

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет



## ОСВІТНЬО-НАУКОВА ПРОГРАМА

«Кібербезпека»

(повна назва освітньо-професійної програми)

третього (освітньо-наукового) рівня вищої освіти

за спеціальністю 125 - Кібербезпека

(шифр та найменування спеціальності)

галузі знань 12 - Інформаційні технології

(шифр та найменування галузі знань)


СМЯ НАУ ОНП \_\_\_\_\_ – \_\_\_\_\_ – 2021

Освітньо-наукова програма  
Затверджена Вченою радою  
Національного авіаційного  
університету  
протокол № \_\_\_\_\_ від \_\_\_\_\_ 2021 р.

Вводиться в дію наказом ректора  
Ректор  
\_\_\_\_\_ М. Луцький

Наказ № \_\_\_\_\_ від \_\_\_\_\_ 2021 р.

КИЇВ

	<b>ОСВІТНЬО-НАУКОВА ПРОГРАМА</b> «Кібербезпека» Спеціальність 125 - Кібербезпека Галузь знань 12 - Інформаційні технології Рівень вищої освіти - третій (освітньо-науковий)	Шифр документа	СМЯ НАУ ОНП ____ - 0_ - 2021
		Стор. 2 з 21	

Діє як тимчасова до введення стандарту вищої освіти України за спеціальністю 125 - Кібербезпека, галузі знань 12 – Інформаційні технології для третього (освітньо-наукового) рівня вищої освіти

## ЛИСТ ПОГОДЖЕННЯ освітньо-наукової програми

### ПОГОДЖЕНО

Науково-методичною радою Національного авіаційного університету

Протокол № \_\_\_\_

від « \_\_\_\_ » \_\_\_\_\_ 2021 р.

Голова науково-методичної ради

\_\_\_\_\_ / Полухін А. В.

### ПОГОДЖЕНО

Вченою радою факультету кібербезпеки, комп'ютерної та програмної інженерії

Протокол № \_\_\_\_

від « \_\_\_\_ » \_\_\_\_\_ 2021 р.

Голова вченої ради факультету

\_\_\_\_\_ / Нестеренко К.С.

### ПОГОДЖЕНО

В.о. проректора з наукової роботи

\_\_\_\_\_ / Радченко О.В.

від « \_\_\_\_ » \_\_\_\_\_ 2021 р.

### ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

Протокол № \_\_\_\_

від « \_\_\_\_ » \_\_\_\_\_ 2021 р.

Завідувач кафедри

\_\_\_\_\_ / Корченко О.Г.

### ПОГОДЖЕНО

Науковим товариством студентів, докторантів та молодих учених НАУ


Протокол № \_\_\_\_

від « \_\_\_\_ » \_\_\_\_\_ 2021 р.

Голова Наукового товариства студентів, докторантів та молодих учених НАУ

\_\_\_\_\_ / Одарченко Р. С.



	<p>ОСВІТНЬО-НАУКОВА ПРОГРАМА «Кібербезпека» Спеціальність 125 - Кібербезпека Галузь знань 12 - Інформаційні технології Рівень вищої освіти - третій (освітньо-науковий)</p>	Шифр документа	СМЯ НАУ ОНП ____ - 0_ - 2021
		Стор. 4 з 21	


Педченко Євгеній Максимович

Pre-SaleEngineer, ТОВ «ІНТРАСИСТЕМС», Україна

Рівень документа – 3б

Плановий термін між ревізіями – 1 рік

**Контрольний примірник**

	<p>ОСВІТНЬО-НАУКОВА ПРОГРАМА «Кібербезпека» Спеціальність 125 - Кібербезпека Галузь знань 12 - Інформаційні технології Рівень вищої освіти - третій (освітньо-науковий)</p>	Шифр документа	СМЯ НАУ ОНП ____ – 0_ – 2021
		Стор. 5 з 21	

## 1. Профіль освітньо-наукової 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	Доктор філософії / Doctor of Philosophy (Ph.D) Доктор філософії з кібербезпеки / Doctor of Philosophy of Cybersecurity
1.3	Офіційна назва освітньо-наукової програми	Освітньо-наукова програма «Кібербезпека»
1.4	Тип диплому та обсяг освітньо-наукової програми	Диплом доктора філософії, одиничний; перший науковий ступінь, що здобувається на третьому (освітньо-науковому) рівні вищої освіти; 4 академічних роки; освітня складова – 50 кредитів ЄКТС.
1.5	Акредитаційна інституція	Національне агентство забезпечення якості вищої освіти
1.6	Період акредитації	Підлягає акредитації вперше
1.7	Цикл / рівень	Третій (освітньо-науковий) рівень QF for ENEA – третій цикл, EQF for LLL – 8 рівень; НРК України – 8 рівень
1.8	Передумови	Наявність освітнього ступеня магістра або освітньо-кваліфікаційного рівня спеціаліст спеціальності 125 Кібербезпека чи спорідненої / еквівалентної спеціальності (зокрема, за результатами процедури визнання іноземних документів про освіту для іноземців)
1.9	Форма навчання	Інституційна з елементами дистанційної: очна, заочна
1.10	Мови викладання	Українська та / або англійська
1.11	Інтернет-адреса постійного розміщення опису освітньо-наукової програми	<a href="https://nau.edu.ua/ua/menu/quality/ects/zagalna-informatsiya/informatsiya-po-osvitnih-programah.html">https://nau.edu.ua/ua/menu/quality/ects/zagalna-informatsiya/informatsiya-po-osvitnih-programah.html</a>
Розділ 2. Ціль освітньо-наукової програми		
2.1	Ціллю освітньо-наукової програми <b>Підготовки Докторів Філософії за спеціальністю 125 Кібербезпека</b> є відтворення інтелектуального потенціалу держави шляхом підготовки висококваліфікованих на національному та міжнародному рівнях наукових кадрів з <b>Кібербезпеки</b> для наукових та освітніх установ, органів державної влади та управління, підприємств усіх форм власності в	



