Проєкт
(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Адміністративний менеджмент у сфері захисту інформації»
(найменування освітньої програми)
Другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)
галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

СМЯ НАУ 09.01.08 – 01 – 2020

Освітньо-професійна програма
Затверджена Вченою радою
протокол №____від_____20___р.

Вводиться в дію наказом ректора
Ректор
_____В.Ісаєнко
наказ №____від_____20__ р.

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО

Радою з якості університету

протокол №_____

від "_____"_____20___ р.

Голова Ради з якості НАУ

_____(Ісаєнко В.М.)

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол №_____

від "_____"_____20___ р.

Голова Вченої ради
Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____(Азаренко О.В.)

ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

протокол засідання №_____

від "_____"_____20___ р.

Завідувач кафедри

_____(Корченко О.Г.)

ПОГОДЖЕНО

Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол №_____

від "_____"_____20___ р.

Голова Студентської ради
Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____(Осипчук Т.О.)

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 Кібербезпека) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ІВАНЧЕНКО Є.В., к.т.н., доц., професор кафедри безпеки інформаційних технологій _____

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОРЧЕНКО О.Г., д.т.н., проф., завідувач кафедри безпеки інформаційних технологій _____
(підпис)

БРИЛЬ В.М., к.т.н., проф., професор кафедри безпеки інформаційних технологій _____
(підпис)

ХОХЛАЧОВА Ю.Є., к.т.н., доц., доцент кафедри безпеки інформаційних технологій _____
(підпис)

ПЕДЧЕНКО Є.М., студент кафедри безпеки інформаційних технологій, групи АМ-571 _____
(підпис)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР
ЛАХНО В.А., д.т.н., проф., завідувач кафедри комп'ютерних систем і мереж Національного університету біоресурсів і природокористування України _____
(підпис)

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Врахований примірник №2

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет, Факультет кібербезпеки, комп'ютерної та програмної інженерії, кафедра безпеки інформаційних технологій
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Адміністративний менеджмент у сфері захисту інформації
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
1.5.	Акредитаційна інституція	Акредитовано, Акредитаційна комісія Міністерства освіти і науки України, сертифікат про акредитацію УД 11008106 від 27 грудня 2018 р.
1.6.	Період акредитації	1 липня 2024 р.
1.7.	Цикл/рівень	Восьмий кваліфікаційний рівень НРК України
1.8.	Передумови	Наявність ступеня бакалавра
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://fccpi.nau.edu.ua/ http://www.bit.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціль освітньої програми полягає в підготовці висококваліфікованих та конкурентоспроможних фахівців з ґрунтованими компетентностями у розробці, використанні та впровадженні сучасних технологій забезпечення інформаційної та кібербезпеки на підприємстві.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	Об'єкт діяльності: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, технології забезпечення складових безпеки інформації: інформаційна безпека, кібербезпека, безпека інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Теоретичний зміст: принципи формування систем забезпечення інформаційної та/або кібербезпеки; методи та засоби виявлення, управління та ідентифікації ризиків; загальні принципи та правила застосування криптографічних способів, методи та механізми забезпечення безпеки в сучасних цифрових системах.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма прикладної орієнтації, що базується на загальновідомих наукових результатах в галузі захисту інформації, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта другого (магістерського) рівня спеціальності 125 Кібербезпека Ключові слова: кібербезпека, 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; – теорії систем управління захистом інформації; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів технічного та крипто-графічного захисту інформації; – автоматизованих систем проєктування засобів захисту інформації. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки програма передбачає: – реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; – залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі ІТ, а також представників бізнесу. Це забезпечує можливість отримання якісної професійної освіти в галузі ІТ та робить вказану ОПП унікальною.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України : - фахівець із організації інформаційної безпеки; - фахівець із організації захисту інформації з обмеженим доступом; - фахівець з режиму секретності ; - фахівець з розроблення комп'ютерних програм; - фахівець з інформаційних технологій; - інспектор з організації захисту секретної інформації.
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)	Лекції, лабораторні роботи, семінари, практичні заняття, проєктна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика на підприємствах, підготовка кваліфікаційної магістерської роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, кваліфікаційний екзамен, захист кваліфікаційної магістерської роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна Компетентність (ІК)	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення захисту інформації, що характеризується комплексністю та неповною визначеністю умов.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК3. Вміння виявляти, ставити та вирішувати

