(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи та технології кібербезпеки»

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 «Кібербезпека та захист інформації»

галузі знань 12 «Інформаційні технології»

СМЯ НАУ 08.01 – 02– 2024

Освітньо-професійна програма
затверджена Вченою радою Університету
протокол № 7 від 17.04. 2024 р.

Голова комісії з реорганізації НАУ,
в.о. ректора

Ксенія СЕМЕНОВА

Наказ № 166/од від 23.04. 2024 р.

КИЇВ

Враховано Стандарт вищої освіти України: другого (магістерського) рівня, галузі знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека». Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою

Національного авіаційного університету

протокол № 3

від "16" 04 2024 р.

Голова НМР НАУ,

Проректор з навчальної роботи

_____ Анатолій ПОЛУХІН

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки та програмної інженерії

протокол № 2

від "9" квітня 2024 р.

Голова Вченої ради

Факультету кібербезпеки та програмної інженерії

_____ Олександр ПОНОМАРЕНКО

ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

протокол засідання № 3а

від "01" квітня 2024 р.

В.о. завідувача кафедри

_____ Євгенія ІВАНЧЕНКО

ПОГОДЖЕНО

Студентською радою Факультету кібербезпеки та програмної інженерії

протокол № 24/6-н-ФКПІ

від "07" квітня 2024 р.

Голова студентської ради

Факультету кібербезпеки та програмної інженерії

_____ Анна ВАСЬКОВСЬКА

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 «Кібербезпека та захист інформації», рік вступу – 2024-й та наступні до нової редакції освітньої програми) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ІВАНЧЕНКО Є.В., к.т.н., проф., в.о. завідувача кафедри безпеки інформаційних технологій

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОРЧЕНКО О.Г., д.т.н., проф., в.о. проректора з наукової роботи Національного авіаційного університету, професор кафедри безпеки інформаційних технологій

(підпис)

ПОГОРЄЛОВ В.В., к.т.н., доц., доцент кафедри безпеки інформаційних технологій

(підпис)

ХОХЛАЧОВА Ю.Є., к.т.н., проф., доцент кафедри безпеки інформаційних технологій

(підпис)

ВАСЬКОВСЬКА А.О., студентка кафедри безпеки інформаційних технологій, групи АМ-171М

(підпис)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР
ЛАХНО В.А., д.т.н., проф., професор кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України

(підпис)

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Врахований примірник №1

ПРИМІТКА. Відповідно до п. 1.47 наказу голови комісії з реорганізації НАУ, в.о. ректора від 28.03.2024 № 120/од «Про введення в дію рішень Вченої ради університету від 20 березня 2024 року (проток ол № 3)» реалізація освітнього процесу за цією редакцією освітньої програми в 2024-2025 навчальному році відтермінована у зв'язку з реорганізацією Національного авіаційного університету.

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет, Факультет кібербезпеки та програмної інженерії, кафедра безпеки інформаційних технологій Навчально-науковий інститут неперервної освіти (заочна форма навчання)
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та захисту інформації
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Системи та технології кібербезпеки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці (денна форма навчання) / 1 рік 4 місяці (заочна форма навчання)
1.5.	Акредитаційна інституція	Національне агентство із забезпечення якості вищої освіти
1.6.	Період акредитації	Підлягає акредитації вперше
1.7.	Цикл/рівень	Другий (магістерський) рівень 7 рівень Національної рамки кваліфікацій України (НРК України), другий цикл Європейського простору вищої освіти (FQ-EHEA), 7 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Для здобуття освітнього рівня магістра можуть вступати особи, що здобули освітній рівень бакалавра. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека та захист інформації для першого (бакалаврського) рівня вищої освіти. Заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані за попередньою освітньою програмою підготовки магістра (спеціаліста) за іншою спеціальністю. Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми. Умови вступу регулюються Правилами прийому до Національного авіаційного університету.
1.9.	Форма навчання	Очна (денна), заочна
1.10	Мова(и) викладання	Українська
1.11	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://fcpi.nau.edu.ua/ http://www.bit.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціль освітньо-професійної програми полягає в підготовці висококваліфікованих та конкурентоспроможних фахівців на глобальному ринку праці, які володіють достатніми ґрунтовними компетентностями для ефективного виконання завдань інноваційного	

