(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ 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»
(125 «Кібербезпека та захист інформації»)

галузі знань F «Інформаційні технології»
(12 «Інформаційні технології»)

СМЯ КАІ ОП Б ID68646 – 01 – 2025

Для здобувачів 2025 року вступу введено навчальну дисципліну «Основи національного спротиву», рішення Вченої ради університету від 22 вересня 2026 року (протокол № 12).

Освітньо-професійна програма
затверджена Вченою радою КАІ
протокол № 6 від 23.04. 2025 р.
Вводиться в дію наказом в.о. президента КАІ
від 29.04. 2025 р. № 283/од

В.о. президента

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 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 № 4
від «22» 04 2025 р.
Голова НМР КАІ, проректор з наукових досліджень та трансферу технологій
_____ Сергій ГНАТЮК

ПОГОДЖЕНО
Вченою радою факультету комп'ютерних наук та технологій
протокол № 5
від «16» 04 2025 р.
Голова Вченої ради
факультету комп'ютерних наук та технологій
_____ Андрій ФЕСЕНКО

ПОГОДЖЕНО
Кафедрою технічного захисту інформації
протокол засідання № 7
від «14» квітня 2025 р.

Завідувач кафедри
_____ Валерій КОЗЛОВСЬКИЙ

ПОГОДЖЕНО
Студентською радою
факультету комп'ютерних наук та технологій
протокол № 25-03-и – Фкнт
від «16» квітня 2025 р.
Голова Студентської ради факультету
_____ Хомчова Ю.

ПЕРЕДМОВА

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

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

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

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

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

(підпис)

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

(підпис)

ШВЕЦЬ В.А. – к.т.н., доцент, доцент кафедри технічного захисту інформації Факультету комп'ютерних наук та технологій

(підпис)

ТОКАР А.О. – здобувач вищої освіти за освітньою програмою, група Б-125-21-2-СЗ

(підпис здобувача вищої освіти)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР

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

(підпис)

Рецензія зовнішнього стейкхолдера додається.

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

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Державний університет «Київський авіаційний інститут» Факультет комп'ютерних наук та технологій Кафедра технічного захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Освітній ступінь - 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. Умови вступу регулюються Правилами прийому до КАІ.
1.9.	Мова(и) 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.	Метою (цілями) освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» є: - 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.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об'єкт діяльності, теоретичний зміст)	**Об'єкт навчання**: - 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 та нейтралізація реальних та 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, 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 та спеціалізації (за наявності)	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: – 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; – автоматизованих систем обробки інформації з обмеженим доступом. 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.
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)	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. **Методи, методики та технології**: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення кібербезпеки та захисту інформації.

		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. 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. Технології дистанційного навчання, що 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. 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. **Інструменти та обладнання:** – 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 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 професії. **ЗК3**. Здатність спілкуватися державною мовою як усно, так письмово. **ЗК4.** Здатність спілкуватися іноземною мовою. **ЗК5.** Здатність вчитися і оволодівати сучасними знаннями. **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. **ЗК7.** Здатність ухвалювати рішення й діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **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.

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 та 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 оцінювати захищеність інформації усіх видів, що циркулює на об’єктах інформаційної діяльності. **ФК12.** Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об’єктах

		інформаційної діяльності та в інформаційно-комунікаційних системах. **ФК13.** Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв. **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.
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.** Спілкування 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'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 кібербеспеки 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 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, організовувати допуск та доступ персоналу підприємств до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. **ПРН23.** Організовувати внутрішньо-об'єктовий та пропускний режими на об'єктах авіаційної критичної інфраструктри. **ПРН24.** Вирішувати задачі розробки та супроводу комплексних систем захисту інформації та комплексів технічного захисту інформації на авіаційних об'єктах інформаційної діяльності.

		ПРН25. Виявляти закладні пристрої несанкціонованого отримання інформації на об’єктах інформаційної діяльності. **ПРН26.** Вирішувати задачі забезпечення кібербезпеки та захисту інформації на об’єктах інформаційної діяльності на основі концепції забезпечення сталого розвитку інформаційного суспільства. **ПРН27.** Визначати показники захищеності інформації на об’єктах інформаційної діяльності.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	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. До організації освітнього процесу залучаються професіонали з досвідом наукової, педагогічної, дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП: – 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).

		Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі.
8.3.	Інформаційне та навчально-методичне забезпечення	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки ДУ «КАІ». Всі студенти забезпечені підручниками та навчальними посібниками з компонентів ОПП. Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment). Офіційний веб-сайт www.kai.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.kai.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки ДУ «КАІ»: http://er.kai.edu.ua.
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	У рамках двосторонніх договорів між ДУ «Київський авіаційний інститут» та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між ДУ «КАІ» та навчальними закладами ЄС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

2.1. Перелік 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				
ОК1.	Університетські студії	3.0	Диф. залік	1
ОК2.	Основи авіації	3.0	Диф. залік	2
ОК3.	Інтенсивний курс англійської мови	6.0	Диф. залік Екзамен	1, 2
ОК4.	Фахова англійська мова	7.0	Диф. залік Екзамен	3, 4
ОК5.	Академічна та публічна комунікація українською мовою	3.0	Диф. залік	1
ОК6.	Історія, філософія та етика технічного прогресу: український дискурс	4.0	Диф. залік	2
ОК7.	Фізика	9.0	Диф. залік Екзамен	1, 2
ОК8.	Інформаційні технології	9.5	Диф. залік Екзамен	2, 1
ОК9.	Основи автоматизованої обробки інформації	6.5	Диф. залік Екзамен	1, 2
ОК10.	Основи кібербезпеки	4.5	Екзамен	1
ОК11.	Вища математика	12.0	Диф. залік Екзамен	2, 1, 3
ОК12.1	Апаратне забезпечення інформаційних систем	5.0	Диф. залік Екзамен	3, 4
ОК12.2	Курсова робота з навчальної дисципліни «Апаратне забезпечення інформаційних систем»	1.0	Захист	3
ОК13.	Компонентна база засобів технічного захисту інформації	3.5	Екзамен	3

