ПРОЄКТ

(Ф 03.02 – 107)

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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Безпека інформаційних і комунікаційних систем»

(найменування освітньої програми)

Першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»

(код і найменування спеціальності)

галузі знань F «Інформаційні технології»

(шифр і найменування галузі знань)

КАІ ОП Б ID68644 – 02 – 2026

Освітньо-професійна програма
затверджена Вченою радою КАІ
Протокол № __ від ___ _____ 2026 р.
Вводиться в дію наказом президента КАІ
від ___ _____ 2026 р. № _____

Президент Ксенія СЕМЕНОВА

КИЇВ

Враховано Стандарт вищої освіти України: перший (бакалаврський) 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 04.10.2018 №1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 р. № 1547).

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою КАІ
протокол №_____
від «_____» _____2026 р.

Голова НМР КАІ, проректор
з навчальної роботи та якості освіти
Лариса ШАУЛЬСЬКА

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 кібербезпеки
протокол засідання №_____
від «_____»_____2025 р.

Завідувач кафедри кібербезпеки
Анна ІЛЬЄНКО

ПОГОДЖЕНО

Студентською радою факультету
комп'ютерних наук та технологій
протокол №_____
від «_____»_____2025 р.

Голова Студентської ради факультету
Орина БОЛИЧОВА

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності F5 «Кібербезпека та захист інформації», рік вступу – 2026-й та наступні до нової редакції освітньої програми) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

Олена ВИСОЦЬКА	к.т.н., доцент кафедри кібербезпеки

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Анна ІЛЬЄНКО	к.т.н., доцент, завідувач кафедри кібербезпеки
Володимир АХРАМОВИЧ	д.т.н., професор, професор кафедри кібербезпеки
Андрій ПЕТРЕНКО	к.т.н., доцент, доцент кафедри кібербезпеки
Софія ЛИСЮК	здобувачка вищої освіти за освітньою програмою, група Б-125-24-1-БІ
Каміла ТАРАНЕНКО	здобувачка вищої освіти за освітньою програмою, група Б-125-23-1-БІ

ЗОВНІШНІ СТЕЙКГОЛДЕРИ

Павло СКЛАДАННИЙ	к.т.н., доцент, завідувач кафедри інформаційної та кібернетичної безпеки ім. проф. Володимира Бурячка Київського столичного університету ім. Бориса Грінченка
Олександр ІЛЛЮША	директор ТОВ «Центр інформаційної та технічної підтримки «Сапфоріс»
В’ячеслав КУЛІУШ	Начальник Управління протидії кіберзлочинам в м.Києві Департаменту кіберполіції Національної поліції України, полковник поліції

Рецензії-відгуки зовнішніх стейкголдерів (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	Національний університет «Київський авіаційний інститут». Факультет комп'ютерних наук та технологій Кафедра кібербезпеки
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Освітній ступінь бакалавра. Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації.
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем».
1.4.	Тип диплому, обсяг освітньо-професійної програми, форми здобуття освіти та розрахункові строки виконання освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС. Очна (денна), заочна форми здобуття освіти. Розрахункові строки виконання освітньої програми: – 4 роки (денна форма здобуття освіти); – 4 роки (заочна форма здобуття освіти)
1.5.	Акредитаційна інституція	Акредитовано, Акредитаційна комісія Міністерства освіти і науки України, сертифікат про акредитацію НД 1193809 від 31 жовтня 2017 року
1.6.	Період акредитації	До 01.07.2027.
1.7.	Цикл/рівень	6 рівень Національної рамки кваліфікацій України (НРК України), перший цикл Європейського простору вищої освіти (FQ-EHEA), 6 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL)
1.8.	Передумови (вимоги до освіти осіб, які можуть розпочати навчання за освітньою програмою)	Вступ на навчання на освітньо-професійну програму обсягом 240 кредитів ЄКТС здійснюється на базі повної загальної середньої освіти. На базі здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством. Умови вступу регулюються Правилами прийому до КАІ.

