ПРОЕКТ

(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»
(найменування ОПП)

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)

галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

СМЯ НАУ ОПП 09.01.10 – 01 – 2020

Освітньо-професійна програма
затверджена Вченою радою Університету
Протокол № ____ від _____2020 р.

Вводиться в дію наказом ректора

Ректор

_____ _____

Наказ № ____ від _____2020 р.

КИЇВ

Стандарт вищої освіти України: перший (бакалаврський) рівень
галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від «04» жовтня 2018 р. № 1074.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Радою з якості Національного авіаційного університету

протокол № _____

від «___» _____ 20___ р.

Голова Ради з якості

_____ _____

ПОГОДЖЕНО

Вченою радою факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № _____

від «___» _____ 20___ р.

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

_____ (_____)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № ____

від «___» _____ 20__ р.

Завідувач кафедри

_____ (_____)

ПОГОДЖЕНО

Студентською радою факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № ____

від «___» _____ 20__ р.

Голова Студентською ради факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ (_____)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (спеціальності 125 "Кібербезпека") у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ТЕМНІКОВ В.О. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В. – д.т.н., професор, завідувач кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____

(підпис)

ЛАЗАРЕНКО С.В. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____

(підпис)

ШВЕЦЬ В.А. – к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____

(підпис)

ВОЙТЕНКО С.Д. – к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____

(підпис)

_____ _____

(П.І.Б. здобувача вищої освіти) (підпис)

ЗОВНІШНІ СТЕЙКХОЛДЕРИ

Толюпа С.В. – д.т.н., професор, професор кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

_____

(підпис)

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 Факультет кібербезпеки, комп'ютерної та програмної інженерії Кафедра засобів захисту інформації
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 технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців (денна форма навчання) / 4 роки 6 місяців (заочна форма навчання). Диплом бакалавра, одиничний, 180 кредитів ЄКТС (скорочений термін навчання), термін навчання 2 роки 10 місяців навчання (денна форма навчання) / 3 роки 6 місяців (заочна форма навчання).
1.5.	Акредитаційна інституція	Міністерство освіти і науки України, рішення Акредитаційної комісії від 18.01.2017 сертифікат серія НД-ІІ № 1181256
1.6.	Період акредитації	По 01.07.2022 р., чергова
1.7.	Цикл/рівень	6 рівень Національної рамки кваліфікацій України (НРК України), перший цикл Європейського простору вищої освіти (FQ-EHEA), 6 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Вступ на навчання на освітню програму обсягом 240 кредитів ЄКТС здійснюється на базі повної загальної середньої освіти при наявності атестату. Вступ на навчання на скорочений термін освітньої програми обсягом 180 кредитів ЄКТС здійснюється на базі ОС молодшого бакалавра, а також передбачений для осіб, які мають диплом про вищу освіту (ОС бакалавр, ОКР спеціаліст, ОС магістр) за будь-якою іншою спеціальністю, якщо академічна різниця із змістом попередньої освіти не перевищує 30 кредитів. Умови вступу визначаються Правилами прийому до НАУ, затвердженими вченою радою Університету.

1.9.	Форма навчання	Інституційна з елементами дистанційної: очна, заочна, мережева.
1.10.	Мова(и) викладання	Українська
1.11.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Метою ОПП «Системи технічного захисту інформації, автоматизація її обробки» є підготовка висококваліфікованих фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями інформаційної та/або кібербезпеки та специфічними знаннями особливостей професійної діяльності в авіаційному секторі, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації. ОПП «Системи технічного захисту інформації, автоматизація її обробки» відповідає місії НАУ, у якій наголошується, щодо внеску НАУ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і практики, так і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям при підготовці фахівців з Кібербезпеки в авіаційно-космічній галузі.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об’єкт діяльності, теоретичний зміст)	Об’єкт діяльності: системи та комплекси технічного захисту інформації на об’єктах інформаційної діяльності; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків). Теоретичний зміст предметної області: методи та засоби технічного захисту інформації, технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів.
3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію. Базується на загальновідомих положеннях, результатах сучасних наукових досліджень та нових знаннях в галузі інформаційних технологій, необхідних для майбутньої професійної діяльності бакалаврів з Кібербезпеки, здатних вирішувати певні проблеми і задачі за умови оволодіння системою загальних та фахових компетентностей.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації (за наявності)	Спеціальна освіта та професійна підготовка в галузі 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. Ключові слова: технічний захист інформації, інформаційна та/або кібербезпека, захист інформації.

