

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



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи та технології кібербезпеки»

Першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»


галузі знань F «Інформаційні технології»

СМЯ КАІ ОП Б ID65459 – 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

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ КАІ ОП Б ID65459– 01 – 2025</p>
	<p align="right">стор. 2 з 25</p>		

Враховано Стандарт вищої освіти України: перший (бакалаврський) рівень,
галузь знань 12 Інформаційні технології
спеціальність 125 Кібербезпека та захист інформації

Стандарт вищої освіти України затверджено і введено в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547

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 «_____» _____ 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

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ КАІ ОП Б ID65459– 01 – 2025</p>
	<p align="right">стор. 3 з 25</p>		

ПЕРЕДМОВА

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

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

<p><i>Приходько Тетяна Юріївна</i> <i>к.т.н., доцент кафедри технічного захисту інформації</i></p>	<hr/> <p>(підпис)</p>
---	-----------------------

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

<p><i>Козловський Валерій Валерійович</i> <i>д.т.н., професор, завідувач кафедри технічного захисту інформації</i></p>	<hr/> <p>(підпис)</p>
---	-----------------------

<p><i>Зибін Сергій Вікторович</i> <i>д.т.н., професор кафедри технічного захисту інформації</i></p>	<hr/> <p>(підпис)</p>
--	-----------------------

<p><i>Іванченко Ігор Сергійович</i> <i>к.т.н., доцент кафедри технічного захисту інформації</i></p>	<hr/> <p>(підпис)</p>
--	-----------------------

<p><i>прізвище, ім'я, по батькові</i> <i>здобувач(ка) вищої освіти за освітньою програмою, група...</i></p>	<hr/> <p>(підпис)</p>
--	-----------------------


ЗОВНІШНІ СТЕЙКГОЛДЕРИ

<p><i>Савченко Віталій Анатолійович</i> <i>д.т.н., професор, професор кафедри управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій</i></p>	<hr/> <p>(підпис)</p>
---	-----------------------

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).


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

Контрольний примірник

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ КАІ ОП Б ID65459- 01 – 2025</p>
	<p>стор. 4 з 25</p>		

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут». Факультет комп'ютерних наук та технологій Кафедра технічного захисту інформації
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	Системи та технології кібербезпеки
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	Акредитаційна інституція Міністерство освіти і науки України, рішення Акредитаційної комісії від 31.10.2017 сертифікат серія НД № 1193809
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 ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані в межах попередньої освітньої програми молодшого бакалавра (молодшого спеціаліста), обсягом не більше ніж 120 кредитів ЄКТС. На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти. Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-

	<p style="text-align: center;">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ КАІ ОП Б ID65459- 01 – 2025
		стор. 5 з 25	


		кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством Умови вступу регулюються Правилами прийому до КАІ.
1.9.	Мови викладання	<i>Українська, англійська</i>
1.10.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://kai.edu.ua

Розділ 2. Мета (цілі) освітньо-професійної програми


2.1.	Ціль освітньої програми полягає в підготовці висококваліфікованих та конкурентоспроможних фахівців з ґрунтованими компетентностями у розробці та впровадженні сучасних систем та технологій кібербезпеки здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу. ОПІ «Системи та технології кібербезпеки» відповідає місії та цілям КАІ, щодо внеску КАІ у розвиток суспільства через генерацію нових знань і надання високоякісних освітніх послуг при підготовці фахівців з кібербезпеки в авіаційно-космічній галузі.
------	---

Розділ 3. Характеристика освітньо-професійної програми


3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	<p>Об'єкт:</p> <ul style="list-style-type: none"> - 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. <p>Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації;</p> <p>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.</p> <p>Методи, методики та технології: методи, методики та технології розв'язанні теоретичних і практичних задач кібербезпеки та захисту інформації</p> <p>Інструменти та обладнання:</p>
-----	--	--

	<p style="text-align: center;">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ КАІ ОП Б ID65459- 01 – 2025
		стор. 6 з 25	


		засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформативні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма прикладної орієнтації, що базується на загальновідомих наукових і практичних результатах в галузі інформаційної безпеки, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми	Загальна вища освіта першого (бакалаврського) рівня спеціальності 125 Кібербезпека та захист інформації. Програма спрямована на підготовку висококваліфікованих фахівців у сфері кібербезпеки, здатних розробляти, впроваджувати та підтримувати комплексні системи захисту інформаційних і комунікаційних систем із урахуванням специфіки авіаційної галузі. Ключові слова: кібербезпека, інформаційна безпека, системи та технології кібербезпеки, криптографічний захист інформації, технічний захист інформації, захист персональних даних, антивірусний захист, захист від несанкціонованого доступу, кібербезпека провідних та безпроводових мереж.
3.4.	Особливості освітньо-професійної програми	Освітньо-професійна програма передбачає вивчення: <ul style="list-style-type: none"> – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем кібербезпеки; – теорії, методів і моделей управління доступом до інформаційних ресурсів; – теорії систем управління кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків кібербезпеки; – методів та засобів оцінювання і забезпечення необхідного рівня кібербезпеки; – методів і засобів технічного та криптографічного захисту інформації; – захищених інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення систем кібербезпеки тощо.

