

ПРОЕКТ

(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет



ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Аудит кібербезпеки»

(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

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «АУДИТ КІБЕРБЕЗПЕКИ» - Першого (бакалаврського) рівня вищої освіти за спеціальністю: <u>125 «Кібербезпека»</u> галузі знань: <u>12 «Інформаційні технології»</u>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 01 - 2020
		стор. 2 з 24	

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 Студентської ради факультету
кібербезпеки, комп'ютерної та
програмної інженерії

_____ (_____)

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «АУДИТ КІБЕРБЕЗПЕКИ» - Першого (бакалаврського) рівня вищої освіти за спеціальністю: <u>125 «Кібербезпека»</u> галузі знань: <u>12 «Інформаційні технології»</u></p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 01 - 2020
		стор. 3 з 24	

ПЕРЕДМОВА

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

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ВОЙТЕНКО С.Д. – к.т.н., доцент, доцент 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)

ТЕМНІКОВ В.О. – д.т.н., доцент, доцент 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)

_____ (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)	Аудит 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) / 4 роки 6 місяців (заочна форма навчання).
1.5.	Акредитаційна інституція	-
1.6.	Період акредитації	-
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. 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 «Аудит кібербезпеки» 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 «Аудит кібербезпеки» 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: аудит інформаційної та/або кібернетичної безпеки, системи та комплекси 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 аудиту інформаційної та/або кібербезпеки, технології створення, обробки, передачі, приймання, знищення, відображення та 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: аудит кібербезпеки, 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 принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – використання методів та засобів проведення аудиту та сертифікації інформаційної та/або кібернетичної безпеки; – впровадження методів оцінки ефективності системи аудиторського контролю у галузі управління операційною діяльністю та підтримкою ІТ; – застосування теорії систем управління інформаційною та/або кібербезпекою; – використання методів та засобів виявлення та локалізації каналів витоку інформації; – застосування методів та засобів виявлення, управління та ідентифікації ризиків; – використання методів та засобів



		<p>оцінювання та забезпечення необхідного рівня захищеності інформації;</p> <ul style="list-style-type: none">– впровадження методів та засобів технічного та криптографічного захисту інформації;– використання сучасних інформаційно-комунікаційних технологій та програмно-апаратного забезпечення;– автоматизованих систем проектування;– встановлення рівня відповідності інформаційних систем визначеним критеріям стандартів аудиту кібербезпеки. <p>На відміну від інших освітніх програм увага приділяється аудиту та сертифікації інформаційної та/або кібернетичної безпеки.</p>
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	<p>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.</p>
4.2.	Подальше навчання	<p>Можливість продовження навчання за програмами другого (магістерського) циклу вищої освіти (НРК України - 7 рівень, FQ-EHEA - другий цикл, EQF LLL - 7 рівень).</p>
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	<p><i>Методи, засоби та технології:</i></p> <p>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.</p> <p>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.</p> <p>Технології дистанційного навчання, що реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій; дистанційних занять, конференцій,</p>



5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	<p>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.</p> <p>Проєктні технології навчання реалізуються через наскрізні міждисциплінарні курсові проєкти зі сталого розвитку та фахового спрямування.</p> <p><i>Інструменти та обладнання:</i> матеріали, апаратно-програмні комплекси, засоби технологічного, інформаційного, інструментального, метрологічного та організаційного забезпечення освітнього процесу.</p>
5.2.	Оцінювання	<p>Усні, письмові, творчі, тестові та комбіновані екзамени, диференційовані заліки, лабораторні звіти, звіти із практичних робіт та практик, реферати, захист курсових проєктів, презентації, поточний контроль, захист кваліфікаційної роботи.</p>
Розділ 6. Програмні компетентності		
6.1.	Інтегральні Компетентності (ІК)	<p>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.</p>
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 професійною спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>ЗК5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК6. Здатність адаптуватися до нових теоретичних і практичних досягнень в області аудиту інформаційної та/або кібербезпеки.</p>



6.2.	Загальні компетентності (ЗК)	<p>ЗК7. Здатність планувати та проводити аудит інформаційної та/або кібербезпеки.</p> <p>ЗК8. 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.</p> <p>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.</p>
6.3.	Фахові компетентності (ФК)	<p>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.</p> <p>ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.</p> <p>ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності.</p> <p>ФК6. Здатність здійснювати розробку, впровадження та моніторинг системних і логічних засобів контролю інформаційної та/або кібербезпеки.</p> <p>ФК7. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту</p>