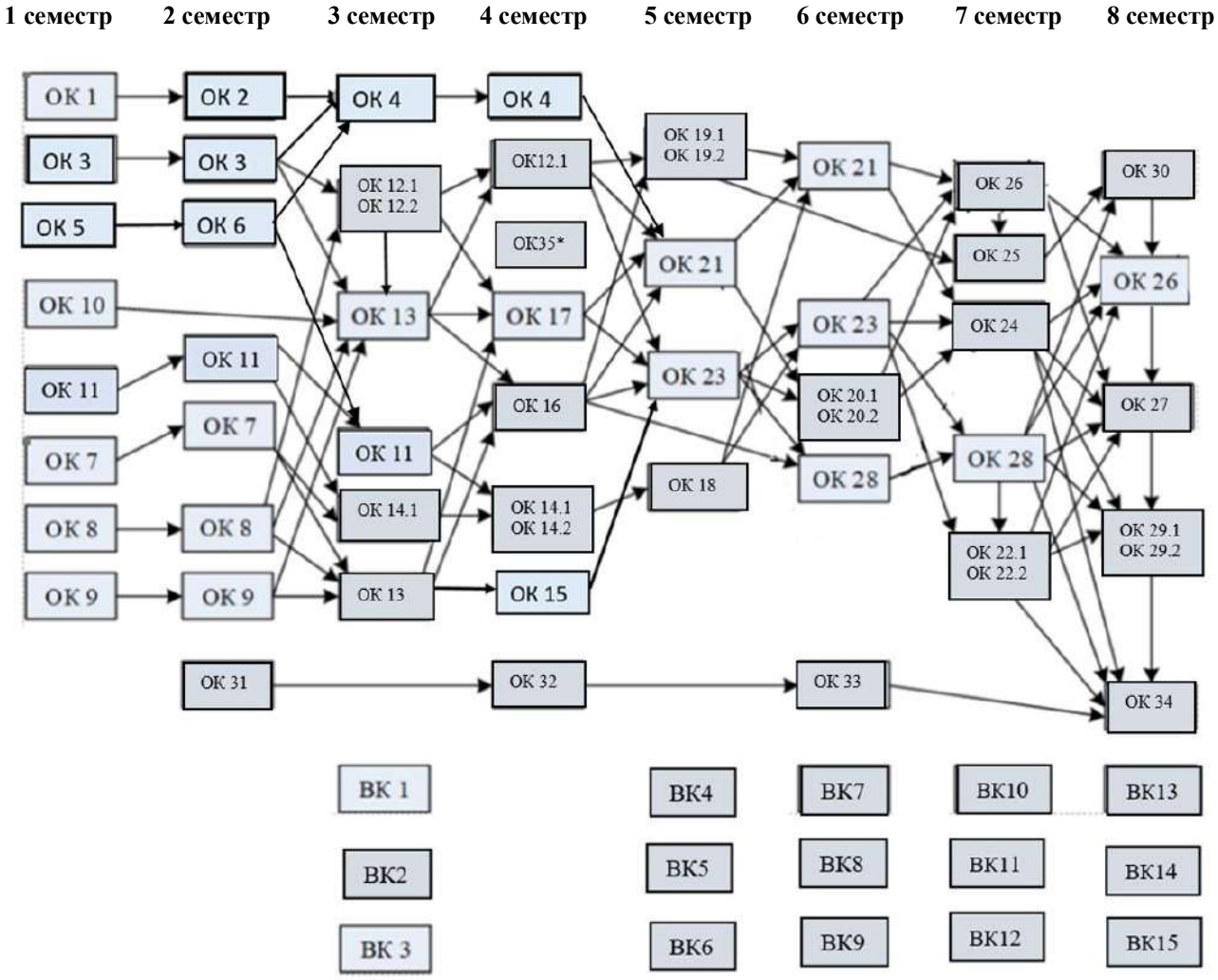
ОК14.1	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	8.5	Екзамен	3, 4
ОК14.2	Курсова робота з навчальної дисципліни «Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації»	1.0	Захист	3
ОК15.	Виявлення закладних пристроїв на об'єктах інформаційної діяльності	3.5	Диф. залік	4
ОК16.	Схемотехніка пристроїв технічного захисту інформації	4.5	Диф. залік	4
ОК17.	Безпека інформаційно-комунікаційних систем	4.5	Диф. залік	4
ОК18.	Поля і хвилі в системах технічного захисту інформації	4.0	Екзамен	5
ОК19.1	Засоби передавання сигналів в системах технічного захисту інформації	4.5	Екзамен	5
ОК19.2	Курсова робота з навчальної дисципліни « Засоби передавання сигналів в системах технічного захисту інформації»	1.0	Захист	5
ОК20.1	Управління інформаційною безпекою	3.0	Екзамен	6
ОК20.2	Курсова робота з навчальної дисципліни «Управління інформаційною безпекою»	1.0	Захист	6
ОК21.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	8.5	Екзамен	5,6
ОК22.1	Прикладна криптологія	7.0	Диф. залік Екзамен	7 8
ОК22.2	Курсова робота з навчальної дисципліни «Прикладна криптологія»	1.0	Захист	7
ОК23.	Захищені комп'ютерні системи та мережі	7.5	Диф. залік Екзамен	5, 6
ОК24.	Системи технічного захисту інформації	3.0	Екзамен	7
ОК25.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	3.5	Диф. залік	7
ОК26.	Цифрова обробка сигналів	4.0	Екзамен	7
ОК27.	Методи та засоби технічного захисту інформації	5.0	Диф. залік	8

ОК28.	Операційні системи та технології їх захисту	6.5	Диф. залік Екзамен	6, 7
ОК29.1	Проєктування систем технічного захисту інформації	3.0	Екзамен	8
ОК29.2	Курсова робота з навчальної дисципліни «Проєктування систем технічного захисту інформації»	1.0	Захист	8
ОК30.	Комплексні системи захисту інформації	4.0	Екзамен	8
ОК31.	Фахова ознайомлювальна практика	3.0	Диф. залік	2
ОК32.	Комп'ютерна практика	3.0	Диф. залік	4
ОК33.	Технологічна практика	3.0	Диф. залік	6
ОК34.	Єдиний державний кваліфікаційний іспит	1.5	Складання	8
ОК35*.	Основи національного спротиву	3.0	Визначається програмою дисципліни	4
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
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		

Примітка:

*** 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



3. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти ОС «Бакалавр» 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 зі спеціальності «Кібербезпека та захист інформації».