3.4.	Особливості освітньо-професійної програми	Освітньо-професійна програма передбачає: – обов'язкове проходження переддипломної практики; – застосування законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – застосування практичних навичок у сфері технічного захисту інформації; – використання принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – використання теорії, моделей та принципів управління доступом до інформаційних ресурсів; – застосування теорії систем управління інформаційною та/або кібербезпекою; – практичного використання методів та засобів виявлення та локалізації каналів витоку інформації; – застосування методів та засобів виявлення, управління та ідентифікації ризиків; – практичного використання методів та засобів виявлення закладних пристроїв; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – практичного використання методів та засобів технічного та криптографічного захисту інформації; – застосування сучасних інформаційно-комунікаційних технологій; – використання сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – практичного використання автоматизованих систем проектування. На відміну від інших освітніх програм увага приділяється автоматизованим системам та комплексам технічного захисту інформації.

Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники отримують можливість працевлаштування на підприємствах (організаціях, установах) різних форм власності в галузі Інформаційних технологій за спеціальністю Кібербезпека на посадах, визначених чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010) та обіймати посади в інших секторах економіки при наявності сертифікатів про опанування відповідних програм підготовки.
4.2.	Подальше навчання	Можливість продовження навчання за програмами другого (магістерського) циклу вищої освіти (НРК України - 7 рівень, FQ-EHEA - другий цикл, EQF LLL - 7 рівень).
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	*Методи, засоби та технології:* Проблемно-орієнтоване навчання, яке передбачає формулювання та вирішення проблеми під час лекцій, розв`язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи здобувачів вищої освіти. Практико-орієнтоване навчання через різні види практик на підприємствах, установах та організаціях різних форм власності на підставі договорів про проходження практики, організація якої здійснюється за принципом неперервності. Виконання практичних та лабораторних робіт в умовах виробництва. Технології дистанційного навчання, що реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій; дистанційних занять, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів й інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб-технологій. Інформаційні технології навчання: робота здобувачів вищої освіти у спеціалізованих кабінетах облаштованих мультимедійними комплексами, що забезпечує можливість проведення інтерактивних лекцій та віртуальних лабораторних робіт, застосування пошукової методики здобуття нових знань, організації проєктної роботи, проведення комп'ютеризованого тестового контролю якості знань.

		Проектні технології навчання реалізуються через наскрізні міждисциплінарні курсові проекти зі сталого розвитку та фахового спрямування. *Інструменти та обладнання:* матеріали, апаратно-програмні комплекси та засоби лінійного/просторового захисту інформації, комбіновані системи контролю та управління доступом, проектування систем технічного захисту інформації; засоби технологічного, інформаційного, інструментального, метрологічного та організаційного забезпечення освітнього процесу.
5.2.	Оцінювання	Усні, письмові, творчі, тестові та комбіновані екзамени, диференційовані заліки, лабораторні звіти, звіти із практичних робіт та практик, реферати, захист курсових проектів, презентації, поточний контроль, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні Компетентності (ІК)	ІК1. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, 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 професійною спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. Здатність використовувати технічні засоби захисту та охорони інформаційних ресурсів і баз даних обмеженого доступу. ЗК7. Здатність організовувати функціонування системи організаційно-службових і спеціальних (охоронних) заходів із забезпечення інформаційної та/або кібербезпеки установ, підприємств, організацій. ЗК8. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного)

6.2.	Загальні компетентності (ЗК)	суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК9. 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, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
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 інформаційної та/або кібербезпеки. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об’єктах інформаційної діяльності. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем та комплексів технічного захисту інформації після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

6.3.	Фахові компетентності (ФК)	ФК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. ФК12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв. ФК13. Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки. ФК14. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК15. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН2. Застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН3. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

7.1.	Програмні результати навчання (ПРН)	ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН5. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних у галузі інформаційної та\або кібербезпеки. ПРН6. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН7. Розробляти моделі загроз та порушника. ПРН8. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН9. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН10. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН11. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН12. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН13. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН14. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

7.1.	Програмні результати навчання (ПРН)	ПРН15. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної та\або кібербезпеки. ПРН16. Виявляти небезпечні сигнали технічних засобів. ПРН17. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН18. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН19. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН20. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН21. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів. ПРН22. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН23. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. ПРН24. Організовувати внутрішньо-об’єктовий та пропускний режими на підприємстві.

