Проєкт

(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Управління інформаційною безпекою»
(найменування освітньої програми)
Першого (бакалаврського) 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

Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека. Затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1047

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:

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

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ЗАРІЦЬКИЙ О.В., д.т.н., доцент кафедри безпеки інформаційних технологій _____

(підпис)

ІВАНЧЕНКО І.С., к.т.н., доцент кафедри безпеки інформаційних технологій _____

(підпис)

СИДОРЕНКО В.М., к.т.н., старший викладач кафедри безпеки інформаційних технологій _____

(підпис)

БАЛАНДА А.А., студент кафедри безпеки інформаційних технологій, групи УБ-471 _____

(підпис)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР
ХЛАПОНІН Ю.І., д.т.н., проф.,
завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, _____

(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	Бакалавр Бакалавр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Управління інформаційною безпекою
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців (денна форма навчання)
1.5.	Акредитаційна інституція	Акредитовано, Акредитаційна комісія Міністерства освіти і науки України, сертифікат про акредитацію НД 1193809 від 31 жовтня 2017 року
1.6.	Період акредитації	1 липня 2027 р.
1.7.	Цикл/рівень	Сьомий кваліфікаційний рівень НРК України
1.8.	Передумови	Повна загальна середня освіта
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 та впровадженні сучасних систем управління інформаційною безпекою	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	Об'єкти діяльності: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення складових безпеки інформації: інформаційна безпека, кібербезпека, безпека інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Теоретичний зміст: Знання: – законодавчої, нормативно-правової бази України та вимог відповідних, в тому числі, міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; 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 інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення; автоматизованих

		систем проєктування.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма прикладної орієнтації, що базується на загально-відомих наукових в практичних результатах в галузі інформаційної безпеки, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації (за наявності)	Загальна вища освіта першого (бакалаврського) рівня спеціальності 125 Кібербезпека Ключові слова: кібербезпека, інформаційна безпека, управління інформаційною безпекою, криптографічні та технічні методи захисту інформації, захист персональних даних, захист інформації, захист від несанкціонованого доступу, кібербезпека проводових та безпроводових мереж, система менеджменту інформаційної безпеки.
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення основ: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів впровадження і супроводу систем управління інформаційною безпекою; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною безпекою; – методів та засобів виявлення, управління та ідентифікації ризиків та інцидентів інформаційної безпеки; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів і засобів технічного та крипто-графічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих засобів проєктування систем управління інформаційною безпекою. 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 «Управління інформаційною безпекою». Проведений аналіз показав необхідність продовжувати підготовку фахівців здатних використовувати і впроваджувати технології управління інформаційною та/або кібербезпекою, 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.

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 розробки та тестування програмного забезпечення; -фахівець з розроблення комп'ютерних програм; -фахівець з інформаційних технологій; -інспектор з організації захисту секретної інформації.
4.2.	Подальше навчання	Право продовжити навчання на другому (магістерському) 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, навчальний комп’ютерний практикум та фахова технологічна практика, підготовка кваліфікаційної роботи.
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 використовувати поглиблені теоретичні та фундаментальні знання для ефективного розв’язування складних спеціалізованих задач та практичних проблем під час професійної діяльності у галузі управління та адміністрування інформаційною безпекою, що характеризується комплексністю та неповною визначеністю умов.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Здатність до пошуку, оброблення та аналізу інформації. ЗК5. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
6.3.	Фахові компетентності (ФК)	ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, стандарти і рекомендовані практики з метою здійснення професійної діяльності в галузі інформаційної безпеки. ФК2. Здатність до використання інформаційно-

		комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики інформаційної безпеки підприємства. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних системах з метою реалізації інформаційної безпеки підприємства. ФК6. Здатність відновлювати штатне функціонування інформаційно-комунікаційних систем після реалізації кіберзагроз, здійснення кібератак, збоїв та відмов різних класів і походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації. ФК8. Здатність здійснювати процедури управління інцидентами інформаційної безпеки, проводити розслідування, надавати їм оцінку. ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК10. Здатність застосовувати методи та засоби криптографічного і технічного захисту інформації. ФК11. Здатність виконувати моніторинг процесів функціонування інформаційно-комунікаційних систем згідно встановленої політики інформаційної безпеки підприємства. ФК12. Здатність аналізувати, виявляти та оцінювати можливі кіберзагрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам підприємства (галузі, регіону, держави). ФК13. Здатність застосовувати методи теорії інформації та кодування, обробки та захисту інформації при наявності завад в каналах передачі даних. ФК14. Здатність застосовувати теоретичні знання та практичні навички із побудови, керування, модернізації, моніторингу та аналізу продуктивності сучасних інформаційно-комунікаційних систем. ФК15. Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання ефективного програмного забезпечення для керування обчислювальними ресурсами в багато користувальницьких операційних системах. ФК16. Здатність застосовувати методи та засоби організаційного характеру для побудови системи управління інформаційною безпекою. ФК17. Здатність застосовувати методи та засоби стеганографічного захисту інформації.

Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Розв'язувати задачі інформаційної безпеки за рахунок використання сучасних методів і засобів криптографічного захисту інформації. ПРН2. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня інформаційної безпеки. ПРН3. Визначати відомості, які відносяться до різних видів конфіденційної інформації, організовувати допуск та доступ персоналу до конфіденційної інформації згідно встановленої політики інформаційної безпеки підприємства. ПРН4. Організовувати внутрішньо об'єктовий та пропускний режими на підприємстві. ПРН5. Організовувати контроль за станом безпеки конфіденційної інформації на підприємстві згідно відповідної політики безпеки. ПРН6. Здатність продемонструвати знання та розуміння архітектури комп'ютерів та описати в загальних поняттях і термінах структуру комп'ютера та його апаратних компонентів, принципів їх взаємодії; систему команд; протоколи за засоби обміну даними; систему переривань; методику проєктування арифметичних та управляючих пристроїв; засоби підвищення продуктивності та надійності цифрової обчислювальної техніки. ПРН7. Здатність продемонструвати знання та розуміння основ побудови систем управління інформаційною безпекою та описати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії. ПРН8. Здатність продемонструвати знання та розуміння основ побудови комп'ютерних мереж та описати в загальних поняттях і термінах принципи та методи організації мережевих комунікацій; архітектуру та функціонування локальних, комбінованих і глобальних комп'ютерних мереж; систему мережевих стандартів, способи адресації та протоколи маршрутизації; інтерфейси та методи доступу до передавального середовища. ПРН9. Здатність продемонструвати знання та розуміння організації баз даних та розробляти проєкти баз даних інформаційних систем, використовуючи сучасні методи і моделі інформаційної безпеки. ПРН10. Здатність продемонструвати знання та розуміння системного програмування та розробляти системні програми, алгоритми обробки різних типів даних та тестування програмного забезпечення. ПРН11. Реалізовувати основи системного підходу, критерії ефективної організації обчислювального процесу для постановки та рішення завдань організації оптимального і безпечного функціонування обчислювальних систем.

		ПРН12. Вибирати, обґрунтовуючи свій вибір, оптимальні алгоритми керування ресурсами, порівнювати та оцінювати різні методи, що лежать в основі планування і диспетчеризації процесів. ПРН13. Здатність продемонструвати знання та розуміння системного програмного забезпечення та описати в загальних поняттях і термінах процеси функціонування операційних систем та їх складових частин, сучасних операційних середовищ та систем програмування, засоби та технології їх експлуатації та адміністрування. ПРН14. Здатність продемонструвати знання та розуміння технологій проєктування комп'ютерних систем інформаційної безпеки та виконувати системне, операційне, функціонально-логічне і технічне проєктування комп'ютерних пристроїв, використовуючи сучасні засоби автоматизованого проєктування. ПРН15. Здатність продемонструвати знання та розуміння діагностування та експлуатації систем інформаційної безпеки та застосовувати на практиці засоби автоматичного контролю і діагностування . ПРН16. Здатність продемонструвати знання та розуміння сучасних методів і моделей інформаційної безпеки. ПРН17. Здатність продемонструвати знання та розуміння інженерії програмного забезпечення та описати в загальних поняттях і термінах процеси, методи і засоби автоматизації проєктування, виробництва, випробувань та оцінки якості програмних продуктів; методи організації колективної розробки програмного забезпечення інформаційних систем; мовні засоби і специфікації інтерфейсів об'єктів програмування. ПРН18. Здатність продемонструвати знання та розуміння застосовування методів і засобів криптографічного та технічного захисту інформації. ПРН19. Здатність продемонструвати знання та розуміння професійної діяльності на основі впровадженої системи управління інформаційною безпекою. ПРН20. Здатність продемонструвати знання і розуміння інформаційної безпеки та обґрунтовано обирати і застосовувати на практиці методи виявлення інформаційних загроз; програмні та програмно-апаратні засоби захисту даних та операційних систем; методи протидії спробам несанкціонованого доступу до інформаційних ресурсів; організаційні та адміністративні заходи підвищення рівня інформаційної безпеки. ПРН21. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проєктів, дипломних робіт. ПРН22. 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

