

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет



ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи та технології кібербезпеки»

(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.



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:

КІНЗЕРЯВИЙ В.М., к.т.н., доцент кафедри безпеки
інформаційних технологій

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОРЧЕНКО О.Г., д.т.н., проф., завідувач кафедри
безпеки інформаційних технологій

(підпис)

СКВОРЦОВ С.О., к.т.н., доц., доцент кафедри
безпеки інформаційних технологій

(підпис)

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

(підпис)

ГОРОЖАНОВА А.О., студент кафедри безпеки
інформаційних технологій, групи СК-372

(підпис)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР

ВАСІЛІУ Є.В., д.т.н., проф.,
директор Навчально-наукового інституту
Радіо, телебачення та інформаційної безпеки
Одеської національної академії зв'язку ім. О.С. Попова,

(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)	Системи та технології кібербезпеки
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, Англійська
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 та технологій кібербезпеки здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу	
Розділ 3. Характеристика освітньо-професійної програми		
3.1.	Предметна область (Об'єкт діяльності, теоретичний зміст)	Об'єкти діяльності: 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, 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 проектування.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма прикладної орієнтації, що базується на загальновідомих 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, системи та технології кібербезпеки, криптографічний захист інформації, технічний захист інформації, захист персональних даних, антивірусний захист, захист від несанкціонованого доступу, кібербезпека провідних та безпроводових мереж.
3.4.	Особливості освітньо-професійної програми	<p>Програма передбачає вивчення основ:</p> <ul style="list-style-type: none">– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;– принципів супроводу систем кібербезпеки;– теорії, методів і моделей управління доступом до інформаційних ресурсів;– теорії систем управління кібербезпекою;– методів та засобів виявлення, управління та ідентифікації ризиків кібербезпеки;– методів та засобів оцінювання і забезпечення необхідного рівня кібербезпеки;– методів і засобів технічного та криптографічного захисту інформації;– захищених інформаційно-комунікаційних технологій;– сучасного програмно-апаратного забезпечення систем кібербезпеки тощо. <p>Постійний та систематичний моніторинг ринку освітніх послуг, аналіз вакансій і потенційних можливостей ринку праці, експертне опитування керівників і провідних спеціалістів підприємств різних форм власності стали основою з підготовки фахівців освітньо-професійної програми «Системи та технології кібербезпеки». Проведений аналіз показав необхідність продовжувати формування та реалізацію моделі підготовки фахівців здатних використовувати і впроваджувати сучасні системи та технології кібербезпеки, які володіють знаннями механізмів забезпечення безпеки та ефективними засобами обмежень ризиків в інформаційних системах. Це забезпечує можливість отримання якісної професійної освіти в галузі ІТ та робить вказану ОПП унікальною.</p>
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України : <ul style="list-style-type: none">- фахівець із організації інформаційної безпеки;- фахівець із організації захисту інформації з обмеженим доступом;- фахівець з режиму секретності ;- фахівець з розроблення комп'ютерних програм;



		<ul style="list-style-type: none">- 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, проектна 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 забезпечення інформаційної та/або кібербезпеки, що передбачає застосування сучасних систем та технологій кібербезпеки та характеризуються комплексністю та невизначеністю умов.
6.2.	Загальні компетентності (ЗК)	<p>ЗК1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>ЗК4. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК5. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>ЗК6. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій.</p>
6.3.	Фахові компетентності (ФК)	<p>ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, рекомендовані практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки.</p> <p>ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей кібербезпеки.</p> <p>ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації для забезпечення кібербезпеки.</p> <p>ФК4. Здатність забезпечувати неперервність бізнесу (роботи інформаційно-комунікаційних систем) згідно встановленої політики кібербезпеки.</p>