7.1.	Програмні результати навчання (ПРН)	ПРН25. Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об’єкті інформаційної діяльності. ПРН26. Складати звітність та вести технічну документацію.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Кадрове забезпечення відповідає ліцензійним вимогам. У освітньому процесі беруть участь доктори та кандидати наук, професори та доценти, старші викладачі й асистенти за спеціальністю 125 Кібербезпека та за іншими спеціальностями, які забезпечують підготовку бакалаврів з Кібербезпеки. До організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП: – забезпеченість комп'ютерними робочими місцями та прикладними комп'ютерними програмами достатнє для виконання навчальних планів; – усі комп’ютери кафедри під’єднані до локальної мережі університету з можливістю виходу в глобальну мережу Інтернет; – для ведення документації та забезпечення навчально-методичними матеріалами освітнього процесу кафедра в достатній кількості забезпечена оргтехнікою (принтерами, МФУ, сканерами); – навчальні лабораторії оснащені технічними засобами та спеціалізованим програмним забезпеченням, необхідними приладами та обладнанням (охоронними системами відеоспостереження, засобами та комплексами виявлення закладних пристроїв, засобами просторового та мережевого захисту інформації). Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі, наявна соціальна інфраструктура включає спортивний комплекс, пункти харчування, центр творчості, медпункт і базу відпочинку.

8.3	Інформаційне та навчально-методичне забезпечення	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки НАУ. Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment). 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	Національна кредитна мобільність здобувачів вищої освіти, наукових і науково-педагогічних працівників, у т.ч. навчання, стажування, проведення наукових досліджень, викладання та підвищення кваліфікації організовується на підставі партнерських угод про співпрацю між Національним авіаційним університетом та закладами вищої освіти в Україні: – Національним технічним університетом України «Київським політехнічним інститутом імені Ігоря Сікорського»; – Харківським національним університетом радіоелектроніки.
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	**Іноземці та особи без громадянства,** які проживають в Україні на законних підставах, мають право на здобуття вищої освіти за освітньо-професійною програмою нарівні з громадянами України. Умовою зарахування іноземців на навчання для отримання певного освітнього ступеня є володіння ними мовою навчання на рівні, достатньому для засвоєння навчального матеріалу. Іноземці зараховуються на навчання за освітньо-професійною програмою до НАУ за результатами співбесіди.

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

2.1. Перелік освітніх компонент ОПП, 240 кредитів ЄКТС

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				
Ядро програми (Core), (*soft-skills*)				
ОК1.	Історія української державності та культури	3.0	Екзамен	1
ОК2.	Ділова українська мова	3.0	Екзамен	2
ОК3.	Філософія сталого розвитку	3.0	Екзамен	4
ОК4.	Фахова іноземна мова	6.0	Залік, екзамен	1, 2
ОК5.	Вища математика	12.0	Залік, екзамен	1, 2
ОК6.	Фізика	12.0	Залік	1, 2
Професійно-практична підготовка (Major)				
ОК7.	Інформаційні технології	12.0	Залік, екзамен	1, 2
ОК8.	Основи автоматизованої обробки інформації	6.0	Екзамен, залік	1, 2
ОК9.	Вступ до інформаційної безпеки	6.0	Екзамен	1
ОК10.	Основи проектування систем технічного захисту інформації	6.0	Екзамен	3
ОК11.	Схемотехніка пристроїв технічного захисту інформації	6.0	Екзамен	3
ОК12.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	6.0	Екзамен	3
ОК13.	Засоби передавання сигналів в системах технічного захисту інформації	6.0	Екзамен	4
ОК14.	Безпека інформаційно-комунікаційних систем	6.0	Екзамен	4
ОК15.	Контрольно-вимірювальна апаратура систем технічного захисту інформації	6.0	Екзамен	5
ОК16.	Поля і хвилі в системах технічного захисту інформації	6.0	Екзамен	5
ОК17.	Теорія інформації та кодування	6.0	Екзамен	6
ОК18.	Мікропроцесори в системах технічного захисту інформації	6.0	Екзамен	6
ОК19.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	6.0	Екзамен	6, 7

