10**	**ОК11**	**ОК12**	**ОК13**	**ВК1**	**ВК2**	**ВК3**	**ВК4**	**ВК5**	**ВК6**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ПРН1	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН2	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН3		+	+	+	+			+			+	+	+						
ПРН4		+	+			+	+		+	+	+	+	+						
ПРН5				+	+	+	+	+			+	+	+						
ПРН6			+			+	+	+	+	+	+	+	+						
ПРН7	+			+	+	+	+	+	+	+	+	+	+						
ПРН8				+	+		+		+	+	+	+	+						
ПРН9			+			+	+		+	+	+	+	+						
ПРН10						+	+	+	+	+	+	+	+						
ПРН11						+	+		+	+	+	+	+						
ПРН12						+	+				+	+	+						
ПРН13			+								+	+	+						
ПРН14						+	+		+	+	+	+	+						
ПРН15		+		+	+	+	+	+	+	+	+	+	+						
ПРН16		+		+	+	+	+				+	+	+						
ПРН17	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН18		+		+	+	+	+				+	+	+						
ПРН19	+	+	+	+	+	+	+				+	+	+						

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ПРН20	+	+	+	+	+	+	+	+			+	+	+						
ПРН21						+	+	+			+	+	+						
ПРН22		+						+			+	+	+						
ПРН23	+		+	+	+	+	+	+	+	+	+	+	+						
ПРН24						+	+				+	+	+						
ПРН25							+	+			+	+	+						
ПРН26						+	+	+			+	+	+						
ПРН27						+	+				+	+	+						

6. Система внутрішнього забезпечення якості вищої освіти НАУ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та освітньої діяльності КАІ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 № 1556-VII (із 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» для другого (магістерського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 18.03.2021 № 332 (із змінами).
8. Положення про освітні програми Національного авіаційного університету, погоджено Радою з якості НАУ (протокол від 28.04.2020 № 2) та уведено в дію наказом ректора від 07.05.2020 № 148/од.

(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 ознайомлення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ 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	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				