(Ф 03.02 – 107)

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»
(125 Кібербезпека та захист інформації)

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

СМЯ КАІ ОП Б ID68643 – 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 23.04. 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-н-ФКНТ
від «16» квітня 2025 р.
Голова Студентської ради факультету

ПЕРЕДМОВА

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

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

Приходько Тетяна Юріївна	*к.т.н., доцент кафедри технічного захисту інформації*	(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Козловський Валерій Валерійович	*д.т.н., професор, завідувач кафедри технічного захисту інформації*	(підпис)
Зибін Сергій Вікторович	*д.т.н., професор кафедри технічного захисту інформації*	(підпис)
Іванченко Ігор Сергійович	*к.т.н., доцент кафедри технічного захисту інформації*	(підпис)
Мазур Олександра Анатоліївна	*здобувач(ка) вищої освіти за освітньою програмою, група Б-125-21-3-СК*	(підпис)

ЗОВНІШНІ СТЕЙКГОЛДЕРИ

Савченко Віталій Анатолійович	*д.т.н., професор, професор кафедри управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій*	(підпис)

Рецензії-відгуки зовнішніх стейкголдерів (додаються).

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

Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	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 здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми кредити ЄКТС, отримані в межах попередньої освітньої програми підготовки фахівців Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється в порядку, визначеному законодавством Умови вступу регулюються Правилами прийому

		до КАІ.
1.9.	Мови викладання	Українська, англійська
1.10.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://kai.edu.ua
Розділ 2. Мета (цілі) освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в підготовці висококваліфікованих та конкурентоспроможних на національному та міжнародному ринках праці фахівців з 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. Програма також передбачає 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**: - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; - об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання**: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації; **Теоретичний зміст предметної області**: принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язанні теоретичних і практичних задач кібербезпеки та захисту інформації **Інструменти та обладнання**: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформативні системи та комплекси проєктування, 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 F5 «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 проводових та безпроводових мереж.
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; – 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 крипто-графічного захисту інформації; – захищених інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення систем кібербезпеки тощо. – цифрової криміналістики та реагування на інциденти; – авіаційної безпеки та кібербезпеки авіаційних інформаційних систем; – захист критичних інформаційних систем

		авіаційної галузі. 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. Особливістю програми є її авіаційна спрямованість, що дозволяє випускникам реалізовувати захист критичних інформаційних систем авіаційної галузі, а також адаптуватися до нових викликів у сфері кібербезпеки завдяки постійному розвитку компетенцій.
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 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, індивідуально-творчий підхід; навчання через лекції, лабораторні роботи, семінари, практичні заняття, консультації з викладачами, проєктну роботу в командах, навчальну та виробничі практики. **Методи, методики та технології.** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також

		методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативноправових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
5.2.	Оцінювання	Відповідно до Положення про організацію освітнього процесу в КАІ, рейтингової системи оцінювання набутих студентом знань та вмінь, визначеної для кожної навчальної дисципліни її робочою програмою, інших нормативних документів.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації
6.2.	Загальні компетентності (ЗК)	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності **ЗК3.** Здатність спілкуватися державною мовою як усно, так і 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-процесіву 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 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. **ФК14.** Здатність забезпечувати кібербезпеку критичних авіаційних інформаційних систем відповідно до міжнародних стандартів та національного законодавства. **ФК15.** Здатність застосовувати знання та навички для протидії кіберзлочинності, захисту державних інформаційних ресурсів та сприяння безпечному й правовому використанню кіберпростору в контексті сталого розвитку інформаційного суспільства, спрямованого на досягнення миру, справедливості та сильних інститутів.
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 кібербезпеки та захисту інформації для здійснення професійної діяльності. **ПРН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях 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 до

		інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. **ПРН23.** Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об'єкті інформаційної діяльності. **ПРН24.** Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. **ПРН25.** Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-комунікаційних систем. **ПРН26.** Розробляти проєкти комплексних систем захисту інформації та комплексів технічного захисту інформації. **ПРН27**. 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. **ПРН28.** Проводити аудит кібербезпеки критичних потоків в авіаційних інформаційних системах, розробляти рекомендації щодо підвищення рівня їхньої безпеки та відповідності міжнародним стандартам. **ПРН29.** Вирішувати задачі розробки та впровадження політики кібербезпеки для суб'єктів авіаційної діяльності, зокрема авіакомпаній, аеропортів та підприємств. **ПРН30.** Застосовувати спеціалізовані знання та практичні навички для виявлення, аналізу, запобігання та протидії кіберзлочинності, ефективно захищати державні інформаційні ресурси, а також сприяти встановленню безпечного, правового та етичного використання кіберпростору як важливої складової сталого розвитку інформаційного суспільства, що є необхідною умовою для досягнення миру, справедливості та функціонування сильних інститутів (відповідно до Цілей сталого розвитку 9 та 16).
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Викладачі, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної, науково-педагогічної роботи та