	характеру у сфері захисту інформації, розробці, використанні та впровадженні сучасних технологій забезпечення інформаційної та кібербезпеки, а також опануванні специфічних знань особливостей професійної діяльності в авіаційному секторі, дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в авіаційній галузі задля внеску НАУ у розвиток суспільства через генерацію нових знань і надання високоякісних освітніх послуг при підготовці фахівців з кібербезпеки з урахуванням специфіки авіаційної галузі.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	*Об'єкт діяльності:* — сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; — інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; — інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; — системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); — інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); — програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; — системи управління інформаційною безпекою та/або кібербезпекою; — інформаційні ресурси та технології; — технології забезпечення складових безпеки інформації: інформаційна безпека, кібербезпека, безпека інформації; — процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту; — технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. *Теоретичний зміст предметної області. Знання:* - теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки; - принципи побудови, супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, теорії систем управління інформаційною та/або кібербезпекою; - методи та засоби виявлення, управління та ідентифікації ризиків; - методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації;

		- методи та засоби технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення; автоматизованих систем проєктування.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма має прикладну орієнтацію, що базується на загальновідомих наукових і практичних результатах в галузі інформаційної безпеки. Акцентована на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності, а також на розвиток здатності розв'язувати складні задачі і проблеми в галузі інформаційних технологій, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта в галузі «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері систем та технологій кібербезпеки, в тому числі моделювання, оптимізації та адмініструванні безпекових процесів в сфері захисту інформації. Ключові слова: кібербезпека, системи та технології кібербезпеки, інформаційна безпека, криптографічний захист інформації, захист персональних даних, захист інформації, захист від несанкціонованого доступу, електронний цифровий підпис.
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – принципів супроводу систем кібербезпеки; – теорії систем управління захистом інформації; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів технічного та криптографічного захисту інформації; – автоматизованих систем проєктування засобів захисту інформації; – захищених інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення систем кібербезпеки тощо. 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. Проведений аналіз показав необхідність продовжувати формування та реалізацію моделі підготовки фахівців з акцентом на технічний напрям ІТ підприємств, та урахуванням потреб сучасної транспортної, а саме, авіаційної галузі України. Це забезпечує можливість отримання якісної професійної освіти в галузі ІТ та робить вказану ОПП унікальною. **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 нормативно-правових 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.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи у сфері захисту інформації та кібербезпеки в складі відповідних департаментів організацій, підприємств та банків; у сфері: адміністрування систем інформаційної та кібернетичної безпеки; аудиту інформаційних технологій (з кібербезпеки); у сфері проектування: систем захисту в кіберпросторі; систем протидії інцидентам; інфраструктури кіберзахисту; у сфері розробки програмних та програмно-апаратних засобів захисту інформації в кіберпросторі; в галузі кібербезпеки в складі правоохоронних органів; у сфері забезпечення кібербезпеки в кіберпросторі (зокрема, в соціальних мережах, об'єктах критичної інфраструктури, в службах авіаційної безпеки)
4.2.	Подальше навчання	Право продовжити навчання на третьому (освітньо-науковому) рівні вищої освіти. Право набувати додаткові кваліфікації в системі післядипломної освіти
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Реалізація освітнього процесу передбачає поєднання студентоцентрованого, проблемно-орієнтованого навчання із застосування наступних технологій і видів навчальних занять: лекцій, лабораторних і практичних занять із розв'язанням ситуаційних завдань, самостійна робота з інформаційними джерелами; аналіз і узагальнення інформації; розробка проектної та програмної документації, із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі, планування

		та реалізація конкретних проектів і робіт при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна Компетентність (ІК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
6.3.	Фахові компетентності (ФК)	ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК6. Здатність аналізувати, контролювати та

		забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. ***Додаткові фахові компетентності, пов'язані з особливостями освітньої програми:*** ФК11. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. ФК12. Здатність організовувати роботу колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем захисту інформації. ФК13. Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень. ФК14. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації, а також застосовувати методи і засоби організаційного характеру щодо захисту інформації на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення

		результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної

		інфраструктури. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. ***Додаткові програмні результати навчання,***

		пов'язані з особливостями освітньої програми: ПРН24. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки, в тому числі в галузі авіаційної безпеки. ПРН25. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки, що дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в тому числі і в сфері авіаційної безпеки.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. У процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне Забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
8.3	Інформаційне та навчально-методичне Забезпечення	Офіційний веб-сайт www.nau.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 НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/14303 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 НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	У рамках двосторонніх договорів між Національним авіаційним університетом та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

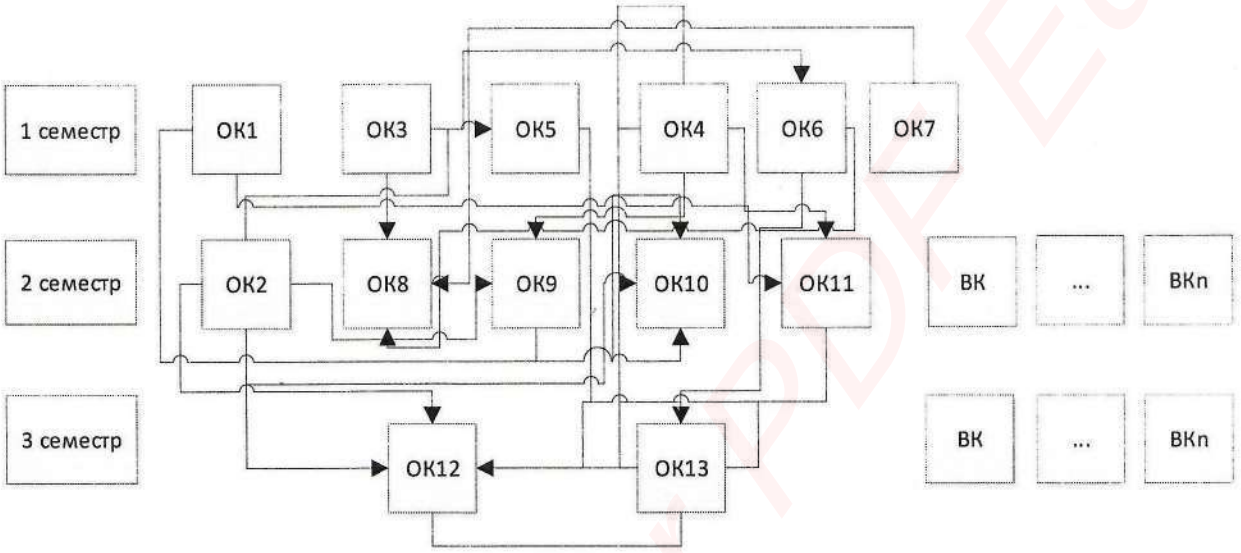
2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонентів

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кіль-кість креди-тів	Форма підсумкового контролю	Семестр (відповідно до форми навчання)
				денна
Обов'язкові компоненти ОПП				
ОК1.	Ділова іноземна мова	3,5	Екзамен	1
ОК2.	Наукові комунікації у фаховій діяльності	3,5	Диференційований залік	2
ОК3.	Методи побудови та аналізу криптосистем	6,0	Екзамен	1
ОК4.	Методологія прикладних досліджень у сфері кібербезпеки	6,5	Диференційований залік	1
ОК5.	Курсовий проєкт з дисципліни «Методологія прикладних досліджень у сфері кібербезпеки»	1,5	Захист	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	6,0	Екзамен	1
ОК7.	Організаційні моделі кібербезпеки	6,5	Диференційований залік	1
ОК8.	Аудит інформаційної безпеки	3,0	Екзамен	2
ОК9.	Інтелектуалізовані системи інформаційної безпеки	4,5	Екзамен	2
ОК10.	Курсова робота з дисципліни «Інтелектуалізовані системи інформаційної безпеки»	1,0	Захист	2
ОК11.	Науково-дослідна практика в області систем та технологій кібербезпеки	6,0	Диференційований залік	2
ОК12.	Переддипломна практика	9,0	Диференційований залік	3
ОК13.	Кваліфікаційна робота	9,0	Захист	3
Загальний обсяг обов'язкових компонентів:		**66 кредитів ЄКТС**		
Вибіркові компоненти *				
ВК 1.	Дисципліна 1	4,0	Диференційований залік	2
ВК 2.	Дисципліна 2	4,0	Диференційований залік	2
ВК 3.	Дисципліна 3	4,0	Диференційований залік	2
ВК 4.	Дисципліна 4	4,0	Диференційований залік	3
ВК 5.	Дисципліна 5	4,0	Диференційований залік	3
ВК 6.	Дисципліна 6	4,0	Диференційований залік	3
Загальний обсяг вибіркових компонентів		**24 кредити ЄКТС**		
Загальний обсяг освітньо-професійної програми		**90 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 НАУ. Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	**Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.**
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.
Вимоги до публічного захисту (демонстрації)	Захист кваліфікаційних робіт проводиться шляхом публічного захисту на відкритому засіданні ЕК.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ВК1	ВК2	…	ВКn
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК1		+	+			+	+	+	+	+	+	+	+				
ЗК2	+	+	+		+	+	+	+	+	+		+	+				
ЗК3		+		+		+		+					+				
ЗК4		+		+	+	+	+	+				+	+				
ЗК5	+	+								+	+	+	+				
ФК1				+				+					+				
ФК2	+	+		+	+	+	+				+	+	+				
ФК3			+	+	+	+	+		+	+			+				
ФК4						+	+	+	+				+				
ФК5					+	+		+					+				
ФК6			+			+		+		+			+				
ФК7				+	+	+	+		+				+				
ФК8			+					+					+				
ФК9				+		+	+		+	+		+	+				
ФК10		+		+					+	+		+	+				
ФК11	+	+		+					+	+	+	+	+				
ФК12		+		+					+	+	+	+	+				
ФК13		+			+		+		+	+		+	+				
ФК14		+		+		+		+			+		+				

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ВК1	ВК2	…	ВКn
ПРН1	+								+	+	+	+	+				
ПРН2		+		+		+			+	+	+	+	+				
ПРН3		+	+	+	+	+							+				
ПРН4			+			+	+	+	+	+		+	+				
ПРН5	+	+		+	+	+	+					+	+				
ПРН6			+		+	+		+					+				
ПРН7				+	+		+						+				
ПРН8				+		+	+					+	+				
ПРН9			+	+	+			+					+				
ПРН10					+	+	+						+				
ПРН11		+		+	+	+			+	+	+	+	+				
ПРН12						+	+						+				
ПРН13			+	+	+	+	+					+	+				
ПРН14						+		+	+	+	+	+	+				
ПРН15		+		+	+	+			+	+	+	+	+				
ПРН16				+		+	+						+				
ПРН17		+				+			+	+	+	+	+				
ПРН18		+		+	+				+	+		+	+				
ПРН19			+	+		+	+					+	+				
ПРН20		+		+								+	+				
ПРН21						+		+					+				
ПРН22									+	+	+	+	+				
ПРН23			+	+				+					+				
ПРН24				+		+	+	+			+	+	+				
ПРН25				+	+			+	+	+			+				

6. Система внутрішнього забезпечення якості вищої освіти НАУ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та діяльністю НАУ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності, затвердженим рішенням Вченої ради університету від 28.11.2018 (протокол №8), та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 №1556-VII (зі 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 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. Національний класифікатор України. Класифікатор професій ДК 003:2010, затверджений наказом Держспоживстандарту України від 28.07.2010 № 327 (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10.

7. Стандарт вищої освіти зі спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 18.03.2021 № 332.

8. Професійний стандарт «Аудитор інформаційних технологій (з кібербезпеки)», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.

9. Професійний стандарт «Фахівець з підтримки інфраструктури кіберзахисту», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.

