

ПРОЄКТ

(Ф 03.02 – 107)

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



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Системи технічного захисту інформації, автоматизація її обробки»

Першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 «Кібербезпека та захист інформації»
галузі знань F «Інформаційні технології»»

КАІ ОП ОП Б ID68646 – 02 – 2026

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

Президент Ксенія СЕМЕНОВА

КИЇВ

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	КАІ ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 2 з 24	

Враховано Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 «Інформаційні технології»; спеціальність 125 «Кібербезпека та захист інформації» (в редакції постанови Кабінету міністрів України від 16.12.2022 №1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»); Стандарт вищої освіти України затверджено і введено в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

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

Кафедрою технічного захисту інформації
Протокол № __ від __ _____ 2026 р.
Завідувач кафедри
Валерій КОЗЛОВСЬКИЙ

ПОГОДЖЕНО

Вченою радою
Факультету комп'ютерних наук та технологій
Протокол № __ від __ _____ 2026 р.
Голова Вченої ради факультету
Андрій ФЕСЕНКО

ПОГОДЖЕНО

Студентською радою Факультету
комп'ютерних наук та технологій
Протокол № __ від __ _____ 2026 р.
Голова Студентської ради факультету

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	КАІ ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 3 з 24	

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:

Володимир ТЕМНІКОВ

д.т.н., доцент, професор кафедри технічного захисту інформації Факультету комп'ютерних наук та технологій

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Валерій КОЗЛОВСЬКИЙ

д.т.н., професор, завідувач кафедри технічного захисту інформації Факультету комп'ютерних наук та технологій

Сергій ЛАЗАРЕНКО

д.т.н., професор, професор кафедри технічного захисту інформації Факультету комп'ютерних наук та технологій

Андрій МІЩЕНКО

д.т.н., професор, професор кафедри технічного захисту інформації Факультету комп'ютерних наук та технологій

здобувач вищої освіти за освітньою програмою, група Б-125-___-СЗ

ЗОВНІШНІЙ СТЕЙКГОЛДЕР

Віталій САВЧЕНКО

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

Рецензія зовнішнього стейкхолдера додається.

Рівень документа – 3б

Плановий термін між ревізіями – 1 рік

Контрольний примірник

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 4 з 24	

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 технічного захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Освітній ступінь - Бакалавр, Освітня кваліфікація - Бакалавр з кібербезпеки та захисту інформації
1.3.	Офіційна назва освітньо-професійної програми	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 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	Міністерство освіти і науки України, рішення Акредитаційної комісії від 31.10.2017 сертифікат серія НД № 1193809
1.6.	Період акредитації	До 01.07.2027 р., чергова
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)	Для здобуття освітнього ступеня бакалавра зі спеціальності «Кібербезпека та захист інформації» можуть вступати особи, які здобули повну загальну середню освіту. 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 кредити 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.

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 5 з 24	

		Умови вступу регулюються Правилами прийому до KAI.
1.9.	Мови викладання	Українська
1.10.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://kai.edu.ua http://www.kzzi.kai.edu.ua

Розділ 2. Мета (цілі) освітньо-професійної програми

2.1.	<p>Метою (цілями) освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» є:</p> <ul style="list-style-type: none"> - відтворення інтелектуального потенціалу держави; - підготовка висококваліфікованих фахівців, які володіють спеціальними знаннями та технологіями в сфері інформаційних технологій, здатні використовувати і впроваджувати технології кібербезпеки та захисту інформації, розв'язувати складні задачі у галузі кібербезпеки та захисту інформації; - опанування специфічних знань особливостей професійної діяльності в авіаційному секторі, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації. <p>Означена мета відповідає місії університету, яка визначена в Стратегії розвитку KAI 2025-2030.</p>
------	---

Розділ 3. Характеристика освітньо-професійної програми

3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	<p>Об'єкт навчання:</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 та нейтралізація реальних та потенційних загроз національній безпеці України у кіберпросторі.</p> <p>Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації.</p>
-----	--	---