		досвід практичної роботи. У процесі організації освітнього процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою. Матеріально-технічна база кафедри технічного 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).
8.3.	Інформаційне та навчально-методичне забезпечення	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки КАІ. 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. 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
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 «Київський авіаційний інститут» та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

2.1. Перелік освітніх компонентів

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
1	2	3	4	5
	Обов'язкові компоненти			
ОК1.	Університетські студії	3,0	Диф. залік	1
ОК2.	Основи авіації	3,0	Диф. залік	2
ОК3.	Інтенсивний курс англійської мови	6,0	Диф. залік	1
			Екзамен	2
ОК4.	Фахова англійська мова	7,0	Диф. залік	3
			Екзамен	4
ОК5.	Історія, філософія та етика технічного прогресу: український дискурс	4,0	Диф. залік	2
ОК6.	Академічна та публічна комунікація українською мовою	3,0	Диф. залік	1
ОК7.	Вища математика	12,0	Екзамен	1
			Диф. залік	2
			Екзамен	3
ОК8.	Фізика	9,0	Диф. залік	1
			Екзамен	2
ОК9.	Інформаційні технології	9,5	Екзамен	1
			Диф. залік	2
ОК10.	Основи автоматизованої обробки інформації	6,5	Диф. залік	1
			Екзамен	2
ОК11.	Основи кібербезпеки	4,5	Екзамен	1
ОК12.1	Апаратне забезпечення інформаційних систем	5,0	Диф. залік	3
			Екзамен	4
ОК12.2	Курсова робота з дисципліни Апаратне забезпечення інформаційних систем	1,0	Захист	3
ОК13.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	8,5	Екзамен	5, 6
ОК14.	Захищені комп'ютерні системи та мережі	7,5	Диф. залік	5
			Екзамен	6
ОК15.1	Управління інформаційною безпекою	3,0	Екзамен	6
ОК15.2	Курсова робота з дисципліни «Управління інформаційною безпекою»	1,0	Захист	6
ОК16.1	Прикладна криптологія	7,0	Диф. залік	7
			Екзамен	8
ОК16.2	Курсова робота з дисципліни «Прикладна	1,0	Захист	7