ОСВІТНЬО-НАУКОВА ПРОГРАМА  
«Кібербезпека»  
Спеціальність 125 - Кібербезпека  
Галузь знань 12 - Інформаційні технології  
Рівень вищої освіти - третій (освітньо-науковий)

Шифр  
документа

СМЯ НАУ  
ОНП \_\_\_\_ - 0\_ - 2021

Стор. 6 з 21

	<p>галузі <b>12 - Інформаційних технологій</b> та інших галузей через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і практики, а також формування у здобувачів вищої освіти (аспірантів) цінностей фаховості, прозорості, чесності та відкритості, соціальної відповідальності за результати наукової та науково-педагогічної діяльності перед суспільством, принципів міждисциплінарного підходу, розвитку і трансферу наукових досліджень. ОП «Кібербезпека» відповідає місії НАУ. У освітньо-наукової програми немає аналогів серед ЗВО України.</p>	
<b>Розділ 3. Характеристика освітньо-професійної (наукової) програми</b>		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	Галузь знань – 12 - Інформаційні технології Спеціальність (освітня) – 125 Кібербезпека
3.2	Орієнтація освітньо-наукової програми	Академічна відповідно до Міжнародної стандартної класифікації освіти (ISCED 2011 / UNESCO)
3.3	Основний фокус освітньо-наукової програми	Формування у здобувачів вищої освіти (аспірантів) здатності розв'язувати комплексні проблеми професійної та / або дослідницько-інноваційної діяльності в області <b>Кібербезпеки</b> та інших галузях, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та / або професійної практики.
3.4	Особливості освітньо-наукової програми	<ol style="list-style-type: none"><li>1. Організаційне забезпечення підготовки докторів філософії здійснюється через аспірантуру Національного авіаційного університету.</li><li>2. Організація освітньо-наукового процесу на основі системи методів проблемно-розвиваючого навчання та методології наукових досліджень, яка ґрунтується на принципах цілеспрямованості, бінарності (безпосередня взаємодія викладача та аспіранта, наукового керівника та аспіранта, наукового керівника та викладача для корекції процесу підготовки кожного аспіранта залежно від його індивідуальних потреб), показовому, діалогічному, евристичному, дослідницькому та програмованому методах.</li><li>3. Диференціація років підготовки за спрямованістю:<ul style="list-style-type: none"><li>– перший та другий рік підготовки – домінування освітньої складової у поєднанні за науковою;</li><li>– третій та четвертий рік підготовки – домінування наукової складової у поєднанні з освітньою (науково-педагогічною діяльністю).</li></ul></li><li>4. Можливість зарахування до 5 кредитів ЄКТС включно (10 % від загального обсягу програми) та результатів навчання, отриманих у неформальній освіті (наприклад, курси Prometheus, Coursera, Cisco, соціально-освітній проєкт «Upgradey-ourselfwithlifecell», курси від компаній</li></ol>