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	стор. 6 з 24		

		Інструменти та обладнання: 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	Освітня програма має прикладну орієнтацію відповідно до Міжнародної стандартної класифікації освіти (ISCED 2011 / UNESCO). Базується на загальновідомих положеннях, результатах сучасних наукових досліджень та нових знаннях в галузі інформаційних технологій, необхідних для майбутньої професійної діяльності бакалаврів з кібербезпеки та захисту інформації, здатних вирішувати певні проблеми і задачі за умови оволодіння системою загальних та фахових компетентностей.
3.3.	Основний фокус освітньо-професійної програми	Вища освіта першого (бакалаврського) рівня в галузі F – 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: кібербезпека, технічний захист інформації, автоматизовані системи захисту інформації, обробка інформації з обмеженим доступом.
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 в галузі кібербезпеки та захисту інформації; – методів і засобів забезпечення кібербезпеки та захисту інформації; – методів використання систем та комплексів кібербезпеки та захисту інформації; – методів та засобів виявлення та локалізації каналів витоку інформації; – теорії, моделей та принципів управління доступом до інформаційних ресурсів;

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 7 з 24	

		<p>– автоматизованих систем обробки інформації з обмеженим доступом.</p> <p>На відміну від інших освітніх програм увага приділяється підготовці фахівців в сфері автоматизованих систем та комплексів технічного захисту інформації, а також автоматизованих систем обробки інформації з обмеженим доступом з урахуванням потреб авіаційної галузі України.</p>
--	--	---

Розділ 4. Можливості працевлаштування та подальшого навчання випускників

4.1.	Можливості працевлаштування	Випускники отримують можливість працевлаштування на посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти за спеціальності F5 Кібербезпека та захист інформації.
4.2.	Подальше навчання	Випускники мають право на здобуття освіти на другому (магістерському) рівні вищої освіти та здобуття або на 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)	<p>Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуальнотворчий підхід; навчання через лекції, лабораторні роботи, семінари, практичні заняття, виконання курсових робіт та проєктів, а також проєктну роботу в командах, навчальну та виробничі практики.</p> <p>Методи, методики та технології:</p> <p>Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення кібербезпеки та захисту інформації.</p> <p>Проблемно-орієнтоване навчання, яке передбачає формулювання та вирішення проблеми під час лекцій, розв'язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи здобувачів вищої освіти.</p> <p>Практико-орієнтоване навчання через різні види практик на підприємствах, установах та організаціях різних форм власності на підставі договорів про проходження практики, організація якої здійснюється за принципом неперервності.</p> <p>Технології дистанційного навчання, що</p>
------	--	--

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 8 з 24	

		<p>реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій; дистанційних занять, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів й інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб-технологій.</p> <p>Інформаційні технології навчання: робота здобувачів вищої освіти у спеціалізованих кабінетах облаштованих мультимедійними комплексами, що забезпечує можливість проведення інтерактивних лекцій та віртуальних лабораторних робіт, застосування пошукової методики здобуття нових знань, організації проектної роботи, проведення комп'ютеризованого тестового контролю якості знань.</p> <p>Інструменти та обладнання:</p> <ul style="list-style-type: none"> – системи розробки, забезпечення, моніторингу та контролю процесів кібербезпеки та захисту інформації; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – апаратно-програмні комплекси та засоби лінійного/просторового захисту інформації; – комбіновані системи контролю та управління доступом; – засоби технологічного, інформаційного, інструментального, метрологічного та організаційного забезпечення освітнього процесу.
5.2.	Оцінювання	Відповідно до Положення про організацію освітнього процесу в KAI, 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)	<p>ЗК1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК2. Знання та розуміння предметної області і розуміння професії.</p>



		<p>ЗК3. Здатність спілкуватися державною мовою як усно, так 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-процесів 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</p>

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 10 з 24	

		<p>функціонування комплексних систем захисту 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><i>Додаткові фахові компетентності, пов'язані з особливостями освітньої програми:</i></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>
Розділ 7. Програмні результати навчання		
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</p>



комунікації.

ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності 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 встановлюваною 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

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 13 з 24	

		<p>технічного захисту інформації.</p> <p>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.</p> <p><i>Додаткові програмні результати навчання, пов'язані з особливостями освітньої програми:</i></p> <p>ПРН22. Визначати відомості, які відносяться до інформації з обмеженим доступом, організувати допуск та доступ персоналу підприємств до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.</p> <p>ПРН23. Організувати внутрішньо-об'єктовий та пропусковий режими на об'єктах авіаційної критичної інфраструктури.</p> <p>ПРН24. Вирішувати задачі розробки та супроводу комплексних систем захисту інформації та комплексів технічного захисту інформації на авіаційних об'єктах інформаційної діяльності.</p> <p>ПРН25. Виявляти закладні пристрої несанкціонованого отримання інформації на об'єктах інформаційної діяльності.</p> <p>ПРН26. Вирішувати задачі забезпечення кібербезпеки та захисту інформації на об'єктах інформаційної діяльності на основі концепції забезпечення сталого розвитку інформаційного суспільства.</p> <p>ПРН27. Визначати показники захищеності інформації на об'єктах інформаційної діяльності.</p>
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	<p>В освітньому процесі беруть участь доктори та кандидати наук, професори та доценти, старші викладачі й асистенти за спеціальністю «Кібербезпека та захист інформації» та за іншими спеціальностями, які забезпечують підготовку бакалаврів з кібербезпеки та захисту інформації.</p> <p>До організації освітнього процесу залучаються</p>

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 14 з 24	

		професіонали з досвідом наукової, педагогічної, дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	<p>Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП:</p> <ul style="list-style-type: none"> – забезпеченість комп'ютерними робочими місцями та прикладними комп'ютерними програмами достатнє для виконання навчальних планів; – усі комп'ютери кафедри під'єднані до локальної мережі університету з можливістю виходу в глобальну мережу Інтернет; – для ведення документації та забезпечення навчально-методичними матеріалами освітнього процесу кафедра в достатній кількості забезпечена оргтехнікою (принтерами, сканерами); – навчальні лабораторії оснащені технічними засобами та спеціалізованим програмним забезпеченням, необхідними приладами та обладнанням (охоронними системами відеоспостереження, засобами та комплексами виявлення закладних пристроїв, засобами просторового та мережевого захисту інформації). <p>Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі.</p>
8.3.	Інформаційне та навчально-методичне забезпечення	<p>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 НУ «KAI».</p> <p>Всі студенти забезпечені підручниками та навчальними посібниками з компонентів ОПП.</p> <p>Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment).</p> <p>Офіційний веб-сайт www.kai.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні</p>

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	Шифр документа	КАІ ОП ОП Б ID68646 – 02 – 2026
	стор. 15 з 24		

		<p>підрозділи, правила прийому, контакти. 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 НУ «КАІ»: http://er.kai.edu.ua.</p>
Розділ 9. Академічна мобільність		
9.1.	Внутрішня академічна мобільність	У рамках двосторонніх договорів між НУ «КАІ» та вітчизняними закладами вищої освіти.
9.2.	Міжнародна академічна мобільність	У рамках Еразмус+К1 договір про співробітництво між НУ «КАІ» та навчальними закладами ЄС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

2.1. Перелік освітніх компонентів

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
OK1.	Університетські студії	3.0	Диф. залік	1
OK2.	Основи авіації	3.0	Диф. залік	2
OK3.	Інтенсивний курс англійської мови	8.0	Диф. залік Екзамен	1, 2
OK4.	Фахова англійська мова	8.0	Диф. залік Екзамен	3, 4
OK5.	Історія, філософія та етика технічного прогресу: український дискурс	4.0	Диф. залік	2

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	стор. 16 з 24		

OK6.	Академічна та публічна комунікація українською мовою	3.0	Диф. залік	1
OK7.	Математика для ІТ	15.0	Диф. залік Екзамен	2, 1, 3
OK8.	Дискретна математика	4.0	Диф. залік	4
OK9.	Загальна фізика	7.0	Диф. залік Екзамен	1, 2
OK10.	Інформаційні технології	10.0	Диф. залік Екзамен	2, 1
OK11.	Основи автоматизованої обробки інформації	6.0	Диф. залік Екзамен	1, 2
OK12.	Основи кібербезпеки та захисту інформації	3.0	Диф. залік	1
OK13.1	Апаратне забезпечення інформаційних систем	5.0	Диф. залік Екзамен	3, 4
OK13.2	Курсова робота з навчальної дисципліни «Апаратне забезпечення інформаційних систем»	1.0	Захист	3
OK14.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	7.0	Диф. залік Екзамен	5, 6
OK15.	Захищені комп'ютерні системи та мережі	7.0	Диф. залік Екзамен	5, 6
OK16	Управління інформаційною безпекою	3.0	Екзамен	6
OK17.1	Прикладна криптологія	8.0	Диф. залік Екзамен	7 8
OK17.2	Курсова робота з навчальної дисципліни «Прикладна криптологія»	1.0	Захист	8
OK18.	Операційні системи та технології їх захисту	7.0	Диф. залік Екзамен	6, 7
OK19.	Системи технічного захисту інформації	3.0	Екзамен	7
OK20.	Компонентна база засобів технічного захисту інформації	3.0	Екзамен	3