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК 11	ОК 12.1	ОК 12.2	ОК 13	ОК 14.1	ОК 14.2	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19.1	ОК 19.2	ОК 20.1	ОК 20.2	ОК 21	ОК 22.1	ОК 22.2	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29.1	ОК 29.2	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34*	ОК 35	ВК 1	ВК 2	ВК --	ВК 15
ІК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*	Визначаються згідно з програмою навчальної дисципліни				
ЗК1	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ЗК2	+	+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ЗК3		+		+																															+	+	+	*					
ЗК4		+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ЗК5	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ЗК6								+	+	+	+	+	+			+	+			+		+	+	+	+	+		+	+	+						+	+	*					
ЗК7					+					+	+	+	+			+		+	+	+						+	+	+	+	+						+	+	*					
ЗК8	+	+	+																																	+	+	*					
ФК1		+		+					+	+			+				+			+			+			+		+	+	+						+	+	*					
ФК2				+				+	+	+	+	+				+	+			+		+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	*					
ФК3								+		+	+	+	+			+	+	+		+		+	+	+	+	+		+	+	+						+	+	*					
ФК4								+	+	+	+	+	+			+	+					+	+		+	+		+	+	+						+	+	*					
ФК5							+			+			+	+	+					+	+		+			+		+	+							+	+	*					
ФК6								+	+	+	+	+				+		+				+	+		+	+		+	+	+						+	+	*					
ФК7								+	+	+	+	+				+	+			+		+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	*					
ФК8								+	+	+	+	+	+			+	+		+	+		+	+		+	+	+	+	+	+						+	+	*					
ФК9								+		+			+				+			+			+			+		+	+							+	+	*					
ФК10						+				+						+	+							+		+		+	+	+						+	+	*					
ФК11								+	+	+			+	+	+		+			+	+	+	+		+	+		+	+							+	+	*					
ФК12							+			+			+	+	+		+		+		+		+			+	+	+	+	+						+	+	*					
ФК13						+	+							+	+	+		+	+								+									+	+	*					
ФК14						+				+						+	+							+		+		+	+	+						+	+	*					

Примітка.

* *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 / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК11	ОК 12.1	ОК 12.2	ОК 13	ОК 14.1	ОК 14.2	ОК15	ОК 16	ОК 17	ОК 18	ОК19.1	ОК19.2	ОК 20.1	ОК 20.2	ОК 21	ОК 22.1	ОК 22.2	ОК 23	ОК24	ОК25	ОК26	ОК27	ОК 28	ОК 29.1	ОК 29.2	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34*	ОК 35	ВК 1	ВК 2	ВК --	ВК 15
ПРН 1		+		+	+			+	+	+									+				+	+	+			+	+	+	+	+	+	+	+		+	+	+	*	Визначаються згідно з програмою навчальної дисципліни				
ПРН 2			+			+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ПРН 3		+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ПРН 4						+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ПРН 5	+		+			+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ПРН 6	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	*					
ПРН 7		+		+				+	+	+	+	+	+	+					+		+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	*					
ПРН 8		+		+				+		+				+					+				+	+	+				+			+	+	+		+	+	+	*					
ПРН 9		+		+				+		+				+					+				+	+	+				+			+	+	+		+	+	+	*					
ПРН 10								+		+	+	+	+						+									+				+				+	+	*					
ПРН 11								+	+	+	+	+	+	+					+									+				+				+	+	*					
ПРН 12		+							+	+				+					+				+	+	+				+				+	+		+	+	+	*					
ПРН 13								+	+	+	+	+	+						+									+				+				+	+	*					
ПРН 14								+	+	+									+									+		+	+	+	+	+	+		+	+	*					
ПРН 15				+				+	+		+	+	+						+									+				+			+	+	+	+	*					
ПРН 16								+	+	+	+	+	+					+	+	+			+	+	+			+	+				+	+	+		+	+	*					
ПРН 17								+	+	+	+	+	+						+				+	+	+			+					+				+	+	*					
ПРН 18								+	+	+	+	+	+	+				+	+	+	+	+	+	+	+			+	+				+	+	+	+	+	+	*					
ПРН 19								+		+									+				+	+	+			+						+	+		+	+	+	*					
ПРН 20								+	+	+									+									+					+				+	+	*					
ПРН 21								+	+	+	+	+	+					+	+	+			+	+	+			+	+				+	+	+		+	+	*					
ПРН 22								+	+	+	+	+	+					+	+	+			+	+	+			+	+				+	+	+		+	+	*					
ПРН 23								+	+	+									+				+	+	+			+	+				+	+	+		+	+	*					
ПРН 24								+		+									+				+	+	+			+	+				+				+	+	*					
ПРН 25								+	+	+									+				+	+	+			+	+				+				+	+	*					
ПРН 26								+		+									+				+	+	+			+	+				+				+	+	*					
ПРН 27								+	+	+									+				+	+	+			+					+				+	+	*					

Примітка.