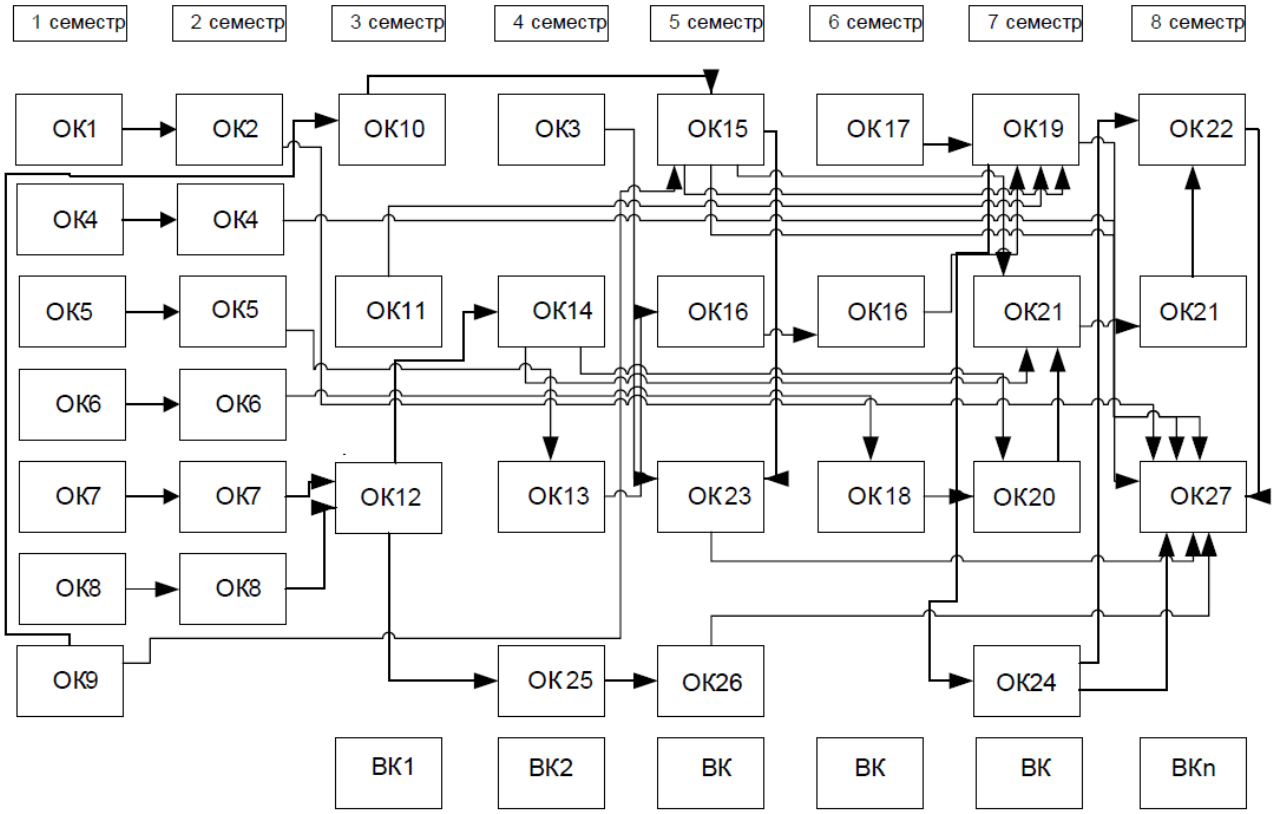
2.1. Перелік компонент

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.	Історія української державності та культури	3.0	Екзамен	1
ОК 2.	Ділова українська мова	3.0	Екзамен	2
ОК 3.	Філософія сталого розвитку	3.0	Екзамен	4
ОК 4.	Фахова іноземна мова	6.0	Диференційований залік Екзамен	1 2
ОК 5.	Вища математика	12.0	Диференційований залік Екзамен	1 2
ОК 6.	Фізика	12.0	Диференційований залік Диференційований залік	1 2
ОК 7.	Інформаційні технології	12.0	Диференційований залік Екзамен	1 2
ОК 8.	Основи автоматизованої обробки інформації	6.0	Диференційований залік Екзамен	1 2
ОК 9.	Основи кібербезпеки	6.0	Екзамен	1
ОК 10	Інформаційно-психологічні впливи в кіберпросторі	6.0	Екзамен	3
ОК 11	Стандарти інформаційної безпеки	6.0	Екзамен	3
ОК 12	Технології програмування	6.0	Екзамен	3
ОК 13	Дискретна математика	6.0	Екзамен	4
ОК 14	Операційні системи та системне програмне забезпечення	6.0	Екзамен	4
ОК 15	Управління ризиками інформаційної безпеки	6.0	Екзамен	5
ОК 16	Криптографія та криптоаналіз	9.0	Диференційований залік Екзамен	5 6
ОК 17	Основи системного аналізу	6.0	Екзамен	6
ОК 18	Технології штучного інтелекту	6.0	Екзамен	6
ОК 19	Комплексні системи захисту інформації	9.0	Екзамен	7
ОК 20	Інформаційне забезпечення управлінської діяльності	6.0	Екзамен	7
ОК 21	Системи управління інформаційною безпекою	6.0	Диференційований залік Екзамен	7 8
ОК 22	Інцидент-менеджмент у кіберпросторі	6.0	Екзамен	8
ОК 23	Наскрізний міждисциплінарний курсовий проєкт зі сталого розвитку	4.0	Курсовий проєкт	5
ОК 24	Наскрізний міждисциплінарний фаховий курсовий проєкт	5.0	Курсовий проєкт	7

ОК 25	Навчальний комп`ютерний практикум	6.0	Диференційований залік	4
ОК 26	Фахова технологічна практика	6.0	Диференційований залік	5
ОК 27	Кваліфікаційна робота	12.0		8
Загальний обсяг обов'язкових компонент:		180 кредитів		