1.9.	Мови викладання	Українська
1.10.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	https://kai.edu.ua/ https://kszi.kai.edu.ua/
Розділ 2. Мета (цілі) освітньо-професійної програми		
2.1.	**Мета освітньо-професійної програми** – підготовка висококваліфікованих, конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації, здатних розробляти, впроваджувати та вдосконалювати сучасні рішення із забезпечення безпеки інформаційних і комунікаційних систем, зокрема в авіаційній та інших критично важливих галузях. Програма спрямована на формування лідерських і професійних компетентностей, розвиток культури добропорядності та відповідальності, генерацію нових знань і впровадження інноваційних технологій, що забезпечують зміцнення кіберстійкості держави з урахуванням специфіки авіаційної галузі, сприяють технологічному прогресу та утвердженню лідерства України у глобальному цифровому середовищі.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об’єкт діяльності, теоретичний зміст)	**Об’єкти:** - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; - об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної області:** принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, 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:** методи, методики та технології розв’язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).

3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію, спрямовану на набуття студентами знань, умінь, навичок та компетентностей, необхідних для успішної професійної діяльності в галузі кібербезпеки та захисту інформації. Вона базується на загальновизнаних наукових результатах та сучасних інформаційних технологіях, що забезпечують можливості для подальшого професійного розвитку та навчання.
3.3.	Основний фокус освітньо-професійної програми	Підготовка фахівців з вищою освітою на першому (бакалаврському) рівні за спеціальністю F5 «Кібербезпека та захист інформації». Підготовка висококваліфікованих фахівців у сфері кібербезпеки, здатних розробляти, впроваджувати та підтримувати комплексні системи захисту інформаційних і комунікаційних систем для об'єктів критичної інфраструктури, зокрема авіаційної галузі та народного господарства, відповідно до міжнародних стандартів та вимог. Програма передбачає опанування сучасних інформаційно-комунікаційних технологій, а також використання сучасного програмно-апаратного забезпечення для забезпечення безпеки та захисту інформації. Ключові слова: Кібербезпека, криптографія, захист інформації, кіберзагрози, авіаційна безпека, технічний захист інформації, інформаційні системи, стеганографія, інцидент-менеджмент, управління ризиками, інформаційна безпека.
3.4.	Особливості освітньо-професійної програми	Освітньо-професійна програма спрямована на підготовку фахівців, здатних забезпечувати кібербезпеку інформаційних і комунікаційних систем завдяки глибоким знанням у криптографії, технічному захисті інформації та управлінні ризиками, що відповідає міжнародним стандартам і законодавчим вимогам. Вона поєднує фундаментальні математичні, технічні та управлінські компетентності з практичними навичками виявлення, аналізу та протидії кіберзагрозам, включаючи цифрову криміналістику та реагування на інциденти. Особливістю програми є її авіаційна спрямованість, що дозволяє випускникам реалізовувати захист критичних інформаційних систем авіаційної галузі, а також адаптуватися до нових викликів у сфері кібербезпеки завдяки постійному розвитку компетенцій.

		Відмінність програми – реалізація моделі підготовки фахівців в сфері безпеки інформаційних і комунікаційних систем 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. Можливості працевлаштування та подальшого навчання випускників		
4.1.	Можливості працевлаштування	На посади у структурних підрозділах установ/ підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації» (125 «Кібербезпека та захист інформації»).
4.2.	Подальше навчання	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуальнотворчий підхід; навчання через лекції, лабораторні роботи, семінари, практичні заняття, консультації з викладачами, проєктну роботу в командах, навчальну та виробничі практики. **Методи, методики та технології:** методи, методики та технології розв’язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
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 розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

6.2.	Загальні компетентності (ЗК)	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності. **ЗК 3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК 4.** Здатність спілкуватися іноземною мовою. **ЗК 5.** Здатність вчитися і оволодівати сучасними знаннями. **ЗК 6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. **ЗК 7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК 8.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
6.3.	Фахові компетентності (ФК)	**ФК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **ФК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **ФК3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **ФК4.** Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **ФК5.** Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **ФК6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту

		інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). **ФК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. **ФК8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **ФК9.** Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. **ФК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. ***Додаткові фахові компетентності, пов'язані з особливостями освітньої програми:*** **ФК11.** Здатність забезпечувати кібербезпеку критичних авіаційних інформаційних систем відповідно до міжнародних стандартів та національного законодавства **ФК12.** Здатність аналізувати сигнали та процеси в інформаційних і технічних системах із застосуванням спектральних методів, методів аналізу перехідних процесів та оцінювання їх впливу на ефективність систем захисту інформації. **ФК13.** Здатність застосовувати сучасні мережеві технології та підходи для забезпечення кібербезпеки інформаційних систем. **ФК14.** Здатність проводити аналіз існуючих технологій і моделей розмежування доступу та методів і технологій ідентифікації та автентифікації і на основі проведеного аналізу здійснювати оптимальний їх вибір для застосування відповідно до політики безпеки та умов використання; здатність розробляти функції ідентифікації і автентифікації користувачів та розмежування доступу до ресурсів на основі обраних технологій. **ФК15.** Здатність розробляти та впроваджувати стратегії кібербезпеки, які сприяють забезпеченню сталого розвитку, включаючи захист критичних інформаційних систем, цифрової інфраструктури та даних від загроз.

Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	**ПРН1.** Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. **ПРН2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **ПРН3.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **ПРН4.** Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. **ПРН5.** Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **ПРН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. **ПРН7.** Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. **ПРН8.** Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. **ПРН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. **ПРН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. **ПРН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з

		урахування вимог до захисту інформації. **ПРН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. **ПРН13.** Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому. **ПРН14.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. **ПРН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **ПРН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; **ПРН17.** Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. **ПРН18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. **ПРН19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. **ПРН20.** Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити

		обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. **ПРН21.** Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах. ***Додаткові програмні результати навчання, пов'язані з особливостями освітньої програми:*** **ПРН22.** Впроваджувати та оцінювати заходи кібербезпеки у критичних авіаційних інформаційних системах відповідно до вимог міжнародних стандартів ICAO, EASA, IATA, NIST. **ПРН23.** Проводити аудит кібербезпеки критичних потоків авіаційних інформаційних систем, розробляти рекомендації щодо підвищення їх безпеки та відповідності міжнародним стандартам. **ПРН24.** Розробляти та впроваджувати політику кібербезпеки для суб'єктів авіаційної діяльності, зокрема авіакомпаній, аеропортів та підприємств. **ПРН25.** Аналізувати та обґрунтовувати вибір операційної системи з урахуванням її функціональних можливостей, рівня захисту, особливостей програмного забезпечення та безпеки користувацьких даних від зловмисних дій. **ПРН26.** Аналізувати сигнали та процеси в інформаційних і технічних системах, застосовуючи методи математичного моделювання та спектрального аналізу для забезпечення ефективності систем захисту інформації. **ПРН27.** Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних систем з урахуванням принципів схемотехніки, особливостей компонентної бази, структурних схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів **ПРН28.** Розробляти та впроваджувати програмні рішення для захисту інформації в

		інформаційно-комунікаційних системах та мережах. **ПРН29.** Аналізувати технології та моделі розмежування доступу, ідентифікації та автентифікації користувачів, здійснювати їх оптимальний вибір відповідно до політики безпеки, а також розробляти функції ідентифікації та автентифікації користувачів і контролю доступу. **ПРН30.** Впроваджувати механізми кіберстійкості та адаптивні заходи кіберзахисту відповідно до глобальних цілей сталого розвитку, сприяючи безпечному цифровому середовищу та сталому розвитку суспільства (Цілі 9,11,16 сталого розвитку).
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	Для реалізації освітньої діяльності за освітньо-професійною програмою може бути залучене за необхідності (відповідно до потреб здобувачів 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, лабораторія інтелектуального відео-спостереження та безпеки на базі штучного інтелекту AxxonSoft, навчальний центр «IT Академія», які входять до складу Факультету комп'ютерних наук та технологій КАІ (https://kszi.kai.edu.ua/materialno-tekhnichne-zabezpechennya, 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	Офіційний веб-сайт www.kai.edu.ua містить інформацію про освітні програми, навчальну,

		наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. На сайті випускової кафедри розміщено основні інформаційні матеріали (навчальні програми та плани, робочі програми) для здобувачів https://kszi.kai.edu.ua/ Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії КАІ за посиланням: https://surl.li/jstxqp Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.kai.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки КАІ: http://er.kai.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 ЕС.
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 освітніх 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				
ОК1	Університетські студії	3,0	Диф. залік	1
ОК2	Основи авіації	3,0	Диф. залік	2
ОК3	Інтенсивний курс англійської мови	8,0	Диф. залік	1
			Екзамен	2
ОК4	Фахова англійська мова	8,0	Диф. залік	3
			Екзамен	4
ОК5	Історія, філософія та етика технічного прогресу: український дискус	4,0	Диф. залік	2
ОК6	Академічна та публічна комунікація українською мовою	3,0	Диф. залік	1
ОК7	Математика для ІТ	15,0	Екзамен	1
			Диф. залік	2
			Екзамен	3
ОК8	Дискретна математика	4,0	Диф. залік	4
ОК 9	Загальна фізика	7,0	Диф. залік	1
			Екзамен	2
ОК 10	Інформаційні технології	10,0	Екзамен	1
			Диф. залік	2
ОК-11	Основи автоматизованої обробки інформації	6,0	Диф. залік	1
			Екзамен	2
ОК12	Основи кібербезпеки та захисту інформації	3,0	Екзамен	1
ОК13.1	Апаратне забезпечення інформаційних систем	5,0	Диф. залік	3
			Екзамен	4
ОК13.2	Курсова робота з навчальної дисципліни «Апаратне забезпечення інформаційних систем»	1,0	Захист	3
ОК14	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	7,0	Екзамен	5
			Екзамен	6
ОК15	Захищені комп'ютерні системи та мережі	7,0	Диф. залік	5
			Екзамен	6
ОК16	Управління інформаційною безпекою	3,0	Екзамен	6
ОК17.1	Прикладна криптологія	8,0	Диф. залік	7
			Екзамен	8
ОК17.2	Курсова робота з навчальної дисципліни «Прикладна криптологія»	1,0	Захист	7

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
ОК18	Операційні системи та технології їх захисту	7,0	Диф. залік	6
			Екзамен	7
ОК19	Системи технічного захисту інформації	3,0	Екзамен	7
ОК20	Компонентна база та схемотехніка в ІКСМ	3,0	Диф. залік	3
ОК21	Основи програмування	3,0	Екзамен	3
ОК22.1	Сигнали та процеси у системах захисту інформації	3,0	Екзамен	4
ОК22.2	Курсова робота з навчальної дисципліни «Сигнали та процеси у системах захисту інформації»	1,0	Захист	4
ОК23	Основи мережевих технологій	4,0	Диф. залік	4
ОК24.1	Технології програмування	9,0	Диф. залік	4
			Екзамен	5
ОК24.2	Курсова робота з навчальної дисципліни «Технології програмування»	1,0	Захист	5
ОК25	Завадостійке кодування в системах захисту інформації	3,0	Екзамен	5
ОК26	Нормативно-правове забезпечення кібербезпеки	4,0	Екзамен	5
ОК27	Програмні засоби захисту інформації	3,5	Диф. залік	8
ОК28	Комплексні системи захисту інформації	3,0	Екзамен	7
ОК29	Безпека інформаційно-комунікаційних систем та мереж	8,0	Диф. залік	7
			Екзамен	8
ОК30	Технології безпечного доступу	5,0	Екзамен	8
ОК31*	Базова загальновійськова підготовка	3,0	Визначається програмою дисципліни	4
ОК32	Фахова ознайомлювальна практика	3,0	Диф. залік	2
ОК33	Комп'ютерна практика	3,0	Диф. залік	4
ОК34	Технологічна практика	3,0	Диф. залік	6
ОК35	Єдиний державний кваліфікаційний іспит	1,5		8
Загальний обсяг обов'язкових компонентів:		**180 кредитів ЄКТС**		
Вибіркові компоненти**				
ВК1	Дисципліна 1	4,0	Диф. залік	3
ВК2	Дисципліна 2	4,0	Диф. залік	3
ВК3	Дисципліна 3	4,0	Диф. залік	3
ВК4	Дисципліна 4	4,0	Диф. залік	5
ВК5	Дисципліна 5	4,0	Диф. залік	5
ВК6	Дисципліна 6	4,0	Диф. залік	5
ВК7	Дисципліна 7	4,0	Диф. залік	6
ВК8	Дисципліна 8	4,0	Диф. залік	6