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ КАІ ОП Б ID65459- 01 – 2025</p>
	<p align="right">стор. 7 з 25</p>		

		<p>Постійний та систематичний моніторинг ринку освітніх послуг, аналіз вакансій і потенційних можливостей ринку праці, експертне опитування керівників і провідних спеціалістів підприємств різних форм власності стали основою з підготовки фахівців освітньо-професійної програми «Системи та технології кібербезпеки». Проведений аналіз показав необхідність продовжувати формування та реалізацію моделі підготовки фахівців здатних використовувати і впроваджувати сучасні системи та технології кібербезпеки, які володіють знаннями механізмів забезпечення безпеки та ефективними засобами обмежень ризиків в інформаційних системах. Це забезпечує можливість отримання якісної професійної освіти в галузі ІТ та робить вказану ОПП унікальною.</p>
<p>Розділ 4. Можливості працевлаштування та подальшого навчання випускників</p>		
4.1.	Можливості працевлаштування	<p>Випускники отримують можливість працевлаштування на посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти за спеціальності F5 Кібербезпека та захист інформації.</p>
4.2.	Подальше навчання	<p>Випускники мають право на здобуття освіти на другому (магістерському) рівні вищої освіти та здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.</p>
<p>Розділ 5. Викладання та оцінювання</p>		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	<p>Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід; навчання через лекції, лабораторні роботи, семінари, практичні заняття, консультації з викладачами, проектну роботу в командах, навчальну та виробничі практики.</p>
5.2.	Оцінювання	<p>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.</p>
<p>Розділ 6. Програмні компетентності</p>		
6.1.	Інтегральна компетентність (ІК)	<p>Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації</p>

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ KAI ОП Б ID65459– 01 – 2025</p>
	<p align="right">стор. 8 з 25</p>		

6.2.	Загальні компетентності (ЗК)	<p>ЗК1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності</p> <p>ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово</p> <p>ЗК4. Здатність спілкуватися іноземною мовою.</p> <p>ЗК5. Здатність вчитися і оволодівати сучасними знаннями.</p> <p>ЗК6. Здатність реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права та свободи людини і громадянина в Україні.</p> <p>ЗК7. Здатність ухвалювати рішення й діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.</p> <p>ЗК8. 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.</p>
6.3.	Фахові компетентності (ФК)	<p>ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.</p> <p>ФК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.</p> <p>ФК3. Здатність забезпечувати неперервність бізнес-процесіву згідно встановленої політики кібербезпеки та захисту інформації.</p> <p>ФК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p>ФК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>ФК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту</p>

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ КАІ ОП Б ID65459- 01 – 2025</p>
	<p align="right">стор. 9 з 25</p>		

		<p>інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).</p> <p>ФК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p>ФК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності</p> <p>ФК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.</p> <p>Додаткові фахові компетентності, пов'язані з особливостями освітньої програми:</p> <p>ФК11. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності.</p> <p>ФК12. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності та в інформаційно-комунікаційних системах.</p> <p>ФК13. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв.</p> <p>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.</p>
<p>Розділ 7. Програмні результати навчання</p>		
7.1.	Програмні результати навчання (ПРН)	<p>ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.</p> <p>ПРН2. Спілкування іноземною мовою з метою забезпечення ефективності професійної комунікації.</p> <p>ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів</p>

недобросовісності у професійній діяльності.

ПРН4. Організувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язування 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 і розуміння математики та фізики в професійній діяльності, формувати задачі предметної галузі кібернетики 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 захисту інформації для здійснення професійної діяльності.

ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організації згідно з встановленою політикою кібербезпеки з урахуванням 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 і 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 і відновлення інформації.

ПРН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлювання 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. Визначати відомості, які відносяться до інформації з обмеженим доступом, організувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.

ПРН23. Організувати внутрішньо-об'єктовий та пропускний режими на підприємстві.