10. Професійний стандарт «Фахівець з реагування на інциденти кіберезпеки», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.

11. Професійний стандарт «Фахівець з кібердосліджень та розробок систем безпеки», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.

12. Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20/ed20240101

13. Annex 17 «The Convention on International Civil Aviation. Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference. International Civil Aviation Organization» (12 видання, липень 2022 року) [Електронний ресурс]. – режим доступу: https://www.icao.int/Documents/annexes_booklet.pdf»

(Ф 03.02 - 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	0302	01.05.2024	Коваль О.И.	Ковал	

(Ф 03.02 - 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

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

(Ф 03.02 - 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	зміненого	заміненого	нового	анульованого			

(Ф 03.02 - 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЙ

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

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
«Системи та технології кібербезпеки»
Спеціальності 125 «Кібербезпека та захист інформації»
другого (магістерського) рівня вищої освіти

Рецензована освітньо-професійна програма «Системи та технології кібербезпеки» розроблена колективом кафедри безпеки інформаційних технологій факультету кібербезпеки та програмної інженерії.

Освітньо-професійна програма «Системи та технології кібербезпеки» за спеціальністю 125 «Кібербезпека та захист інформації» розроблена з урахуванням вимог потенційних роботодавців, які підтвердили потребу у фахівцях цієї спеціальності.

В основі освітньо-професійної програми визначені програмні компетентності виходячи із завдань спеціальності. Вони розподілені на загальні та фахові компетентності. Зміст усіх компетентностей орієнтовано на знання та уміння з використання новітніх методів та підходів забезпезпечення кібербезпеки. Усі компетентності носять практичний характер і можуть бути використані у професійній діяльності майбутніх фахівців.

Освітньо-професійна програма містить систему освітніх компонентів, які побудовані в логічній послідовності вивчення, що забезпечить формування ряду відповідних фахових компетентностей та дозволить підготувати фахівців другого (магістерського) рівня вищої освіти.

Ціль освітньо-професійної програми полягає в підготовці висококваліфікованих та конкурентоспроможних фахівців на глобальному ринку праці, які володіють достатніми ґрунтовними компетентностями для ефективного виконання завдань інноваційного характеру у сфері захисту інформації, розробці, використанні та впровадженні сучасних технологій забезпечення інформаційної та кібербезпеки, а також в опануванні специфічних знань особливостей професійної діяльності в авіаційному секторі, що дозволить вирішувати практичні завдання підвищення рівня безпекових процесів в авіаційній галузі.

Зазначений в освітньо-професійній програмі об'єкт діяльності цілком відповідає сучасним потребам ІТ-галузі та забезпеченню інформаційної та\або кібербезпеки, що цілком обґрунтовує необхідність продовжувати формування та реалізацію моделі підготовки фахівців з акцентом на технічний напрям ІТ підприємств з урахуванням потреб сучасної транспортної, а саме, авіаційної галузі України.

Особливої уваги заслуговує орієнтація освітньо-професійної програми, зокрема, підготовка висококваліфікованих і креативних спеціалістів, які володіють навичками науково-дослідницького й інноваційного характеру та спроможні проводити наукові дослідження, вирішувати певні проблеми та завдання у сфері забезпечення інформаційної та\або кібербезпеки, а також розв'язувати складні задачі і проблеми в галузі інформаційних технологій, у рамках яких можлива подальша професійна кар'єра і подальше навчання.

Освітньо-професійна програма «Системи та технології кібербезпеки» спеціальності 125 «Кібербезпека та захист інформації» повністю відповідає кваліфікаційній характеристиці випускників з повною вищою освітою за освітньо-кваліфікаційним рівнем «Магістр» та професійним стандартам вищої освіти в галузі кібербезпеки і сприяє забезпеченню відповідності результатів навчання запитам потенційних роботодавців.

Професор кафедри
комп'ютерних систем, мереж та
кібербезпеки Національного
університету біоресурсів і
природокористування України,
д.т.н., проф. Валерій ЛАХНО

Підпис засвідчую
Пров. фахівець ... і. Головко

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДДІЛ КАДРІВ
м. КИЇВ