* *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. 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-п

5. Національний класифікатор України. Класифікація видів економічної діяльності: ДК 009:2010, затверджений наказом Держспоживстандарту України від 11.10.2010 № 457 (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/vb457609-10

6. Стандарт вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 "Інформаційні технології" для першого (бакалаврського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 29.10.2024 № 1547

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

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

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				

РЕЦЕНЗІЯ

Освітньо-професійної програми
«Системи технічного захисту інформації, автоматизація її обробки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5/125 «Кібербезпека та захист інформації»
Державного університету «Київський авіаційний інститут»

Представлена на рецензування освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5/125 «Кібербезпека та захист інформації» розроблена робочою групою науково-педагогічних працівників кафедри Технічного захисту інформації Факультету комп'ютерних наук та технологій Державного університету «Київський авіаційний інститут», спрямована на підготовку кваліфікованих фахівців у сфері кібербезпеки та захисту інформації.

Рецензована ОПП за освітнім ступенем «Бакалавр» скорегована у напрямку посилення професійної орієнтації фахівців у сфері забезпечення інформаційної та кібербезпеки. Об'єктивна необхідність ОПП зумовлена формуванням у студентів фундаментальних знань, вмінь та навичок майбутніх фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації.

Представлена програма регламентує мету, очікувані результати навчання, зміст, умови і технологію реалізації освітнього процесу, оцінку якості підготовки здобувачів першого (бакалаврського) рівня за даною спеціальністю і включає в себе: загальну інформацію, мету і характеристику освітньої програми, здатність випускників до подальшого навчання та працевлаштування, викладання та оцінювання, компетентності та програмні результати навчання, ресурсне забезпечення реалізації програми, академічну мобільність, перелік обов'язкових і блок вибіркових компонентів та їх логічну послідовність, структурно-логічну схему освітньої програми, форму атестації здобувачів вищої освіти, матрицю відповідності компетентностей та програмних результатів навчання.

Компоненти освітньої програми дозволяють повною мірою сформувати знання, практичні уміння і навички, необхідні сучасному фахівцеві. У доборі цих компонент витримано баланс між циклами гуманітарної підготовки і циклами професійної та практичної підготовки, теорією і практикою.

У структуру ОПП включені обов'язкові та блок вибіркових компонент підготовки здобувачів вищої освіти, сформульовані у термінах результатів навчання: знання, уміння, комунікація, автономія та відповідальність. Наявність в освітній програмі блоку вільного вибору передбачає можливість реалізації особистісного потенціалу здобувача освіти, враховуючи його здібності, інтереси, потреби, мотивацію, можливості та ґрунтується на виборі здобувачем освіти видів та форм здобуття освіти, навчальних дисциплін і рівня їх складності, методів і засобів навчання, формуючи індивідуальну освітню траєкторію підготовки.

Важливим є те, що до освітньої програми введена навчальна дисципліна «Базова загальновійськова підготовка» (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).

Загальна структура освітньо-професійної програми логічно витримана і дає змогу підсилити фахову та професійну підготовку випускників з подальшою можливістю їх працевлаштування. Пропозиції до змісту освітньо-професійної програми, надані під час погоджувальних робочих зустрічей, враховані у повному обсязі.

Представлена на рецензію ОПП відповідає новому Стандарту вищої освіти України першого (бакалаврського) рівня освіти за спеціальністю F5/125 «Кібербезпека та захист інформації» (у редакції наказу Міністерства освіти та науки України №1547 від 29.10.2024р.), враховує новітні тенденції та проблеми розвитку освітянської галузі й сприятиме підготовці висококваліфікованих фахівців та інтеграції України в європейський загальноосвітній та науковий простір.

Враховуючи викладене зазначаю, що освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» підготовки здобувачів першого (бакалаврського) рівня вищої освіти може використовуватися для підготовки фахівців спеціальності F5/125 «Кібербезпека та захист інформації».

Професор кафедри управління кібербезпекою
та захистом інформації Навчально-наукового
інституту кібербезпеки та захисту інформації
Державного університету інформаційно-
комунікаційних технологій

д.т.н., професор Віталій САВЧЕНКО

Підпис В. Савченка

ЗАСВІДЧУЮ
Учений секретар
Державного університету
інформаційно-комунікаційних технологій Г. Ачева