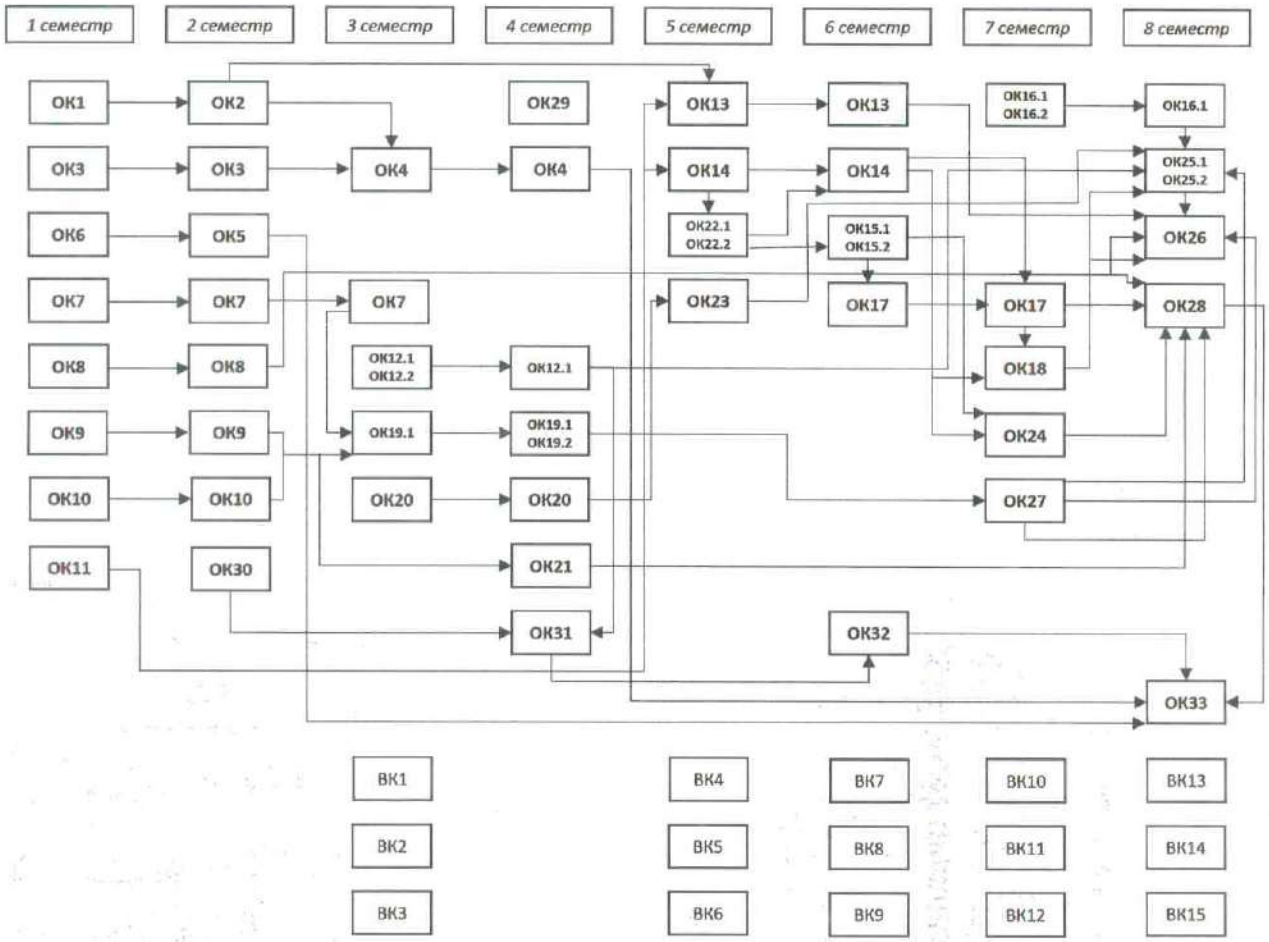
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
1	2	3	4	5
	криптологія»			
ОК17.	Операційні системи та технології їх захисту	6,5	Диф. залік	6
			Екзамен	7
ОК18.	Системи технічного захисту інформації	3,0	Екзамен	7
ОК19.1	Технології програмування	10,5	Екзамен	3, 4
ОК19.2	Курсова робота з дисципліни «Технології програмування»	1,0	Захист	4
ОК20.	Дискретна математика	9,0	Екзамен	3
			Диф. залік	4
ОК21.	Технології виявлення уразливостей інформаційних систем	5,0	Диф. залік	4
ОК22.1	Ризик-менеджмент інформаційної безпеки	4,5	Екзамен	5
ОК22.2	Курсова робота з дисципліни «Ризик-менеджмент інформаційної безпеки»	1,0	Захист	5
ОК23.	Криміналістичний аналіз сфери кібербезпеки	4,0	Екзамен	5
ОК24.	Веб-програмування та інтернет-протоколи	3,5	Диф. залік	7
ОК25.1	Комплексні системи захисту інформації	4,0	Екзамен	8
ОК25.2	Курсовий проєкт з дисципліни «Комплексні системи захисту інформації»	1,5	Захист	8
ОК26.	Оцінювання та тестування стану безпеки інформаційних систем	4,0	Екзамен	8
ОК27.	Управління інцидентами інформаційної безпеки	4,0	Екзамен	7
ОК28.	Безпекові технології штучного інтелекту	3,5	Диф. залік	8
ОК29*	Основи національного спротиву	3,0	Визначається програмою дисципліни	4
ОК30.	Фахово-ознайомлювальна практика	3,0	Диф. залік	2
ОК31.	Комп'ютерна практика	3,0	Диф. залік	4
ОК32.	Технологічна практика	3,0	Диф. залік	6
ОК33.	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
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**		