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	Шифр документа	КАІ ОП ОП Б ID68646 – 02 – 2026
	стор. 17 з 24		

OK21.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	9.0	Екзамен	3, 4
OK22.	Виявлення закладних пристроїв на об'єктах інформаційної діяльності	3.0	Диф. залік	4
OK23.	Безпека інформаційно-комунікаційних систем	4.0	Диф. залік	4
OK24.	Схемотехніка пристроїв технічного захисту інформації	3.0	Екзамен	5
OK25.1	Засоби передавання сигналів в системах технічного захисту інформації	4.0	Екзамен	5
OK25.2	Курсова робота з навчальної дисципліни «Засоби передавання сигналів в системах технічного захисту інформації»	1.0	Захист	5
OK26.	Поля і хвилі в системах технічного захисту інформації	4.0	Екзамен	5
OK27.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	4.0	Диф. залік	7
OK28.	Цифрова обробка сигналів	4.0	Екзамен	7
OK29.	Комплексні системи захисту інформації	3.0	Екзамен	8
OK30.	Проектування систем технічного захисту інформації	4.0	Екзамен	8
OK31.	Методи та засоби технічного захисту інформації	4.0	Диф. залік	8
OK32.	Фахова ознайомлювальна практика	3.0	Диф. залік	2
OK33.	Комп'ютерна практика	3.0	Диф. залік	4
OK34.	Технологічна практика	3.0	Диф. залік	6
OK35.	Єдиний державний кваліфікаційний іспит	1.5		8
OK36*.	Базова загальновійська підготовка (теоретична підготовка)	3.0	Визначається програмою дисципліни	4
Загальний обсяг обов'язкових компонентів:		180 кредитів ЄКТС		
Вибіркові компоненти**				
ВК1	Дисципліна 1	4,0	Залік	3
ВК2	Дисципліна 2	4,0	Залік	3
ВК3	Дисципліна 3	4,0	Залік	3
ВК4	Дисципліна 4	4,0	Залік	5

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	Шифр документа	KAI ОП ОП Б ID68646 – 02 – 2026
	стор. 18 з 24		

ВК5	Дисципліна 5	4,0	Залік	5
ВК6	Дисципліна 6	4,0	Залік	5
ВК7	Дисципліна 7	4,0	Залік	6
ВК8	Дисципліна 8	4,0	Залік	6
ВК9	Дисципліна 9	4,0	Залік	6
ВК10	Дисципліна 10	4,0	Залік	7
ВК11	Дисципліна 11	4,0	Залік	7
ВК12	Дисципліна 12	4,0	Залік	7
ВК13	Дисципліна 13	4,0	Залік	8
ВК14	Дисципліна 14	4,0	Залік	8
ВК15	Дисципліна 15	4,0	Залік	8
Загальний обсяг вибірових компонентів			60 кредитів ЄКТС	
Загальний обсяг освітньо-професійної програми			240 кредитів ЄКТС	

Примітки:

* Навчальна дисципліна «Базова загальновійськова підготовка» (ОК35) 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.