ПРН24. Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об'єкті інформаційної діяльності.

ПРН25. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН26. Виявляти закладні пристрої несанкціонованого отримання інформації.

ПРН27. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки.


ПРН28. Виявляти небезпечні сигнали технічних засобів.

ПРН29. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-комунікаційних систем.


ПРН30. Розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації.

ПРН31. Визначати показники захищеності інформації на об'єкті інформаційної діяльності та можливість (неможливість) створення на ОІД певних технічних каналів витоку інформації.

ПРН32. Аналізувати технології і моделі розмежування доступу до ресурсів інформаційних систем та здійснювати їх оптимальний вибір відповідно до політики безпеки конкретної організації і умов використання системи.

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	<p align="center">Шифр документа</p>	<p align="center">СМЯ КАІ ОП Б ID65459- 01 – 2025</p>
	<p align="right">стор. 13 з 25</p>		


		<p>ПРНЗЗ. Аналізувати методи і технології ідентифікації та автентифікації користувачів інформаційних систем і досліджувати доцільність їх використання</p>
<p align="center">Розділ 8. Ресурсне забезпечення реалізації програми</p>		
8.1.	Кадрове забезпечення	<p>Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напрямку 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.</p>
8.2.	Матеріально-технічне забезпечення	<p>Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.</p>
8.3.	Інформаційне та навчально-методичне забезпечення	<p>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 КАІ за посиланням: https://surl.li/jstxqp 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 КАІ: http://er.nau.edu.ua</p>
<p align="center">Розділ 9. Академічна мобільність</p>		
9.1.	Національна кредитна мобільність	<p>У рамках двосторонніх договорів між ДУ «Київський авіаційний інститут» та вітчизняними закладами вищої освіти.</p>
9.2.	Міжнародна кредитна мобільність	<p>У рамках Еразмус+К1 договір про співробітництво між ДУ «Київський авіаційний інститут» та навчальними закладами ЕС.</p>
9.3.	Навчання іноземних здобувачів вищої освіти	<p>Створено умови для навчання іноземних здобувачів вищої освіти.</p>

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП Б ID65459-01 – 2025
		стор. 14 з 25	

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 проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
OK1.	Історія української державності та культури	3,0	Екзамен	1
OK2.	Ділова українська мова	3,0	Екзамен	2
OK3.	Фахова іноземна мова	4,5	Диф. залік	1
			Екзамен	2
OK4.	Філософія	3,5	Екзамен	4
OK6.	Вища математика	14,0	Диф. залік	2
			Екзамен	3
			Екзамен	1
OK7.	Фізика	10,5	Диф. залік	1
			Екзамен	2
OK8.	Інформаційні технології	11,5	Екзамен	1
			Диф. залік	2
OK9.	Основи автоматизованої обробки інформації	6,5	Диф. залік	1, 2
OK10.	Основи кібербезпеки	4,5	Диф. залік	1
OK11.1	Апаратне забезпечення інформаційних систем	5,0	Диф. залік	3
			Екзамен	4
OK11.2	Курсова робота з дисципліни Апаратне забезпечення інформаційних систем	1,0	Захист	3
OK12.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	8,5	Екзамен	5, 6
OK13.	Захищені комп'ютерні системи та мережі	7,5	Диф. залік	5
			Екзамен	6
OK14.1	Управління інформаційною безпекою	3,0	Екзамен	6
OK14.2	Курсова робота з дисципліни «Управління інформаційною безпекою»	1,0	Захист	6
OK15.1	Прикладна криптологія	7,0	Диф. залік	7
			Екзамен	8
OK15.2	Курсова робота з дисципліни «Прикладна криптологія»	1,0	Захист	7
OK16.	Операційні системи та технології їх захисту	6,5	Диф. залік	6
			Екзамен	7
OK17.	Системи технічного захисту інформації	3,0	Екзамен	7

	<p style="text-align: center;">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ KAI ОП Б ID65459- 01 – 2025
		стор. 15 з 25	