		проблеми за професійним спрямуванням. ЗК4. Здатність до пошуку, оброблення та аналізу інформації. ЗК5. Здатність розв'язувати комплексні задачі та практичні проблеми технологій кібербезпеки в невизначених умовах. ЗК6. Здатність використовувати методи фундаментальних наук для розв'язання загально інженерних , професійних та наукових задач. ЗК7. Здатність використовувати методи загально інженерних наук для розв'язання професійних задач. ЗК8. Здатність до розроблення та управління проєктами. ЗК9. Здатність ефективно формувати комунікаційну стратегію. ЗК10. Здатність приймати обґрунтовані рішення. ЗК11. Здатність до подальшого навчання з високим рівнем автономності. ЗК12. Здатність працювати в міжнародному контексті ЗК13. Здатність до генерації нових ідей і варіантів розв'язання задач в галузі професійної діяльності
6.3.	Фахові компетентності (ФК)	ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі захисту інформації. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей захисту інформації. ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів захисту інформації. ФК4. Здатність відновлювати штатне функціонування інформаційних, інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК5. Здатність здійснювати процедури управління інцидентами безпеки, проводити розслідування, надавати їм оцінку. ФК6. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації. ФК7. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних систем згідно встановленої політики безпеки. ФК8. Здатність ефективно аналізувати, виявляти та оцінювати можливі загрози та уразливості інформації. ФК9. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. ФК10. Здатність використовувати управлінсько-

		організаційні, математичні, технічні та правові методи захисту інформації. ФК11. Здатність до застосування математичного та комп'ютерного моделювання для вирішення широкого спектру задач захисту інформації. 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 організовувати та проводити наукові дослідження, пов'язані із застосуванням математичних та технічних методів для аналізу та дослідження процесів та систем захисту інформації. ФК14. Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Розв'язувати задачі захисту інформації з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН2. Виконувати впровадження та підтримку систем виявлення вторгнень. ПРН3. Використовувати компоненти крипто-графічного захисту для забезпечення необхідного рівня захищеності інформації. ПРН4. Здатність демонструвати знання та розуміння архітектури систем захисту інформації та описати в загальних поняттях архітектуру, характеристики та принципи їх дії. ПРН5. Здатність демонструвати знання та розуміння сучасних методів і моделей захисту інформації. ПРН6. Здатність демонструвати знання та розуміння захисту інформації у комп'ютерних системах та обґрунтовано обирати і застосовувати на практиці методи виявлення інформаційних загроз; програмні та програмно-апаратні засоби захисту даних та операційних систем; ПРН7. Здатність демонструвати знання та розуміння захисту інформації у комп'ютерних системах та обґрунтовано обирати і застосовувати на практиці методи протидії спробам несанкціонованого доступу до інформаційних ресурсів, а також організаційні та адміністративні заходи підвищення рівня інформаційної безпеки комп'ютерних систем. ПРН8. Володіння та застосовування методів і систем штучного інтелекту ПРН9. Володіння та орієнтування в базових аспектах законодавства України, а також відповідних міжнародних стандартів у галузі кібербезпеки. ПРН10. Здатність демонструвати уміння фахово вести дискусію й викладати основи кібербезпеки ПРН11. Здатність демонструвати знання та уміння використовувати профільні знання в галузі математики

		для обробки експериментальних даних і математичного моделювання у сфері захисту інформації ПРН12. Здатність виконувати пошукову оптимізацію в рамках управлінської діяльності. ПРН13. Системно мислити та застосовувати творчі здібності до формування принципово нових ідей. ПРН14. Здатність продемонструвати знання та навики щодо проведення експериментів, збору даних та моделювання у сфері захисту інформації. ПРН15. Оцінювати отримані результати та аргументовано захищати прийняті рішення. ПРН16. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проєктів, дипломних робіт. ПРН17. Здатність володіння англійською мовою, використовувати спеціальну термінологію для проведення літературного пошуку.
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.