Вибіркові компоненти				
ВК 1.	Дисципліна 1			
ВК 2.	Дисципліна 2			
...	…			
ВК n.	Дисципліна n			
Загальний обсяг вибіркових компонент*		60 кредити		
Загальний обсяг освітньо-професійної програми		240 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 захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезеки.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна робота має передбачати розв'язання складної задачі у сфері управління інформаційно безпекою, 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. 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	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ВК1	ВК2	…	ВКn
ІК		+			+			+	+					+	+				+		+	+			+		+				
ЗК1					+	+	+					+	+	+	+	+			+		+	+	+	+	+	+	+				
ЗК2			+						+	+	+			+		+			+		+	+	+	+	+		+				
ЗК3	+	+		+																											
ЗК4	+		+		+			+					+				+	+		+					+	+	+				
ЗК5	+	+								+	+																				
ФК1		+		+					+	+	+				+				+		+	+	+	+			+				
ФК2							+							+					+						+		+				
ФК3							+	+				+		+					+	+		+			+	+	+				
ФК4									+												+	+					+				
ФК5												+						+	+		+				+						
ФК6						+									+				+		+	+									
ФК7																			+		+										
ФК8					+								+									+									
ФК9																				+	+		+	+							
ФК10																+		+													
ФК11																		+			+										
ФК12	+		+						+	+					+							+					+				
ФК13																+											+				
ФК14														+			+										+				
ФК15							+							+		+				+							+				
ФК16															+				+		+	+					+				
ФК17																+											+				

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	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	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				+																							+				

** 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