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
OK18.1	Технології програмування	8,5	Екзамен	3, 4
OK18.2	Курсова робота з дисципліни «Технології програмування»	1,0	Захист	4
OK19.	Дискретна математика	9,0	Екзамен	3
			Диф. залік	4
OK20.	Технології виявлення уразливостей інформаційних систем	3,5	Диф. залік	4
OK21.1	Ризик-менеджмент інформаційної безпеки	4,5	Екзамен	5
OK21.2	Курсова робота з дисципліни «Ризик-менеджмент інформаційної безпеки»	1,0	Захист	5
OK22.	Криміналістичний аналіз сфери кібербезпеки	4,0	Екзамен	5
OK23.	Веб-програмування та інтернет-протоколи	3,5	Диф. залік	7
OK24.1	Комплексні системи захисту інформації	4,0	Екзамен	8
OK24.2	Курсовий проект з дисципліни «Комплексні системи захисту інформації»	1,5	Захист	8
OK25.	Оцінювання та тестування стану безпеки інформаційних систем	4,0	Екзамен	8
OK26.	Управління інцидентами інформаційної безпеки	4,0	Екзамен	7
OK27.	Безпекові технології штучного інтелекту	3,5	Диф. залік	8
OK28*	Базова загальновійськова підготовка	10,0	Визначається програмою дисципліни	4
OK29.	Фахово-ознайомлювальна практика	3,0	Диф. залік	2
OK30.	Комп'ютерна практика	3,0	Диф. залік	4
OK31.	Технологічна практика	3,0	Диф. залік	6
OK32.	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
ВК9	Дисципліна 9	4,0	Диф. залік	6
ВК10	Дисципліна 10	4,0	Диф. залік	7

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ КАІ ОП Б ID65459- 01 – 2025
	стор. 16 з 25		

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 вибіркового компонента		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		240 кредитів ЄКТС		

Примітки:

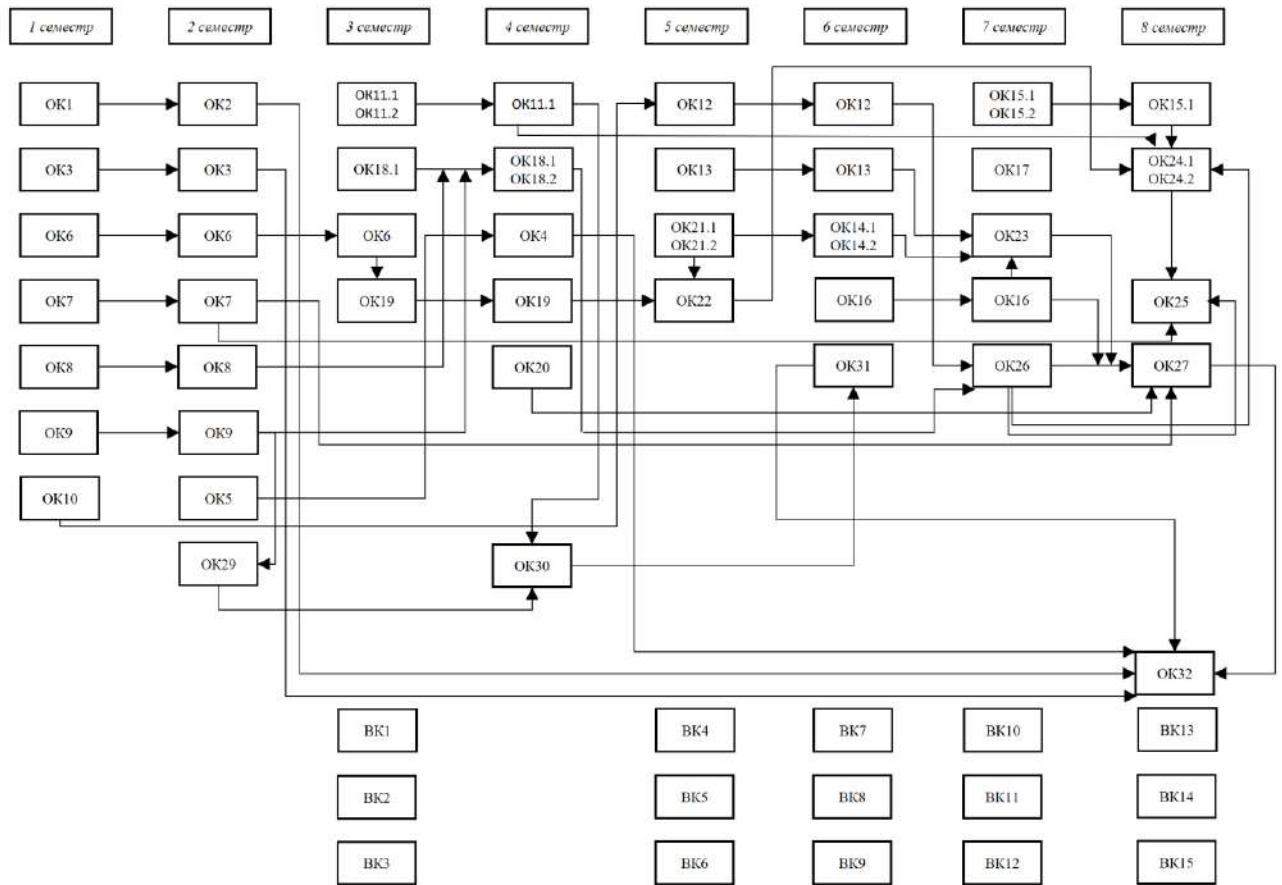
* Навчальна дисципліна «Базова загальновійськова підготовка» (ОК28) введена до освітньої програми на підставі п. 7 Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21.06.2024 № 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, які є альтернативними базовій загальновійськовій підготовці. Ці дисципліни спрямовані на додаткове (поглиблене, розширене, доповнене тощо) досягнення програмних результатів навчання та здобуття компетентностей, які відповідно досягаються та здобуваються за рахунок вивчення інших обов'язкових навчальних дисциплін освітньої програми, що передують вивченню чи вивчаються у тому ж семестрі, що й альтернативні базовій загальновійськовій підготовці навчальні дисципліни. Формування переліку навчальних дисциплін, які є альтернативними базовій загальновійськовій підготовці, визначається внутрішніми нормативними актами КАІ.