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
ВК9	Дисципліна 9	4,0	Диф. залік	6
ВК10	Дисципліна 10	4,0	Диф. залік	7
ВК11	Дисципліна 11	4,0	Диф. залік	7
ВК12	Дисципліна 12	4,0	Диф. залік	7
ВК13	Дисципліна 13	4,0	Диф. залік	8
ВК14	Дисципліна 14	4,0	Диф. залік	8
ВК15	Дисципліна 15	4,0	Диф. залік	8
Загальний обсяг вибіркових компонентів		**60 кредитів ЄКТС**		
Загальний обсяг освітньо-професійної програми		**240 кредитів ЄКТС**		

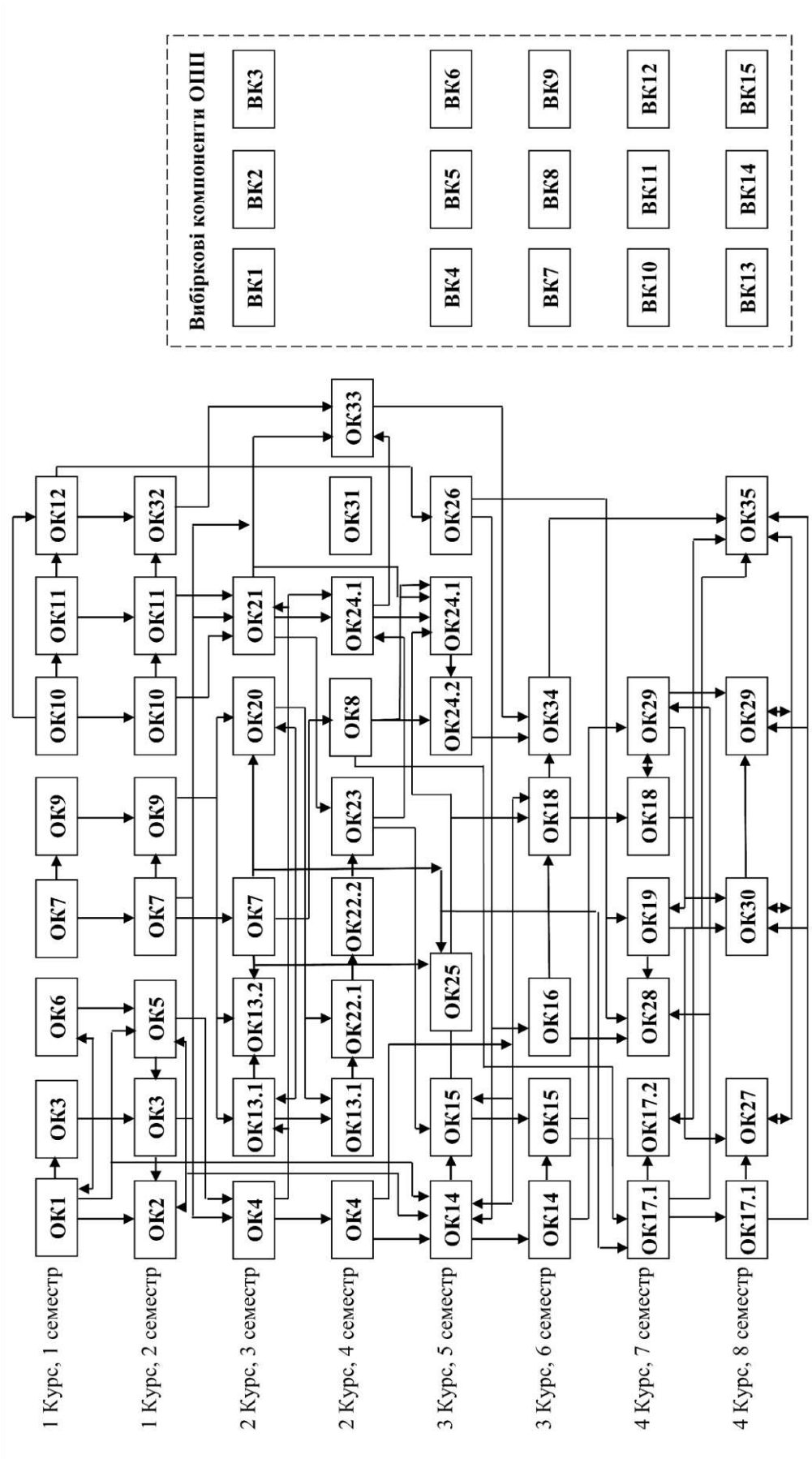
** Навчальна дисципліна «Базова загальновійськова підготовка» (ОК31) введена до освітньої програми на підставі п. 7 Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21.06.2024 № 734.*