		<p>ФК5. Здатність забезпечувати захист інформації для реалізації встановленої політики кібербезпеки підприємства.</p> <p>ФК6. Здатність відновлювати штатне функціонування інформаційно-комунікаційних систем після реалізації кіберзагроз, збоїв і відмов різних класів та походження.</p> <p>ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.</p> <p>ФК8. Здатність розробляти і здійснювати процедури управління кіберінцидентами, проводити розслідування, надавати їм оцінку.</p> <p>ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління кібербезпекою.</p> <p>ФК10. Здатність застосовувати методи та засоби криптографічного і технічного захисту інформації для забезпечення кібербезпеки.</p> <p>ФК11. Здатність виконувати моніторинг процесів функціонування інформаційно-комунікаційних систем згідно встановленої політики кібербезпеки підприємства.</p> <p>ФК12. Здатність аналізувати, виявляти та оцінювати можливі кіберзагрози, уразливості та дестабілізуючі чинники інформаційному простору та критичним інформаційним ресурсам.</p> <p>ФК13. Здатність застосовувати теоретичні знання і практичні навички щодо побудови, модернізації, моніторингу та аналізу безпеки і продуктивності сучасних інформаційних та комунікаційних систем.</p> <p>ФК14. Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання безпечного програмного забезпечення для керування обчислювальними ресурсами в багато-користувацьких операційних системах.</p> <p>ФК15. Здатність застосовувати методи і засоби організаційного характеру щодо захисту інформації на об'єктах критичної інфраструктури держави.</p> <p>ФК16. Здатність застосовувати методи і засоби стеганографічного захисту інформації.</p>
Розділ 7. Програми результати навчання		
7.1.	Програмні результати навчання	<p>ПРН1. Здійснювати вибір і оцінку систем передачі даних та протоколів, визначати основні параметри каналу зв'язку для подальшої передачі інформації.</p> <p>ПРН2. Розв'язувати задачі кібербезпеки та захисту інформації, що циркулює в інформаційно-комунікаційних системах, з використанням сучасних методів та засобів криптографії.</p> <p>ПРН3. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня кібербезпеки.</p>



		<p>ПРН4. Визначати відомості, які відносяться до різних видів інформації з обмеженим доступом, організувати допуск та доступ персоналу до інформації з обмеженим доступом згідно встановленої політики кібербезпеки.</p> <p>ПРН5. Організувати контроль за станом кібербезпеки інформації з обмеженим доступом на підприємстві.</p> <p>ПРН6. Здатність демонструвати знання та розуміння основ комп'ютерної електроніки та описати в загальних поняттях і термінах принципи дії, основні характеристики, параметри і особливості застосування електронних напівпровідникових приладів та інтегральних схем, що використовуються в обчислювальній техніці, автоматичних пристроях, комп'ютерних системах та мережах.</p> <p>ПРН7. Здатність демонструвати знання та розуміння основ комп'ютерної схемотехніки та описати в загальних поняттях і термінах характеристики, параметри, фізичні принципи побудови та логічні основи функціонування цифрових елементів; номенклатуру і функціональне призначення інтегральних мікросхем; типові схеми функціональних вузлів комп'ютерів; методику їх аналізу та розрахунку з використанням пакетів програм систем автоматизованого проектування.</p> <p>ПРН8. Здатність демонструвати 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 проектування арифметичних та управляючих пристроїв; засоби підвищення продуктивності та надійності цифрової обчислювальної техніки.</p> <p>ПРН9. Здатність демонструвати знання та розуміння основ побудови систем кібербезпеки та описати в загальних поняттях і термінах архітектуру, характеристики і принципи їх дії.</p> <p>ПРН10. 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 середовища передавання.</p> <p>ПРН11. Здатність демонструвати знання та розуміння організації баз даних та розробляти проекти захищених баз даних інформаційних систем, використовуючи сучасні методи і моделі кібербезпеки.</p> <p>ПРН12. Здатність демонструвати знання та</p>
--	--	--



		<p>розуміння системного програмування та розробляти захищені системні програми, алгоритми обробки різних типів даних та тестування програмного забезпечення.</p> <p>ПРН13. Реалізувати основи системного підходу, критерії ефективної організації обчислювального процесу для постановки та вирішення завдань організації оптимального функціонування обчислювальних систем.</p> <p>ПРН14. Вибирати, обґрунтовуючи свій вибір, оптимальні алгоритми керування ресурсами, порівнювати та оцінювати різні методи, що лежать в основі планування і диспетчеризації процесів, розробляти алгоритми прикладних програм на основі архітектури "клієнт-сервер".</p> <p>ПРН15. Здатність демонструвати 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.</p> <p>ПРН16. Здатність демонструвати знання та розуміння технологій проектування систем кібербезпеки та виконувати системне, функціонально-логічне і технічне проектування комп'ютерних пристроїв, використовуючи сучасні засоби автоматизованого проектування.</p> <p>ПРН17. Здатність демонструвати знання і розуміння діагностування та експлуатації комп'ютерних систем кібербезпеки та застосовувати на практиці засоби автоматичного контролю і діагностування .</p> <p>ПРН18. Здатність демонструвати знання та розуміння сучасних методів і моделей кібербезпеки.</p> <p>ПРН19. Здатність демонструвати знання та розуміння застосування методів та засобів криптографічного і технічного захисту інформації.</p> <p>ПРН20. Здатність демонструвати знання та розуміння професійній діяльності на основі впровадженної системи кібербезпеки.</p> <p>ПРН21. Здатність продемонструвати знання та розуміння захисту інформації у комп'ютерних системах та обґрунтовано обирати і застосовувати на практиці методи виявлення кіберзагроз; програмні та програмно-апаратні засоби захисту даних та операційних систем; методи протидії спробам несанкціонованого доступу до інформаційних ресурсів; організаційні та адміністративні заходи підвищення рівня кібербезпеки.</p> <p>ПРН22. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проєктів, дипломних робіт.</p> <p>ПРН23. Здатність володіння англійською мовою, використовувати спеціальну термінологію для проведення літературного пошуку.</p>
--	--	--