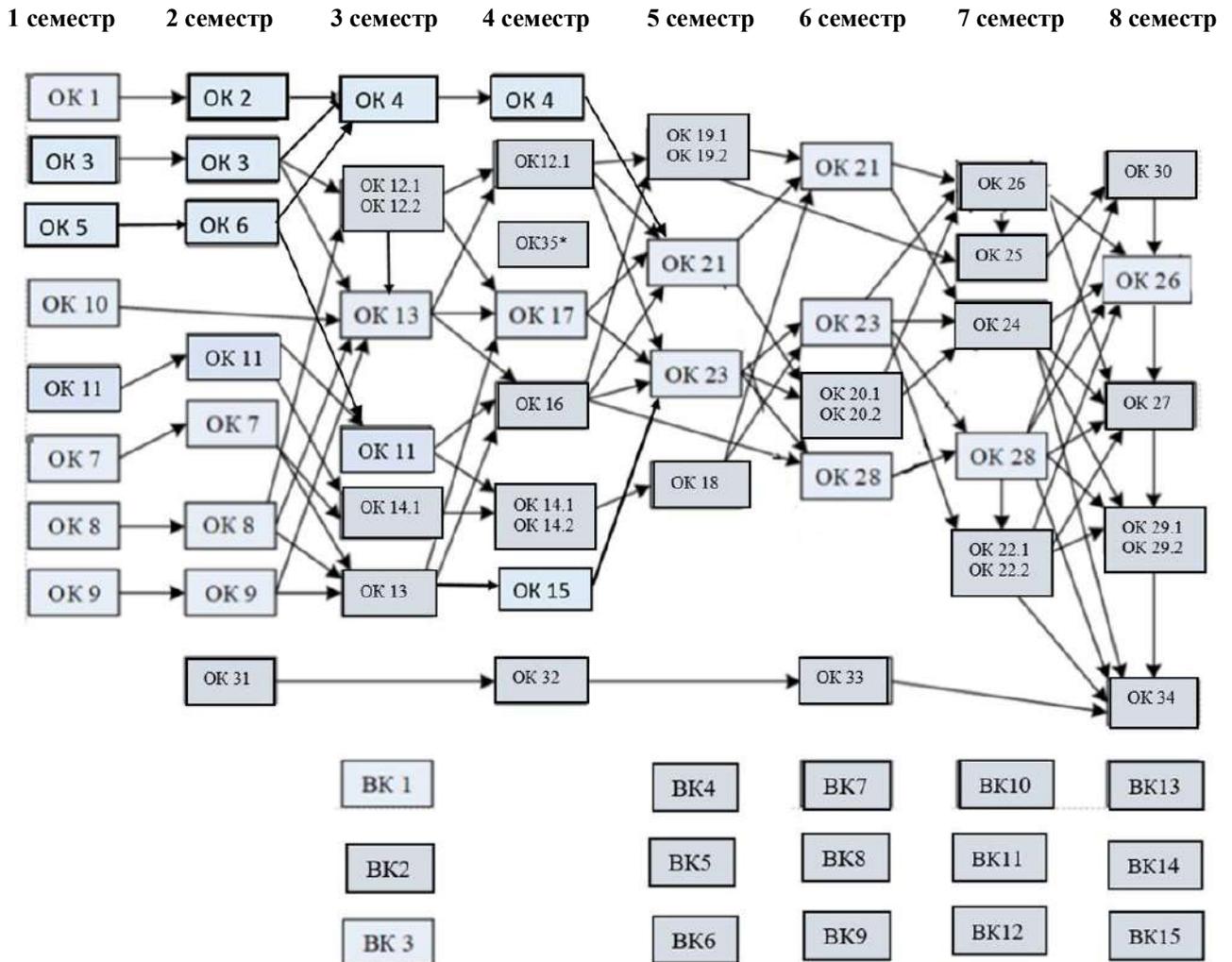
Форми організації освітнього процесу, види навчальних занять, кількість годин, відведених на їх опанування, форми та засоби поточного і підсумкового контролю визначаються програмою навчальної дисципліни, яка розробляється на основі типової програми навчальної дисципліни «Базова загальновійськова підготовка», 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 вибір освітніх компонентів та створення індивідуальної освітньої траєкторії регламентується законодавством України та внутрішніми нормативними актами КАІ.

2.2. Структурно-логічна схема освітньо-професійної програми

Підлягає обговоренню



**OK35 Навчальна дисципліна «Базова загальновійськова підготовка (теоретична 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.*



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Системи технічного захисту інформації, автоматизація її
обробки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 «Кібербезпека та захист інформації»»

Шифр
документа

КАІ ОП ОП Б ID68646 –
02 – 2026

стор. 21 з 24

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	КАІ ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кибербезпека та захист інформації»»	стор. 23 з 24	

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 (ОКЗБ), 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» .*

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Системи технічного захисту інформації, автоматизація її обробки»	Шифр документа	КАІ ОП ОП Б ID68646 – 02 – 2026
	першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»»	стор. 24 з 24	

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» для 5. 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