** 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 КАІ.

2.2. Структурно-логічна схема освітньо-професійної програми




**OK28. Навчальна дисципліна «Базова загальновійськова підготовка» проводиться з метою здобуття громадянами України військово-облікової спеціальності, навичок і умінь, необхідних для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України*

	<p style="text-align: center;">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ КАІ ОП Б ID65459- 01 – 2025
		стор. 18 з 25	

3. Форма атестації здобувачів вищої освіти

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

	<p>Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ КАІ ОП Б ID65459- 01 – 2025
		стор. 20 з 25	

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


*** Вибіркові компоненти обрані із каталогів рекомендованих та альтернативних вибіркових дисциплін Університету мають також забезпечувати визначені програмні результати навчання (ПРН). Кількість вибіркових компонент визначається виходячи із загального обсягу*



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

Компоненти Прогр. результати навчання	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11.1	OK11.2	OK12	OK13	OK14.1	OK14.2	OK15.1	OK15.2	OK16	OK17	OK18.1	OK18.2	OK19	OK20	OK21.1	OK21.2	OK22	OK23	OK24.1	OK24.2	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32*	ВК1	...	ВК15					
	ПРН1		+		+				+	+	+			+							+																	+	+	+	*					
ПРН2			+			+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН3		+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН4						+	+	+	+	+			+	+	+	+	+	+	+	+		+	+		+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН5	+	+	+	+		+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+				+	+	+	+	+	+	+	+	+			
ПРН6				+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ПРН7						+	+	+	+				+	+				+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН8						+	+		+	+	+	+		+				+	+		+			+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ПРН9	+	+		+				+	+	+			+		+	+			+								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ПРН10								+		+	+	+								+	+	+	+		+			+							+	+	+	+	+	+	+	+	+	+		
ПРН11								+	+	+	+	+		+	+	+			+	+		+	+				+	+			+	+				+	+	+	+	+	+	+	+	+	+	
ПРН12		+							+	+				+	+		+	+	+	+	+	+	+							+	+				+	+		+	+	+	+	+	+	+	+	
ПРН13									+	+	+	+						+	+			+	+																							
ПРН14								+	+	+			+							+	+						+	+							+	+	+	+	+	+	+	+	+	+	+	
ПРН15					+				+						+	+					+					+	+	+	+					+	+	+	+	+	+	+	+	+	+	+	+	
ПРН16									+		+	+								+	+													+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН17										+					+	+					+					+	+	+	+							+	+	+	+	+	+	+	+	+	+	
ПРН18										+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН19						+				+								+	+			+	+		+	+			+																	
ПРН20										+	+	+		+	+	+	+				+				+									+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН21														+	+						+						+						+	+	+	+	+	+	+	+	+	+	+	+	+	+

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

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»</p>	Шифр документа	СМЯ КАІ ОП Б ID65459- 01 – 2025
		стор. 23 з 25	

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-p>
4. Постанова Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» (із змінами) [Електронний ресурс]. – режим доступу: <https://zakon.rada.gov.ua/laws/show/266-2015-p>
5. Постанова Кабінету міністрів України від 21.06.2024 № 734 «Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських» [Електронний ресурс]. – режим доступу: <https://zakon.rada.gov.ua/laws/show/734-2024-%D0%BF>
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. 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
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 – 04)

АРКУШ РЕЄСТРАЦІ 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				