Розділ 8. Ресурсне забезпечення реалізації програми

8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напрямку 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+K1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЄС.
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 проекти (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	1
			Екзамен	2
ОК 5.	Вища математика	12.0	Диференційований залік	1
			Екзамен	2
ОК 6.	Фізика	12.0	Диференційований залік	1
			Диференційований залік	2
ОК 7.	Інформаційні технології	12.0	Диференційований залік	1
			Екзамен	2
ОК 8.	Основи автоматизованої обробки інформації	6.0	Диференційований залік	1
			Екзамен	2
ОК 9.	Основи кібербезпеки	6.0	Екзамен	1
ОК 10	Інформаційно-психологічні впливи в кіберпросторі	6.0	Екзамен	3
ОК 11	Захищені комп'ютерні системи та мережі	6.0	Екзамен	3
ОК 12	Технології програмування	6.0	Екзамен	3
ОК 13	Дискретна математика	6.0	Екзамен	4
ОК 14	Прогнозування та моделювання у соціальних інтернет-сервісах	6.0	Екзамен	4
ОК 15	Ризик-менеджмент	6.0	Екзамен	5
ОК 16	Криптографія та криптоаналіз	9.0	Диференційований залік	5
			Екзамен	6
ОК 17	Технології виявлення уразливостей інформаційних систем	6.0	Екзамен	6
ОК 18	Тестування безпеки інформаційних систем	6.0	Екзамен	6
ОК 19	Операційні системи та системне програмне забезпечення	6.0	Екзамен	7
ОК 20	Комплексні системи захисту інформації	9.0	Екзамен	7
ОК 21	Системи управління інформаційною безпекою	6.0	Диференційований залік	7
			Екзамен	8
ОК 22	Інцидент-менеджмент у кіберпросторі	6.0	Екзамен	8
ОК 23	Наскрізний міждисциплінарний курсовий проект зі сталого розвитку	4.0	Курсовий проект	5
ОК 24	Наскрізний міждисциплінарний фаховий	5.0	Курсовий проект	7