1	2	3	4	5
ОК20.	Технічні засоби охорони об'єктів	6.0	Екзамен	7
ОК21.	Організаційно-технічне забезпечення систем технічного захисту інформації	6.0	Екзамен	7
ОК22.	Захист інформації методами криптографії та стеганографії	6.0	Залік, екзамен	7, 8
ОК23.	Методи та засоби технічного захисту інформації	6.0	Екзамен	8
Курсове проєктування				
Наскрізний міждисциплінарний курсовий проект зі сталого розвитку (*soft-skills*)		4,0	захист	3, 4, 5з
Наскрізний міждисциплінарний фаховий курсовий проект		5,0	захист	6, 7з
Практична підготовка				
ОК24.	Фахова схемотехнічна практика	6.0	Залік	4
ОК25.	Фахова технологічна практика	6.0	Залік	5
ОК26.	Фахова виробнича практика. Виконання кваліфікаційної роботи	12.0	Залік	8
	Захист кваліфікаційної роботи		Захист	
Загальний обсяг обов'язкових компонент:		180 кредитів ЄКТС		
Варіативні компоненти*				
ВК1. ВК2. ВК3. ВК4.	Загальноуніверситетський вибір (*soft-skills*)	12.0	заліки	3, 4, 5, 6
ВК5. ВК6. ВК7. --- ВК20.	Фаховий вибір	48	заліки	3, 4, 5, 6, 7, 8
Загальний обсяг варіативних компонент*		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		240 кредитів ЄКТС		

2.2. Перелік освітніх компонент для скороченого терміну навчання, 180 кредитів ЄКТС

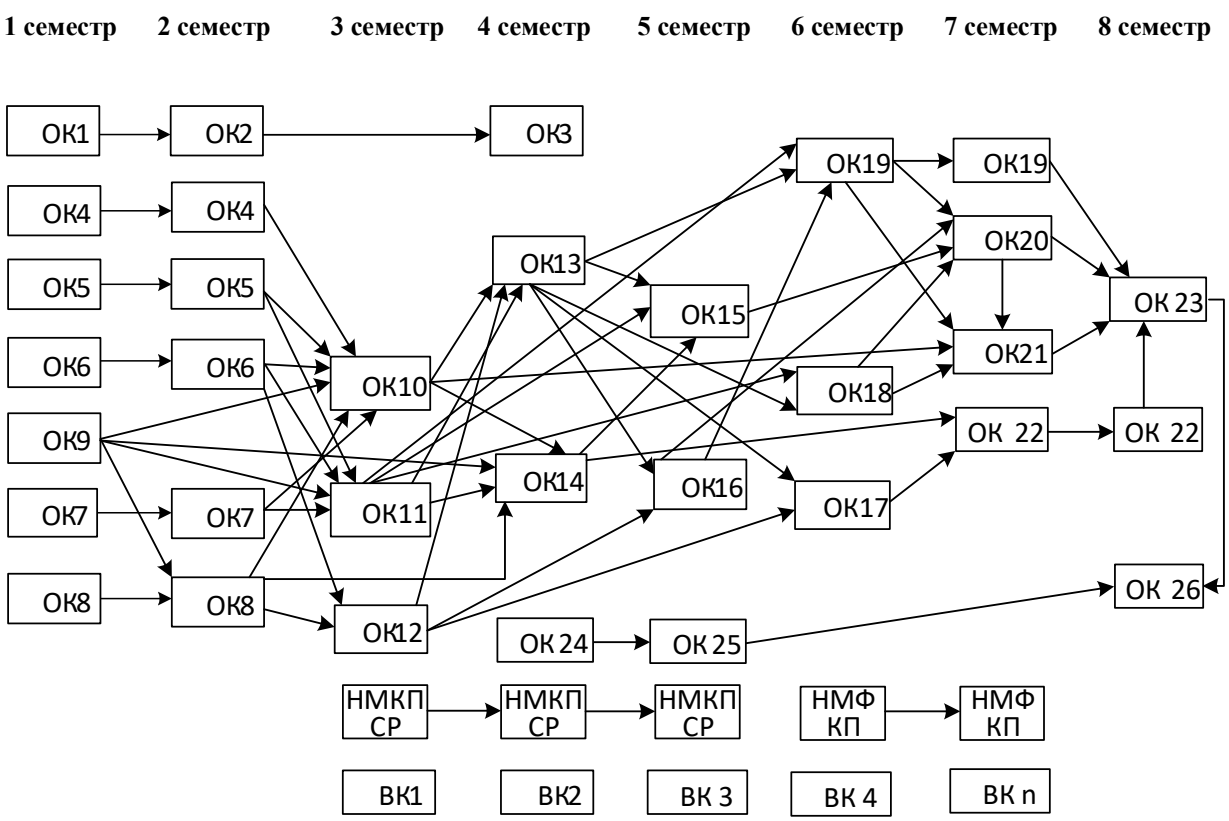
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
Ядро програми (Core), (*soft-skills*)				
ОК3.	Філософія сталого розвитку	3.0	Екзамен	2
ОК4.	Фахова іноземна мова	2.0	Залік, екзамен	1, 2
ОК5.	Вища математика	3.0	Залік	1
Професійно-практична підготовка (Major)				
ОК10.	Основи проектування систем технічного захисту інформації	5.0	Екзамен	1
ОК11.	Схемотехніка пристроїв технічного захисту інформації	6.0	Екзамен	1
ОК12.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	8.0	Залік, екзамен	1, 2
ОК13.	Засоби передавання сигналів в системах технічного захисту інформації	6.0	Екзамен	2
ОК15.	Контрольно-вимірювальна апаратура систем технічного захисту інформації	6.0	Екзамен	3
ОК16.	Поля і хвилі в системах технічного захисту інформації	6.0	Екзамен	3
ОК17.	Теорія інформації та кодування	6.0	Екзамен	4
ОК18.	Мікропроцесори в системах технічного захисту інформації	6.0	Екзамен	4
ОК19.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	6.0	Екзамен	4, 5
ОК20.	Технічні засоби охорони об'єктів	6.0	Екзамен	5
ОК21.	Організаційно-технічне забезпечення систем технічного захисту інформації	6.0	Екзамен	5
ОК22.	Захист інформації методами криптографії та стеганографії	6.0	Залік, екзамен	5, 6
ОК23.	Методи та засоби технічного захисту інформації	6.0	Екзамен	6
Курсове проектування				
Наскрізний міждисциплінарний курсовий проект зі сталого розвитку (*soft-skills*)		4,0	захист	1, 2, 3з
Наскрізний міждисциплінарний фаховий курсовий проект		5,0	захист	4, 5з