6.3.	Фахові компетентності (ФК)	<p>інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).</p> <p>ФК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>ФК10. Здатність здійснювати аудит організаційної та процесної складової безпеки, оцінку технічної захищеності (сканування і тестування на проникнення), оцінку рівня стійкості методам соціальної інженерії (фішинг, вішинг), аудит «тіньових» ІТ, оцінку безпеки процесів аутсорсингу.</p> <p>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.</p> <p>ФК12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв.</p> <p>ФК13. Здатність визначати інформаційні і технічні ресурси, а також об'єкти інформаційної діяльності, які підлягають захисту.</p> <p>ФК14. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК15. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації та звітності.</p>
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	<p>ПРН1. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ПРН2. Застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.</p> <p>ПРН3. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; адаптуватися в умовах частоті зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p>



7.1.	Програмні результати навчання (ПРН)	<p>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.</p> <p>ПРН5. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних у галузі інформаційної та/або кібербезпеки.</p> <p>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.</p> <p>ПРН7. Розробляти моделі загроз та порушника.</p> <p>ПРН8. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.</p> <p>ПРН9. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.</p> <p>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.</p> <p>ПРН11. Планувати, організувати та проводити аудит інформаційної та/або кібербезпеки.</p> <p>ПРН12. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>ПРН13. 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.</p>
------	-------------------------------------	--



7.1.	Програмні результати навчання (ПРН)	<p>ПРН14. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.</p> <p>ПРН15. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.</p> <p>ПРН16. 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.</p> <p>ПРН17. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ПРН 18. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.</p> <p>ПРН19. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.</p> <p>ПРН20. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</p> <p>ПРН21. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.</p> <p>ПРН22. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.</p> <p>ПРН23. Визначати відомості, які відносяться до інформації з обмеженим доступом, організувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.</p> <p>ПРН24. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних</p>
------	-------------------------------------	--



7.1.	Програмні результати навчання (ПРН)	<p>(автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ПРН25. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.</p> <p>ПРН26. Приймати участь у розробці та впровадженні стратегії інформаційної та/або кібербезпеки відповідно до цілей і завдань організації.</p> <p>ПРН27. Складати аудиторську звітність та вести технічну документацію.</p>
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	<p>Кадрове забезпечення відповідає ліцензійним вимогам.</p> <p>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.</p> <p>До організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.</p>
8.2.	Матеріально-технічне забезпечення	<p>Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП:</p> <ul style="list-style-type: none">– 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. <p>Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі, наявна соціальна інфраструктура включає спортивний комплекс, пункти харчування, центр творчості, медпункт і базу</p>



8.3	Інформаційне та навчально-методичне забезпечення	<p>відпочинку.</p> <p>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.</p> <p>Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment).</p> <p>Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua</p> <p>Читальний зал забезпечений бездротовим доступом до мережі Інтернет.</p> <p>Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua</p>
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	<p>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:</p> <ul style="list-style-type: none">– Національним технічним університетом України «Київським політехнічним інститутом імені Ігоря Сікорського»;– Харківським національним університетом радіоелектроніки.
9.2.	Міжнародна кредитна мобільність	<p>У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЄС.</p>
9.3.	Навчання іноземних здобувачів вищої освіти	<p>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.</p> <p>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.</p>



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«АУДИТ КІБЕРБЕЗПЕКИ» -
Першого (бакалаврського) рівня вищої освіти
за спеціальністю: 125 «Кібербезпека»
галузі знань: 12 «Інформаційні технології»

Шифр
документа


СМЯ НАУ ОПП
09.01.10 – 01 - 2020

стор. 14 з 24

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				
<i>Ядро програми (Core), (soft-skills)</i>				
OK1.	Історія української державності та культури	3.0	Екзамен	1
OK2.	Ділова українська мова	3.0	Екзамен	2
OK3.	Філософія сталого розвитку	3.0	Екзамен	4
OK4.	Фахова іноземна мова	6.0	Залік, екзамен	1, 2
OK5.	Вища математика	12.0	Залік, екзамен	1, 2
OK6.	Фізика	12.0	Залік	1, 2
<i>Професійно-практична підготовка (Major)</i>				
OK7.	Інформаційні технології	12.0	Залік, екзамен	1, 2
OK8.	Основи автоматизованої обробки інформації	6.0	Екзамен, залік	1, 2
OK9.	Вступ до інформаційної безпеки	6.0	Екзамен	1
OK10.	Операційні системи	6.0	Екзамен	3
OK11.	Стандарти аудиту інформаційних технологій	6.0	Екзамен	3
OK12.	Політики, стандарти і процедури інформаційної безпеки	6.0	Екзамен	3
OK13.	Оцінка ризиків інформаційних технологій	6.0	Екзамен	4
OK14.	Планування аудиту кібербезпеки	6.0	Екзамен	4
OK15.	Захист інформації	6.0	Екзамен	5
OK16.	Аудиторська звітність	6.0	Екзамен	5
OK17.	Технології збору та аналізу даних аудиту	6.0	Екзамен	6
OK18.	Доступ до об'єктів інформаційної діяльності	6.0	Екзамен	6
OK19.	Стратегія управління системою інформаційної безпеки	6.0	Екзамен	6, 7
OK20.	Управління ризиками в інформаційних системах	6.0	Екзамен	7
OK21.	Процеси зберігання, вилучення, транспортування та утилізації інформаційних ресурсів	6.0	Екзамен	7