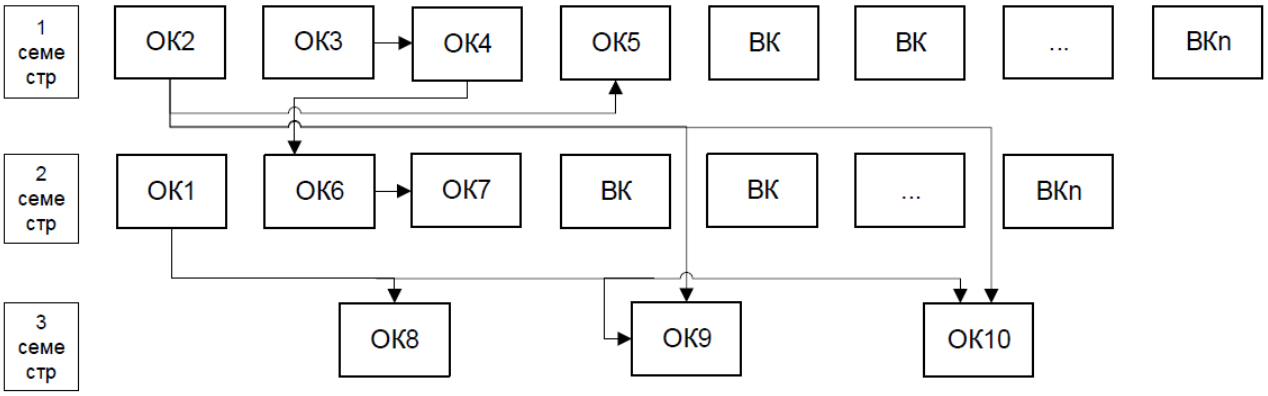
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
ОК 1.	Ділова іноземна мова	7.0	Екзамен	2
ОК 2.	Методологія наукових досліджень в сфері кібербезпеки	4.5	Екзамен	1
ОК 3.	Методи побудови та аналізу криптосистем	4.5	Екзамен	1
ОК 4.	Методи моделювання та оптимізація процесів в сфері захисту інформації	4.5	Екзамен	1
ОК 5.	Кібербезпека	4.5	Диференційований залік	1
ОК 6.	Нормативно-правове забезпечення інформаційної безпеки	7.0	Екзамен	2
ОК 7.	Інтелектуалізовані системи інформаційної безпеки (в т.ч. курсова робота)	7.0	Екзамен	2
ОК 8.	Переддипломна практика	12.0	Диференційований залік	3
ОК 9.	Кваліфікаційний екзамен	1.5	Екзамен	3
ОК 10	Кваліфікаційна магістерська робота	13.5		3
Загальний обсяг обов'язкових компонент:		66 кредитів		
Вибіркові компоненти				
ВК 1.	Дисципліна 1			
ВК 2.	Дисципліна 2			
…	…			
ВК n.	Дисципліна n			
Загальний обсяг вибіркових компонент*		24 кредити		
Загальний обсяг освітньо-професійної програми		90 кредитів		

**Вибіркові компоненти обираються здобувачами вищої освіти із загальноуніверситетського та фахового переліків вибіркових дисциплін Університету, які в свою чергу щороку оновлюються та затверджуються рішенням Ради з якості Національного авіаційного університету. Методика формування переліків та процедура вибору вибіркових компонентів (навчальних дисциплін вільного вибору) наведені у Положенні про порядок реалізації здобувачами вищої освіти права на вибір навчальних дисциплін у Національному авіаційному університеті.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація випускників освітньо-професійної програми проводиться у формі кваліфікаційного екзамену та захисту кваліфікаційної магістерської роботи та завершується видачею документу встановленого зразка про присудження йому освітньої кваліфікації: Магістр з кібербезеки.
Вимоги кваліфікаційного екзамену (екзаменів) (за наявності)	Державний кваліфікаційний екзамен проводиться як комплексна перевірка знань за білетами, складеними у відповідності до програми державної атестації. Форма проведення кваліфікаційного екзамену – письмова.
Вимоги до кваліфікаційної магістерської роботи (за наявності)	Кваліфікаційна робота має передбачати розв'язання складної задачі у сфері кібербезпеки, що потребує проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічний плагіат, фабрикацію та фальсифікацію. Кваліфікаційна робота обов'язково включає елементи наукової новизни та відповідає вимогам академічної доброчесності.
Вимоги до публічного захисту (демонстрації) (за наявності)	Захист кваліфікаційних робіт проводиться шляхом публічного захисту на відкритому засіданні ДЕК. Для виступу здобувачеві вищої освіти надається до 15 хвилин. Обов'язковою умовою є наявність презентації.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми.

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ВК1	ВК2	…	ВКn
ІК		+		+	+	+	+	+	+	+				
ЗК1			+	+	+		+	+	+	+				
ЗК2	+							+	+	+				
ЗК3		+	+	+										
ЗК4		+					+	+	+	+				
ЗК5				+	+		+							
ЗК6			+	+	+		+			+				
ЗК7				+			+							
ЗК8					+		+	+	+	+				
ЗК9			+	+	+					+				
ЗК10		+						+	+	+				
ЗК11								+	+	+				
ЗК12	+	+			+	+								
ЗК13				+			+							
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	ВК1	ВК2	…	ВКn
ПРН1			+											
ПРН2					+		+							
ПРН3			+							+				
ПРН4				+	+									
ПРН5				+	+									
ПРН6					+			+		+				
ПРН7					+			+						
ПРН8							+							
ПРН9	+				+	+								
ПРН10		+			+					+				
ПРН11			+	+										
ПРН12				+		+	+							
ПРН13		+												
ПРН14		+		+				+		+				
ПРН15		+												
ПРН16								+	+	+				
ПРН17	+													

* *Вибіркові компоненти обрані з загальноуніверситетського та фахового переліків вибіркових дисциплін Університету мають також забезпечувати визначені програмні результати навчання (ПРН). Кількість вибіркових компонент визначається виходячи із загального обсягу вибіркових компонент (кредитів) освітньої програми.*

(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 - 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