Форми організації освітнього процесу, види навчальних занять, кількість годин, відведених на їх опанування, форми та засоби поточного і підсумкового контролю визначаються програмою навчальної дисципліни, яка розробляється на основі типової програми навчальної дисципліни «Базова загальновійськова підготовка», розробленої та затвердженої Генеральним штабом Збройних Сил України за погодженням з Міністерством освіти і науки України (з урахуванням норм постанови Кабінету Міністрів України від 21.06.2024 № 734).

Здобувачі вищої освіти, для яких проходження базової загальновійськової підготовки не є обов'язковим і які в таких випадках не проходять її добровільно (з урахуванням норм постанови Кабінету Міністрів України від 21.06.2024 № 734), вивчають дисципліни, формування переліку яких визначається внутрішніми нормативними актами КАІ

*** Реалізація права здобувачів вищої освіти на вибір освітніх компонентів та створення індивідуальної освітньої траєкторії регламентується законодавством України та внутрішніми нормативними актами КАІ.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти та освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13.1	ОК13.2	ОК14	ОК15	ОК16	ОК17.1	ОК17.2	ОК18	ОК19	ОК20	ОК21	ОК22.1	ОК22.2	ОК23	ОК24.1	ОК24.2	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35*	ВК1	…	ВК15
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	Визначаються згідно з п.8 Порядку, затвердженого постановою КМУ від 21.06.2024 № 734	+	+	+	*			
ЗК1	+	+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	*			
ЗК2	+	+			+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+		+	+	+	*			
ЗК3						+																													+	+	+	*			
ЗК4			+	+																																		*			
ЗК5	+	+	+	+	+	+	+	+	+	+	+		+	+	+			+	+			+			+		+	+			+		+	+	+	+	+	*			
ЗК6	+	+			+	+											+													+		+			+			*			
ЗК7	+				+										+								+			+									+		+	*			
ЗК8	+	+			+	+											+	+	+	+	+	+		+	+					+								*			
ФК1												+			+		+			+										+	+	+			+		+	*			
ФК2										+	+		+	+	+	+	+			+		+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	*			
ФК3																	+						+									+					+	*			
ФК4										+	+				+	+	+				+		+			+	+	+		+	+	+	+	+		+	+	*			
ФК5															+	+	+			+						+	+	+			+		+	+			+	+	*			
ФК6													+	+	+						+									+	+	+				+	+	*			
ФК7															+		+					+									+	+					+	*			
ФК8																		+	+																		+	*			
ФК9													+	+	+																						+	*			
ФК10															+		+				+		+			+	+	+			+		+	+			+	+	*			
ФК11															+																								*			
ФК12																								+	+														*			
ФК13																										+													*			
ФК14																																		+					*			
ФК15															+	+															+	+	+	+					*			

Примітка.

Згідно з п. 8 Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21.06.2024 № 734, сукупність вимог до змісту та результатів освітньої діяльності (відповідно і результатів навчання), пов'язаних з базовою загальновійськовою підготовкою (ОК31), визначаються типовою програмою навчальної дисципліни "Базова загальновійськова підготовка", яка розробляється та затверджується Генеральним штабом Збройних Сил України за погодженням з Міністерством освіти і науки України.