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «АУДИТ КІБЕРБЕЗПЕКИ» - Першого (бакалаврського) рівня вищої освіти за спеціальністю: <u>125 «Кібербезпека»</u> галузі знань: <u>12 «Інформаційні технології»</u>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 01 - 2020
		стор. 15 з 24	

1	2	3	4	5
OK22.	Розробка, впровадження та моніторинг системних і логічних засобів контролю безпеки	6.0	Залік, екзамен	7, 8
OK23.	Управління інцидентами кібербезпеки	6.0	Екзамен	8
<i>Курсове проектування</i>				
Наскрізний міждисциплінарний курсовий проект зі сталого розвитку (<i>soft-skills</i>)		4,0	захист	3, 4, 5з
Наскрізний міждисциплінарний фаховий курсовий проект		5,0	захист	6, 7з
<i>Практична підготовка</i>				
OK24.	Фахова схемотехнічна практика	6.0	Залік	4
OK25.	Фахова технологічна практика	6.0	Залік	5
OK26.	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.	Загальноуніверситетський вибір (<i>soft-skills</i>)	12.0	заліки	3, 4, 5, 6
ВК2.				
ВК3.				
ВК4.				
ВК5.	Фаховий вибір	48	заліки	3, 4, 5, 6, 7, 8
ВК6.				
ВК7.				

ВК20.				
Загальний обсяг варіативних компонент*		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		240 кредитів ЄКТС		

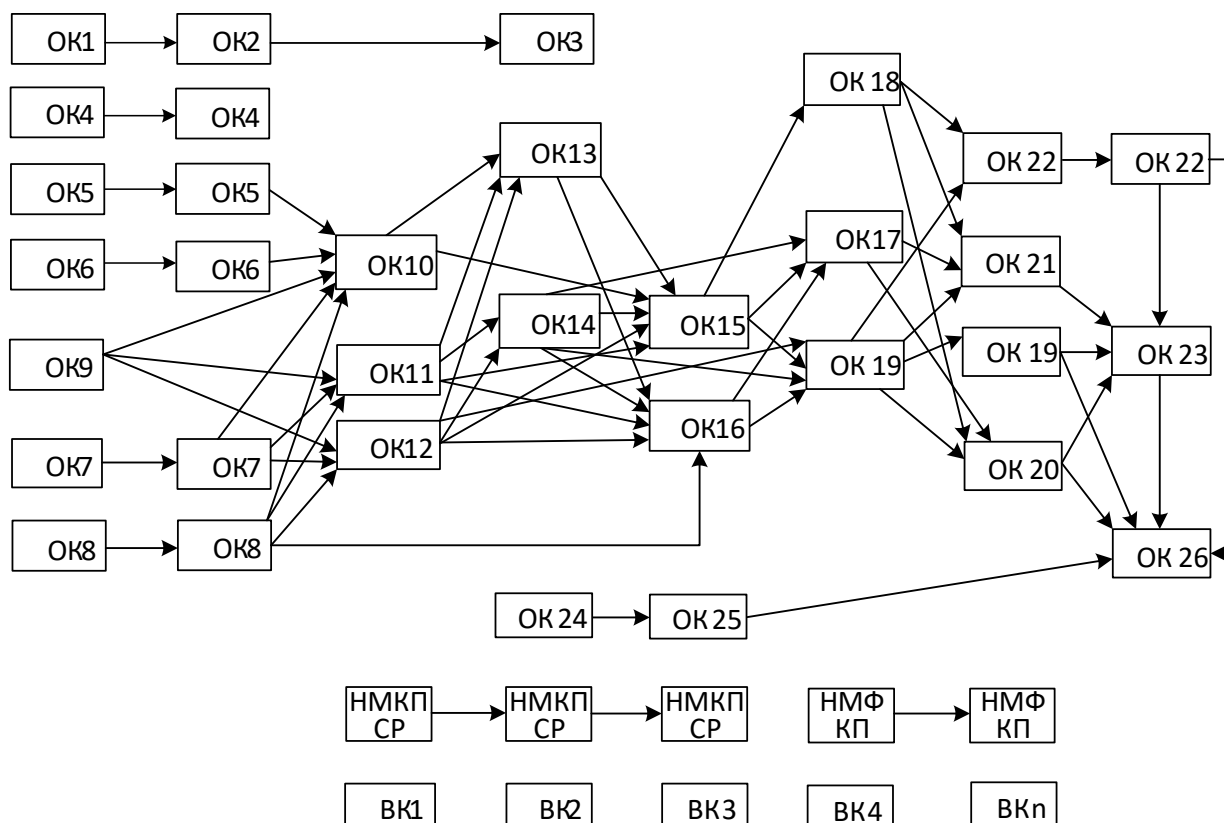
* Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ.