1	2	3	4	5
Практична підготовка				
ОК24.	Фахова схемотехнічна практика	6.0	Залік	2
ОК25.	Фахова технологічна практика	6.0	Залік	3
ОК26.	Фахова виробнича практика. Виконання кваліфікаційної роботи	12.0	Залік	6
	Захист кваліфікаційної роботи		Захист	
Загальний обсяг обов'язкових компонент:		120 кредитів ЄКТС		
Варіативні компоненти*				
Вибір із переліку (Discrete Electives)				
ВК1. ВК2. ВК3. ВК4.	Загальноуніверситетський вибір (*soft-skills*)	12.0	заліки	1, 2, 3, 4
ВК5. ВК6. ВК7. --- ВК20.	Фаховий вибір	48	заліки	1, 2, 3, 4, 5, 6
Загальний обсяг варіативних компонент*		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		180 кредитів ЄКТС		

* *Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ.*

Варіативні 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 здобувачів ОС «Бакалавр» здійснюється у формі публічного захисту кваліфікаційної бакалаврської роботи і завершується видачею документу встановленого зразку про присудження їм освітнього ступеня «Бакалавр» із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки, за спеціальністю 125 «Кібербезпека».
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота бакалавра повинна бути самостійною логічно завершеною теоретичною або експериментальною науково-дослідною роботою, пов'язаною з вирішенням актуальної науково-технічної або іншої проблеми у сфері Кібербезпеки. Кваліфікаційна робота бакалавра не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті Університету або його структурного підрозділу, або у репозитарії.

	Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснювати відповідно до вимог законодавства.
Вимоги до публічного захисту (демонстрації)	Публічний захист кваліфікаційної бакалаврської роботи відбувається на засіданні екзаменаційної комісії. Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	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		ВК 1*	ВК 2*	ВК 3*	ВК 4*	ВК n*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
ІК1	+			+	+	+	+	+	+	+	+	+	+	+		+	+	+		+	+	+	+	+	+	+	+					
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+					
ЗК2							+		+	+	+			+	+		+	+		+	+	+	+	+	+	+	+					
ЗК3	+			+																				+	+	+	+					
ЗК4	+			+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+					
ЗК5	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+					
ЗК6						+	+		+					+							+		+	+	+	+	+					
ЗК7						+	+		+					+						+	+		+	+	+	+	+					
ЗК8	+	+	+																					+	+	+						
ЗК9	+	+	+						+																							
ФК1	+			+					+	+				+						+	+		+	+	+	+	+					
ФК2				+	+	+	+		+	+	+	+	+	+	+	+		+			+			+	+	+	+					
ФК3					+	+	+			+	+			+			+	+			+	+	+	+	+	+	+					
ФК4							+	+	+	+	+	+		+		+	+	+		+	+	+	+	+	+	+	+					
ФК5						+			+					+	+					+			+	+	+	+	+					
ФК6										+	+		+					+	+	+	+		+		+	+						
ФК7							+			+	+	+	+	+	+	+	+	+	+		+	+			+	+	+					
ФК8							+	+		+	+		+	+			+	+	+		+		+		+	+	+					
ФК9							+		+					+			+								+	+	+					
ФК10					+	+																+	+		+	+						
ФК11							+		+	+	+			+	+	+	+	+			+		+		+	+	+					
ФК12						+				+	+	+	+	+	+	+		+	+	+	+		+		+	+	+					

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
ФК13					+	+		+			+	+	+		+	+		+	+	+				+	+	+	+					
ФК14							+					+		+			+							+	+	+	+					
ФК15	+			+				+		+	+		+		+			+	+	+	+		+	+	+	+	+					

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

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

Компоненти / Програмні результати навчання	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		ВК 1*	ВК 2*	ВК 3*	ВК 4*	ВК n*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
ПРН1	+	+	+	+					+																							
ПРН2	+			+																			+	+	+	+	+					
ПРН3					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+					
ПРН4	+			+	+	+	+		+	+			+	+		+	+	+	+	+	+	+	+		+	+	+					
ПРН5	+			+					+	+				+						+	+	+	+	+	+	+	+					
ПРН6	+			+					+	+				+							+		+								
ПРН7	+			+	+	+		+	+	+				+							+		+		+	+	+					
ПРН8										+			+	+				+	+		+		+		+	+	+					
ПРН9					+	+	+			+	+		+	+			+	+	+	+	+	+	+		+	+	+					
ПРН10								+			+		+	+				+	+	+					+	+	+					
ПРН11										+			+	+				+	+	+	+	+	+		+	+	+					
ПРН12							+			+				+			+				+	+	+		+	+	+					
ПРН13									+	+				+						+	+		+		+	+	+					
ПРН14					+	+	+		+					+			+					+		+	+	+	+					
ПРН15	+			+					+	+	+		+	+				+	+	+	+		+		+	+	+					
ПРН16						+					+	+			+	+		+								+						
ПРН17					+	+						+			+	+							+	+	+	+						
ПРН18						+						+			+	+											+	+				
ПРН19	+			+				+		+					+						+		+		+	+	+					
ПРН20					+					+	+				+									+		+	+					
ПРН21	+			+					+	+		+		+	+	+				+	+	+	+		+	+	+					
ПРН22									+	+				+							+	+			+	+	+					

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
ПРН23									+	+				+							+		+		+	+	+					
ПРН24								+		+			+						+	+	+		+		+	+	+					
ПРН25								+		+	+		+		+			+	+	+	+		+		+	+	+					
ПРН26	+			+				+		+	+				+			+		+	+		+	+	+	+	+					

** 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.*

6. Система внутрішнього забезпечення якості вищої освіти НАУ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та освітньої діяльності НАУ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності, затвердженого рішенням вченої ради Університету від 28.11.2018 (протокол № 8) та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 № 1556-VII (Розділ V Забезпечення якості вищої освіти, ст.16).

7. Перелік нормативних документів, на яких базується освітньо-професійна програма

1. «Про освіту»: Закон України від 05.09.2017 № 2145-VIII [Електронний ресурс]. – режим доступу: http://zakon.rada.gov.ua/laws/show/2145-19

2. «Про вищу освіту»: Закон України від 01.07.2014 № 1556-VII [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18

3. Постанова Кабінету Міністрів України від 25.06.2020 р. № 519 «Про внесення змін у додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341».

4. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29.04.2015 р. № 266 [Електронний ресурс]. – режим доступу: http://zakon2.rada.gov.ua/laws/show/266-2015-%D0%BF

5. Класифікація видів економічної діяльності : ДК 009:2010. – На заміну ДК 009:2005; Чинний від 2012-01-01. – (Національний класифікатор України).

6. Класифікатор професій ДК 003:2010. – На заміну ДК 003:2005; Чинний від 2010-11-01. –(Національний класифікатор України).

7. Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека». Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074.

(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				