(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Адміністративний менеджмент у сфері захисту інформації»
(найменування ОПП)

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)
галузі знань 12 Інформаційні технології
(шифр та найменування галузі)
освітня кваліфікація: Магістр з кібербезпеки
(найменування освітньої кваліфікації)
кваліфікація: Науковий співробітник (інформаційна безпека)
Професіонал із організації інформаційної безпеки
(найменування освітньої кваліфікації)

СМЯ НАУ ОПП 14.01.05 – 01 – 2019

Затверджено Вченою радою
Голова Вченої ради
_____ В.Ісаєнко
(протокол №____від_____2019 р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В.Ісаєнко
(наказ №____від_____2019 р.)

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою університету

протокол №_____

від "_____"_____2019 р

Проректор НАУ з навчальної роботи

Голова НМР НАУ

_____(Гудманян А.Г.)

ПОГОДЖЕНО

Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол №_____

від "_____"_____2019 р

Голова Вченої ради Навчально-наукового інституту Інформаційно-діагностичних систем

_____(Гумен М.Б.)

ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

протокол засідання №_____

від "_____"_____2019 р

Завідувач кафедри

_____(Корченко О.Г.)

ПОГОДЖЕНО

Науково-методично-редакційною радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол №____

від "_____"_____2019 р

Заступник голови НМР Навчально-наукового інституту Інформаційно-діагностичних систем

_____(Квасніков В.П.)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека, Адміністративний менеджмент у сфері захисту інформації) у складі:

КЕРІВНИК 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)

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

(підпис)

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

(підпис)

Рецензент Лахно В.А., завідувач кафедри комп'ютерних систем і мереж Національного університету біоресурсів і природокористування України, доктор технічних наук, професор.

Рецензії-відгуки зовнішніх стейкхолдерів (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	Національний авіаційний університет, Навчально-науковий інститут інформаційно-діагностичних систем, кафедра безпеки інформаційних технологій
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр з кібербезпеки, Науковий співробітник (інформаційна безпека), Професіонал із організації інформаційної безпеки
1.3.	Офіційна назва освітньо-професійної програми	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.	Наявність акредитації	Акредитовано, сертифікат про акредитацію УД 11008106 від 27 грудня 2018 року
1.6.	Цикл/рівень	FQ-EHEA – перший цикл, НРК – 8 рівень
1.7.	Передумови	Наявність ступеня бакалавра
1.8.	Мова(и) викладання	Українська
1.9.	Термін дії освітньо-професійної програми	1 липня 2024 р.
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.iids.nau.edu.ua http://www.bit.nau.edu.ua
Розділ 2. Мета освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками розробляти, використовувати і впроваджувати сучасні технології та методи захисту інформації на підприємстві	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна, базується на загально-відомих 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
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; – принципів супроводу систем та комплексів захисту інформації; – 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 оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних захищених інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування засобів захисту інформації.
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	Усі програми доктора філософії галузі знань «Інформаційні технології».
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання	Лекції, лабораторні роботи, семінари, практичні заняття, проектна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика на підприємствах, підготовка кваліфікаційної роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, кваліфікаційний екзамен, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні компетентності	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 проектами. ЗК9. Здатність ефективно формувати комунікаційну стратегію. ЗК10. Здатність приймати обгрунтовані 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 експеримент-тальних 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 проектів, дипломних робіт. ПРН17. Здатність володіння англійською мовою, використовувати спеціальну терміно-логію 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.