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

1 семестр 2 семестр 3 семестр 4 семестр 5 семестр 6 семестр 7 семестр 8 семестр



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 видачою документа 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.



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«АУДИТ КІБЕРБЕЗПЕКИ» -
Першого (бакалаврського) рівня вищої освіти
за спеціальністю: 125 «Кібербезпека»
галузі знань: 12 «Інформаційні технології»

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 01 - 2020

стор. 17 з 24

	<p>Кваліфікаційна робота бакалавра не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації.</p> <p>Кваліфікаційна робота має бути оприлюднена на офіційному сайті Університету або його структурного підрозділу, або у репозитарії.</p> <p>Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснювати відповідно до вимог законодавства.</p>
Вимоги до публічного захисту (демонстрації)	<p>Публічний захист кваліфікаційної бакалаврської роботи відбувається на засіданні екзаменаційної комісії.</p> <p>Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.</p>



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«АУДИТ КІБЕРБЕЗПЕКИ» -
Першого (бакалаврського) рівня вищої освіти
за спеціальністю: 125 «Кібербезпека»
галузі знань: 12 «Інформаційні технології»

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 01 - 2020

стор. 188 з 24

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти Компетентності	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	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					+	+	+		+	+		+			+		+							+	+	+	+					



Система менеджменту якості
 ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
 «АУДИТ КІБЕРБЕЗПЕКИ» -
 Першого (бакалаврського) рівня вищої освіти
 за спеціальністю: 125 «Кібербезпека»
 галузі знань: 12 «Інформаційні технології»

Шифр
 документа

СМЯ НАУ ОПП
 09.01.10 – 01 - 2020

стор. 19 з 24

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 вибіркового компонента визначається виходячи із загального обсягу вибіркового компонента (кредитів) освітньої програми.



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«АУДИТ КІБЕРБЕЗПЕКИ» -
Першого (бакалаврського) рівня вищої освіти
за спеціальністю: 125 «Кібербезпека»
галузі знань: 12 «Інформаційні технології»

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 01 - 2020

стор. 20 з 24

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*		
	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	+			+					+		+	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+					



Система менеджменту якості
 ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
 «АУДИТ КІБЕРБЕЗПЕКИ» -
 Першого (бакалаврського) рівня вищої освіти
 за спеціальністю: 125 «Кібербезпека»
 галузі знань: 12 «Інформаційні технології»


Шифр
 документа

СМЯ НАУ ОПП
 09.01.10 – 01 - 2020

стор. 21 з 24

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	
ПРН22							+		+	+	+	+	+	+	+				+	+	+	+		+	+	+	+						
ПРН23									+			+			+				+	+		+			+	+	+	+					
ПРН24							+	+		+	+	+	+		+	+	+	+		+				+	+	+	+						
ПРН25							+		+	+	+	+					+		+					+	+	+	+						
ПРН26	+			+			+	+	+		+	+	+	+	+				+	+		+		+	+	+	+						
ПРН27	+							+						+	+	+		+			+	+		+	+	+	+						

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


	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА <u>«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ</u> <u>АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»</u> (найменування ОПП)</p>	Шифр документа	СМЯ НАУ ОПП 14.01.04 – 01 - 2019
		стор. 22 з 24	

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.

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ» (найменування ОПП)</p>	Шифр документа	СМЯ НАУ ОПП 14.01.04 – 01 - 2019
		стор. 24 з 24	

(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	Анульованого			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				