** 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



**ОК29. 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.*

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.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12.1	ОК12.2	ОК13	ОК14	ОК15.1	ОК15.2	ОК16.1	ОК16.2	ОК17	ОК18	ОК19.1	ОК19.2	ОК20	ОК21	ОК22.1	ОК22.2	ОК23	ОК24	ОК25.1	ОК25.2	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33*	ВК1	…	ВК15
ІК	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	*			
ЗК1		+	+	+			+	+	+	+	+			+	+	+	+	+	+	+		+	+	+		+	+	+	+	+	+			+		+	+	+	*			
ЗК2		+													+	+	+	+	+	+		+	+			+	+	+	+	+	+			+		+	+	+	*			
ЗК3					+	+																														+	+	+	*			
ЗК4			+	+																																			*			
ЗК5		+			+		+		+		+	+	+	+	+	+	+				+	+	+	+				+	+	+	+	+	+	+		+	+	+	*			
ЗК6	+		+	+	+						+																										+			*			
ЗК7	+	+			+						+																										+		+	*			
ЗК8	+																													+	+		+	+					*			
ФК1		+	+	+																						+	+			+	+			+		+		+	*			
ФК2									+						+	+	+			+	+				+					+	+	+	+			+	+	+	*			
ФК3		+													+	+	+					+	+						+	+	+							+	*			
ФК4											+	+	+	+		+	+			+		+	+		+							+	+	+			+	+	*			
ФК5										+		+	+	+	+	+	+			+																		+	*			
ФК6								+						+		+	+				+	+	+			+	+			+	+					+	+	+	*			
ФК7												+	+			+	+													+	+					+	+	+	*			
ФК8							+				+	+	+			+	+	+	+																		+	+	*			
ФК9											+			+														+	+									+	*			
ФК10									+		+			+	+	+	+				+					+	+	+					+	+					*			
ФК11																+	+	+	+		+				+			+					+	+					*			
ФК12												+	+			+	+	+	+										+	+	+								*			
ФК13															+					+					+			+		+	+	+	+					*			
ФК14														+		+	+									+	+					+									
ФК15																										+	+	+				+	+								

Визначається програмою навчальної дисципліни

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 здобутих компетентностей), пов'язаних з базовою загальновійськовою підготовкою (ОК29), 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 навчальної дисципліни*

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

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

| | | |

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. 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

(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 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	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				

РЕЦЕНЗІЯ-ВІДГУК

освітньо-професійної програми
«Системи та технології кібербезпеки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5/125 «Кібербезпека та захист інформації»
Державного університету «Київський авіаційний інститут»

Представлена на рецензію освітньо-професійна програма «Системи та технології кібербезпеки» першого (бакалаврського) рівня вищої освіти за спеціальністю F5/125 «Кібербезпека та захист інформації» є актуальною в умовах зростаючих загроз у цифровому просторі.

Аналізуючи програму можна виділити такі ключові аспекти: програма відповідає сучасним викликам у сфері кібербезпеки, включаючи захист інформаційних систем, розробку безпечного програмного забезпечення та аналіз кіберзагроз. Значна увага приділяється практичним навичкам, розроблена спільно з компаніями які працюють у сфері інформаційної безпеки та інформаційних технологій, що забезпечує релевантність матеріалу. За такою програмою фахівці з кібербезпеки мають високий попит на ринку праці, як в ВПК та Оборонному секторі України, так і в банківському секторі, державних установах, телекомунікаціях IT-компаніях.

Компоненти освітньої програми дозволяють повною мірою сформувати знання, охоплюють широкий спектр дисциплін, включаючи теоретичні основи кібербезпеки, практичні навички захисту інформації, а також правові та етичні аспекти кібербезпеки. Навчальні плани програм включають як обов'язкові, так і вибіркові дисципліни, що дозволяє студентам спеціалізуватися в певних областях кібербезпеки.

Слід зауважити, що програма сформована згідно нового стандарту, як результат є добре структурованою, що є більш зручним для використання в освітньому процесі. З урахуванням запропонованих удосконалень програма може ще більше підвищити свою ефективність та конкурентоспроможність випускників. До освітньої програми додана навчальна дисципліна «Базова загальновійськова підготовка» введена до освітньої програми на підставі п. 7 Порядку проведення базової загальновійськової підготовки громадян України.

Під час погоджувальних робочих зустрічей були внесені пропозиції до змісту освітньо-професійної програми. Враховані у повному обсязі.

Освітньо-професійна програма «Системи та технології кібербезпеки» спеціальності F5/125 «Кібербезпека та захист інформації» є перспективною для тих, хто планує кар'єру у сфері захисту інформаційних систем. Вона дає базові й поглиблені знання.

Директор
ТОВ «ПЕРША УКРАЇНСЬКА ЛІЗИНГОВА КОМПАНІЯ»
Тадеєва Світлана Василівна

РЕЦЕНЗІЯ

освітньо-професійної програми «Системи та технології кібербезпеки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5/125 «Кібербезпека та захист інформації»
Державного університету «Київський авіаційний інститут»

Аналіз представленої на рецензію освітньо-професійної програми «Системи та технології кібербезпеки» (далі – ОПП) першого (бакалаврського) рівня вищої освіти свідчить про її направленість на підготовку висококваліфікованих фахівців зі спеціальності F5/125 «Кібербезпека та захист інформації».