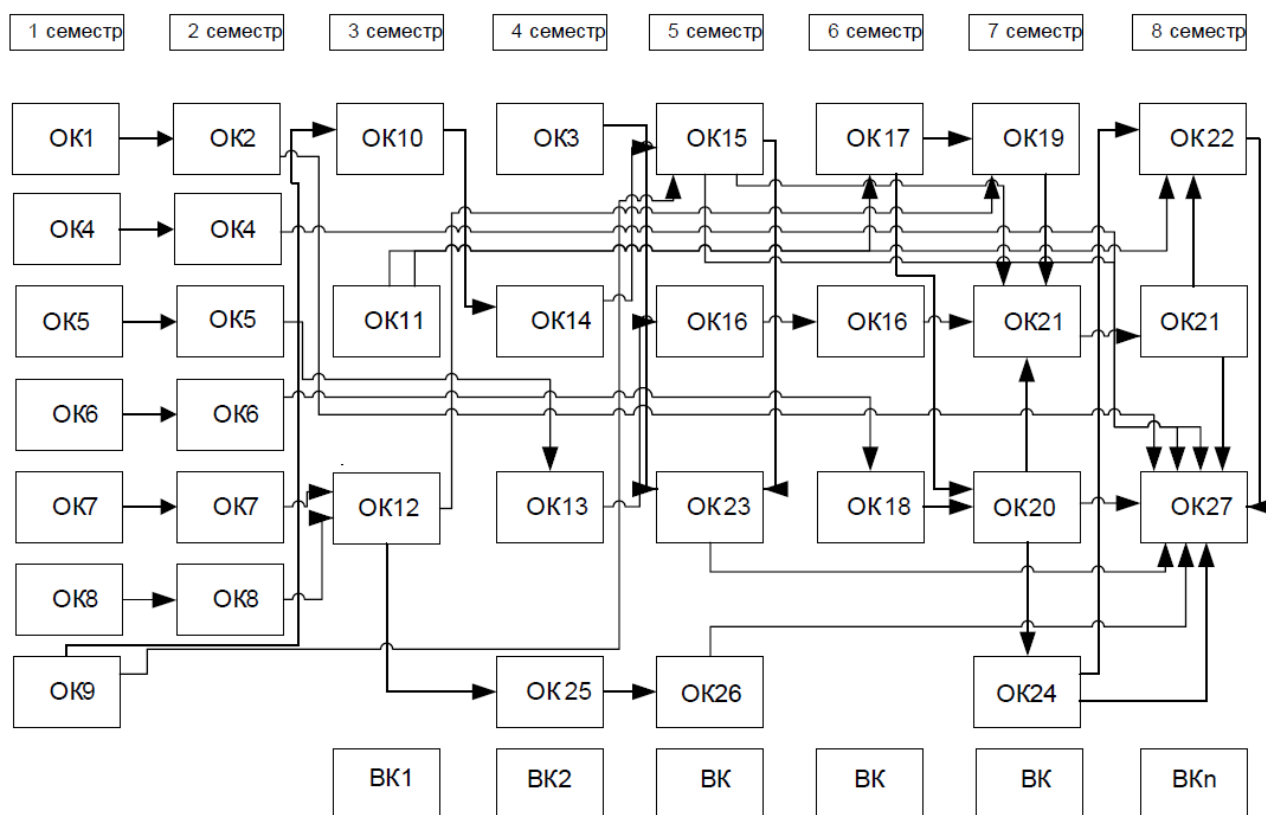


	курсний проект			
ОК 25	Навчальний комп'ютерний практикум	6.0	Диференційований залік	4
ОК 26	Фахова технологічна практика	6.0	Диференційований залік	5
ОК 27	Кваліфікаційна робота	12.0		8
Загальний обсяг обов'язкових компонент:		180 кредитів		
Вибіркові компоненти				
ВК 1.	Дисципліна 1			
ВК 2.	Дисципліна 2			
...	...			
ВК n.	Дисципліна n			
Загальний обсяг вибірових компонент*		60 кредити		
Загальний обсяг освітньо-професійної програми		240 кредитів		

**Вибіркові компоненти обираються здобувачами вищої освіти із загальноуніверситетського та фахового переліків вибірових дисциплін Університету, які в свою чергу щороку оновлюються та затверджуються рішенням Ради з якості Національного авіаційного університету. Методика формування переліків та процедура вибору вибірових 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 кібербезпеки.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна робота має передбачати розв'язання складної задачі у сфері систем та технологій 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. Обов'язковою умовою є наявність презентації.



4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	BK1	BK2	...	BKn
ІК		+					+	+	+		+	+			+				+		+	+			+		+				
ЗК1		+		+	+	+	+	+	+	+	+	+	+		+	+			+	+	+	+	+	+	+	+	+				
ЗК2											+					+			+	+	+	+	+	+	+		+				
ЗК3	+	+		+						+				+												+	+	+			
ЗК4	+		+		+				+	+			+	+											+	+	+				
ЗК5							+				+				+	+			+	+	+	+			+		+				
ЗК6	+								+	+														+	+		+				
ФК1		+		+											+					+	+	+	+	+			+				
ФК2							+				+			+			+	+	+	+	+				+		+				
ФК3							+		+		+	+					+		+	+	+	+			+		+				
ФК4																			+		+	+					+				
ФК5											+	+									+	+				+					
ФК6						+									+			+		+	+	+									
ФК7																					+	+									
ФК8					+																	+									
ФК9																					+				+						
ФК10									+							+		+													
ФК11									+	+							+	+			+										
ФК12	+		+											+	+		+	+				+	+				+				
ФК13											+			+				+									+				
ФК14							+		+		+					+											+				
ФК15																				+	+	+					+				
ФК16									+	+						+											+				



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	БК1	БК2	...	БКn	
ПРН1							+	+			+							+														
ПРН2																+												+				
ПРН3					+								+			+	+	+														
ПРН4									+												+	+										
ПРН5								+													+				+							
ПРН6						+		+						+			+											+				
ПРН7								+			+																					
ПРН8								+												+				+								
ПРН9									+		+								+	+	+			+				+				
ПРН10							+				+								+								+					
ПРН11							+					+		+					+									+				
ПРН12							+					+						+	+													
ПРН13								+		+				+							+				+							
ПРН14							+					+								+												
ПРН15												+								+												
ПРН16											+										+					+						
ПРН17																					+	+										
ПРН18									+	+					+		+	+			+	+										
ПРН19					+								+			+																
ПРН20																					+	+				+	+					
ПРН21										+	+			+						+	+		+									
ПРН22	+	+	+				+					+					+	+		+	+		+					+				
ПРН23				+																								+				

* 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 ознайомлення	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