Якщо передбачається проведення ЄДКІ, то вказуємо примітку:

**Визначається програмою єдиного державного кваліфікаційного іспиту з урахуванням статті 6 Закону України «Про вищу освіту» .*

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

Компоненти / Прогр. результати навчання	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13.1	ОК13.2	ОК14	ОК15	ОК16	ОК17.1	ОК17.2	ОК18	ОК19	ОК20	ОК21	ОК22.1	ОК22.2	ОК23	ОК24.1	ОК24.2	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35*	ВК1	…	ВК15
ПРН1						+																																*			
ПРН2			+	+																																		*			
ПРН3					+																																	*			
ПРН4	+	+				+	+	+	+	+	+	+			+	+		+	+	+		+							+		+	+	+	+		+	+	+	*			
ПРН5	+				+		+	+	+	+	+	+			+	+													+		+	+	+	+		+	+	+	*			
ПРН6	+	+			+	+				+		+			+	+																+			+			+	*			
ПРН7							+	+	+	+	+		+	+	+			+	+		+			+	+				+		+						+		*			
ПРН8							+	+	+	+	+																		+				+	+			+		*			
ПРН9												+			+		+													+		+			+				*			
ПРН10										+	+	+	+	+	+	+	+						+	+	+	+	+	+			+	+	+	+	+	+	+	+	*			
ПРН11																	+									+						+							*			
ПРН12											+		+	+	+	+	+				+		+			+	+	+		+	+	+	+	+	+		+	+	*			
ПРН13													+	+		+	+				+		+			+	+	+			+	+					+	+	*			
ПРН14															+	+	+			+			+			+	+	+										+	*			
ПРН15															+	+	+						+			+	+	+					+	+				+	*			
ПРН16															+						+									+		+						+	*			
ПРН17															+		+																+						+	*			
ПРН18															+			+	+													+							*			

Визначаються згідно з п.8 Порядку, затвердженого постановою КМУ від 21.06.2024 № 734

Компоненти / Прогр. результати навчання	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13.1	ОК13.2	ОК14	ОК15	ОК16	ОК17.1	ОК17.2	ОК18	ОК19	ОК20	ОК21	ОК22.1	ОК22.2	ОК23	ОК24.1	ОК24.2	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35*	ВК1	…	ВК15
ПРН19																		+	+																Визначаються згідно з п.8 Порядку, затвердженого постановою КМУ від 21.06.2024 № 734			+	*			
ПРН20															+						+																+	*			
ПРН21															+		+				+		+			+	+	+			+		+	+			+	*			
ПРН22															+																							*			
ПРН23															+																							*			
ПРН24															+																							*			
ПРН25																				+																		*			
ПРН26																								+	+														*			
ПРН27																						+																+	*			
ПРН28																							+															+	*			
ПРН29																																			+			+	*			
ПРН30							+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+					*			

Примітка.
Згідно з п. 8 Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21.06.2024 № 734, сукупність вимог до змісту та результатів освітньої діяльності (відповідно і результатів навчання), пов'язаних з базовою загальновійськовою підготовкою (ОК31), визначаються типовою програмою навчальної дисципліни "Базова загальновійськова підготовка", яка розробляється та затверджується Генеральним штабом Збройних Сил України за погодженням з Міністерством освіти і науки України.

**Визначається програмою єдиного державного кваліфікаційного іспиту з урахуванням статті 6 Закону України «Про вищу освіту» .*

6. Система внутрішнього забезпечення якості вищої освіти КАІ

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. Стандарт вищої освіти зі спеціальності 125 Кібербезпека та захист інформації 12 Інформаційні технології для першого (бакалаврського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 29.10.2024 № 1547.
5. 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
6. 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
7. International Civil Aviation Organization. (2022). Annex 17 to the Convention on International Civil Aviation: Security—Safeguarding international civil aviation against acts of unlawful interference (12 ed.). ICAO.
8. Наказ Міністерства освіти і науки України від 19.11.2024 № 1625 «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021» (із змінами) [Електронний ресурс]. – режим доступу: https://ips.ligazakon.net/document/re43178?an=1
9. Наказ Міністерства освіти і науки України від 15.05.2024 №686 «Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти» [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/z1013-24#Text