Мета освітньо-професійної програми «Системи та технології кібербезпеки» полягає у підготовці фахівців висококваліфікованих та конкурентоспроможних фахівців з розробки та впровадження 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.

Компоненти освітньої програми дозволяють повною мірою сформувати знання, практичні уміння і навички, необхідні сучасному фахівцеві. Витримано баланс між циклами гуманітарної підготовки і циклами професійної та практичної підготовки, теорією і практикою. Програма відповідає сучасним викликам у сфері кібербезпеки, зокрема, зростаючим загрозам кібератак та необхідності захисту інформаційних систем у державному та приватному секторах.

Вагомою перевагою даної ОПП є те, що окрім обов'язкових компонентів, вона містить блок дисциплін вільного вибору (блок вибіркових компонент), що дає змогу здобувачам реалізовувати своє право на формування індивідуальної освітньої підготовки з урахуванням потреб ринку праці в сфері інформаційної та/або кібербезпеки.

Дана ОПП сформована згідно нового стандарту є добре структурованою та актуальною, що є більш зручним для використання в освітньому процесі. Вона забезпечує ґрунтовні теоретичні знання та практичні навички, необхідні для роботи в галузі кібербезпеки. З урахуванням запропонованих удосконалень програма може ще більше підвищити свою ефективність та конкурентоспроможність випускників. На підставі п. 7 Порядку проведення базової загальновійськової підготовки громадян України до освітньої програми, як обов'язкова, компонента, включена навчальна дисципліна «Базова загальновійськова підготовка».

Пропозиції до змісту освітньо-професійної програми, надані під час погоджувальних робочих зустрічей, враховані у повному обсязі.

З огляду на викладене зазначаю, що освітньо-професійна програма «Системи та технології кібербезпеки» спеціальності F5/125 «Кібербезпека та захист інформації» є сучасним, комплексним і якісним освітнім продуктом, який повністю відповідає актуальним потребам ринку праці, забезпечує глибоку підготовку фахівців, створює умови для їхнього подальшого професійного та особистого зростання.

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. Савчика

ЗАСВІДЧУЮ:
Учений секретар
Державного університету
інформаційно-комунікаційних технологій Г. Ємова



РЕЦЕНЗІЯ

освітньо-професійної програми
«Системи та технології кібербезпеки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 «Кібербезпека та захист інформації»
Державного університету «Київський авіаційний інститут»

Представлена на розгляд та рецензію освітньо-професійна програма «Системи та технології кібербезпеки» (далі – ОПП) першого (бакалаврського) рівня вищої освіти є важливим та актуальним напрямом підготовки висококваліфікованих фахівців зі спеціальності F5 «Кібербезпека та захист інформації».

Освітньо-професійна програма «Системи та технології кібербезпеки» спрямована на підготовку фахівців у сфері інформаційної безпеки, здатних забезпечувати захист інформаційних ресурсів, аналізувати та запобігати кіберзагрозам. Програма орієнтована на сучасні вимоги ринку праці та передбачає здобуття студентами як теоретичних знань, так і практичних навичок.

Щоб забезпечити системний підхід до підготовки фахівців у програмі чітко визначені компетентності, які формують базові навички сучасного фахівця. Витримано баланс між циклами гуманітарної підготовки і циклами професійної та практичної підготовки, теорією і практикою.

ОПП містить блок вибіркових компонент, що дає змогу здобувачам реалізовувати своє право на формування індивідуальної освітньої підготовки з урахуванням потреб ринку праці в сфері кібербезпеки.

Програма передбачає поєднання теоретичних знань з практичними навичками, необхідними для роботи в галузі кібербезпеки, є добре структурованою та актуальною, сформована згідно нового стандарту.

Під час погоджувальних робочих зустрічей пропозиції до змісту освітньо-професійної програми враховані у повному обсязі.

З огляду на викладене вважаю, що освітньо-професійна програма «Системи та технології кібербезпеки» спеціальності F5 «Кібербезпека та захист інформації» відповідає сучасним викликам та потребам ринку праці в галузі кібербезпеки. Враховує тенденції розвитку інформаційних технологій та зростання кіберзагроз.

Директор ТОВ «Інтернет Інвест» Павло Блоцький