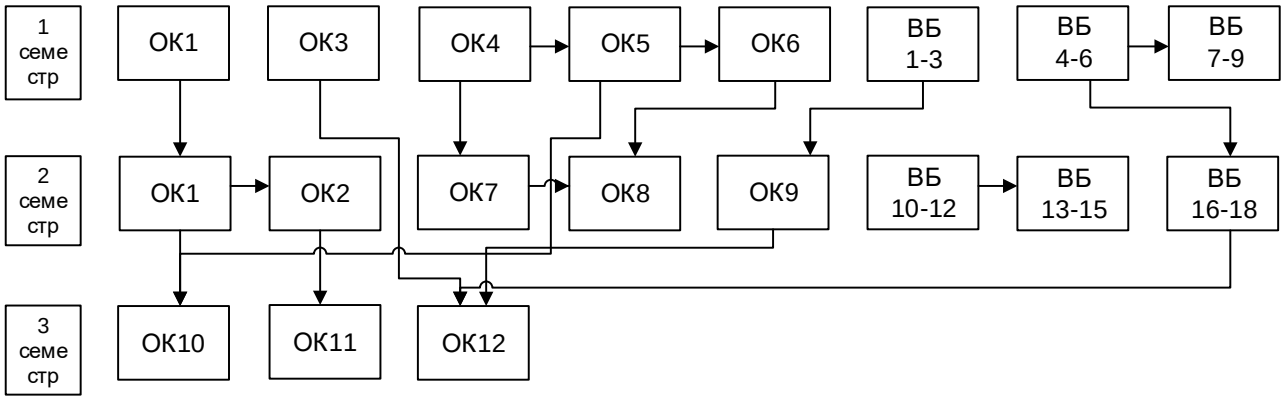
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК 1.	Ділова іноземна мова	4.0	Екзамен Диференційований залік
ОК 2.	Наукові комунікації у фаховій діяльності	4.0	Диференційований залік
ОК 3.	Методи побудови та аналізу криптосистем	4.0	Екзамен
ОК 4.	Методи моделювання та оптимізація процесів в сфері захисту інформації	4.0	Екзамен
ОК 5.	Методологія та організація наукових досліджень	4.0	Екзамен
ОК 6.	Кібербезпека	5.0	Диференційований залік
ОК 7.	Нормативно-правове забезпечення інформаційної безпеки	4.5	Екзамен
ОК 8.	Інтелектуалізовані системи інформаційної безпеки	6.0	Екзамен
ОК 9.	Науково-дослідна практика	4.5	Диференційований залік
ОК 10.	Переддипломна практика	7.5	Диференційований залік
ОК 11.	Кваліфікаційний екзамен	1.5	Екзамен
ОК 12.	Кваліфікаційна робота	18	Захист
Загальний обсяг обов'язкових компонент:		67 кредитів	
Вибіркові компоненти ОПП			
ВБ 1.	Технології підтримки прийняття рішень	5.0	Екзамен
ВБ 2.	Теорія підтримки прийняття рішень	5.0	Екзамен
ВБ 3.	Системи і методи прийняття рішень	5.0	Екзамен
ВБ 4.	Аудит інформаційної безпеки	3.0	Диференційований залік
ВБ 5.	Управління мережевою безпекою	3.0	Диференційований залік
ВБ 6.	Управління безпекою застосунків	3.0	Диференційований залік

ВБ 7.	Управління інцидентами інформаційної безпеки	3.0	Диференційований залік
ВБ 8.	Менеджмент інцидентів в інформаційно-комунікаційних системах	3.0	Диференційований залік
ВБ 9.	Розслідування інцидентів у кіберпросторі	3.0	Диференційований залік
ВБ 10.	Безпека в хмарних технологіях	4.0	Екзамен
ВБ 11.	Управління інформаційною безпекою в хмарних технологіях	4.0	Екзамен
ВБ 12.	Хмарні технології	4.0	Екзамен
ВБ 13.	Рекламно-інформаційний менеджмент	4.0	Диференційований залік
ВБ 14.	SEO-технології в управлінській діяльності	4.0	Диференційований залік
ВБ 15.	Засоби пошукової оптимізації	4.0	Диференційований залік
ВБ 16.	Управління безперервністю бізнесу	4.0	Диференційований залік
ВБ 17.	Системи забезпечення безперервності бізнесу	4.0	Диференційований залік
ВБ 18.	Управління бізнес-процесами в кризових ситуаціях	4.0	Диференційований залік
Загальний обсяг вибіркових компонент		23 кредити	
Загальний обсяг освітньо-професійної програми		90 кредитів	

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми проводиться у формі кваліфікаційного екзамену та захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому освітньої кваліфікації: Магістр з кібербезеки, із присвоєнням кваліфікації: Науковий співробітник (інформаційна безпека), Професіонал із організації інформаційної безпеки.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ВБ1 - ВБ 3	ВБ4 - ВБ 6	ВБ7 - ВБ 9	ВБ10 - ВБ 12	ВБ13- ВБ 15	ВБ16- ВБ 18
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	ОК11	ОК12	ВБ1 - ВБ 3	ВБ4 - ВБ 6	ВБ7 - ВБ 9	ВБ10 - ВБ 12	ВБ13- ВБ 15	ВБ16- ВБ 18
ПРН1			+															
ПРН2						+		+							+			+
ПРН3			+									+						
ПРН4				+		+												
ПРН5				+		+												
ПРН6						+			+	+		+		+	+	+		
ПРН7						+			+	+								
ПРН8								+										
ПРН9						+	+							+				
ПРН10		+			+	+			+			+						
ПРН11			+	+														
ПРН12																	+	
ПРН13		+			+													
ПРН14				+	+				+	+		+						
ПРН15		+			+								+	+				
ПРН16									+	+	+	+						
ПРН17	+																	

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

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

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

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

Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

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

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

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

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				