		<p>акредитованих міжнародними рейтингами Gartner, Forrester тощо) за таких умов:</p> <ul style="list-style-type: none"><li>– зарахування кредитів для обов’язкових освітніх компонентів – не більше 50 % від обсягу кредитів для кожного окремого компонента (з метою досягнення компетентностей та програмних результатів навчання, які забезпечує цей компонент; пп. 4, 5 програми);</li><li>- результати навчання, отримані у неформальній освіті, повинні співпадати або бути близькими за змістом до програмних результатів навчання (п. 5 програми), які забезпечує компонент, за яким зараховуються кредити, отримані у неформальній освіті;</li><li>– зарахування кредитів для вибіркового освітніх компонентів – додаткові обмеження та умови відсутні.</li></ul>
<b>Розділ 4. Придатність випусників до працевлаштування та подальшого навчання</b>		
4.1	Придатність до працевлаштування	<p>Випусник може працювати на посадах, пов’язаних з дослідницько-інноваційною, професійною та науково-педагогічною діяльністю в області <b>1495 Менеджери (управителі) систем з інформаційної безпеки, 3439 Фахівець із організації інформаційної безпеки</b> відповідно до Класифікатора професій ДК 003:2010 з урахуванням цілі (п. 2.1) та фокусу програми (п. 3.3)</p>
4.2	Подальше навчання	<p>Право на продовження освіти у докторантурі. Набуття додаткових кваліфікацій у системі післядипломної освіти</p>
<b>Розділ 5. Викладання та оцінювання</b>		
5.1	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	<ol style="list-style-type: none"><li>1.Підвищення інтенсивності навчального процесу при підготовці фахівців освітньо-наукового ступеня докторі філософії.</li><li>2.Сприяння посиленню ролі методів активного пізнання у навчальному процесі здобувачів вищої освіти (аспірантів).</li><li>3.Підвищення ефективності навчання за рахунок індивідуалізації здобутих навичок здобувачів освіти.</li><li>4.Сприяння підвищенню інформатизації суспільства по оволодінню методологією наукової та педагогічної роботою.</li><li>5.Розвивання умінь, навичок та інших компетентностей здобувачів ступеня доктора філософії, що є необхідними для здійснення самостійних наукових досліджень, розв’язання комплексних проблем у галузі професійної та дослідницько-інноваційної діяльності.</li><li>6.Сприяння розвитку комунікативних здібностей аспірантів.</li><li>7.Науковим керівникам - систематично контролювати виконання освітньо-наукової програми та навчального</li></ol>



		<p>плану підготовки фахівців освітньо-наукового ступеня доктора філософії, здійснювати систематичне керівництво самостійного наукового дослідження аспіранта, аналізувати його результати, а також контролювати хід виконання індивідуального плану наукової роботи аспіранта.</p>
5.2	Оцінювання	<p>Оцінюванню в балах з дисципліни підлягає рівень знань, умінь і навичок аспірантів, що визначається при проведенні контрольних заходів у ході навчального процесу згідно з відповідними критеріями. Контрольні заходи включають поточний та підсумковий контроль.</p> <p>Поточний контроль - оцінювання рівня знань, умінь і навичок аспірантів, що здійснюється в ході навчального процесу проведенням усного опитування, контрольної роботи, тестування, колоквиуму тощо. Результати поточного контролю реєструються в журналі викладача.</p> <p>Підсумковий контроль проводиться з метою оцінювання результатів навчання на певному рівні вищої освіти або на окремих його завершальних етапах.</p> <p>Підсумковий контроль враховує семестровий контроль і атестацію здобувачів вищої освіти.</p> <p>Атестація осіб, які здобувають ступінь доктора філософії, здійснюється після успішного виконання здобувачами освітньої програми на певному рівні.</p> <p>Семестровий контроль проводиться у формі диференційованого заліку з конкретної дисципліни в обсязі матеріалу, визначеному навчальною програмою.</p> <p>У випадку, коли формою підсумкового контролю з дисципліни є диференційований залік, залікова оцінка визначається в балах за результатами виконання всіх видів навчальної роботи протягом семестру.</p> <p>До складання диференційованого заліку з кожної дисципліни допускаються всі аспіранти, які виконали навчальний план з цієї дисципліни, а також стану їхніх справ з інших дисциплін.</p> <p>Аспірантам, які не виконали навчальний план з дисципліни, викладач визначає обсяг додаткової роботи для вивчення цієї дисципліни і термін складання диференційованого заліку. Диференційований залік ці аспіранти складають після закінчення заліково-екзаменаційної сесії за умови повного виконання</p>





ОСВІТНЬО-НАУКОВА ПРОГРАМА  
«Кібербезпека»  
Спеціальність 125 - Кібербезпека  
Галузь знань 12 - Інформаційні технології  
Рівень вищої освіти - третій (освітньо-науковий)

Шифр  
документа

СМЯ НАУ  
ОНП \_\_\_\_ – 0\_ – 2021

Стор. 9 з 21

		навчального плану з дисципліни.
<b>Розділ 6. Програмні компетентності</b>		
6.1	Інтегральна компетентність (ІК)	Здатність розв'язувати комплексні проблеми в галузі професійної та / або дослідницько-інноваційної діяльності <b>за спеціальністю 125 - Кібербезпеки</b> , що передбачає глибоке переосмислення наявних та створення нових цілісних знань та / або професійної практики.
6.2	Загальні компетентності (ЗК)	<b>ЗК01.</b> Розуміння історії, джерел і форм наукової раціональності. <b>ЗК02.</b> Аксиологічний аналіз інтелектуальних і суспільних процесів. <b>ЗК03.</b> Вміння логічно й стилістично правильно видобувати письмові й усні тексти довільної тематики. <b>ЗК04.</b> Вміння ефективно і переконливо доносити свою думку до слухача. <b>ЗК05.</b> Наукова добросовісність і етика науки. <b>ЗК06.</b> Соціальна відповідальність інтелектуала.



6.3	Спеціальні (фахові) компетентності (СК)	<p><b>СК01.</b> Здатність розробляти задачі математичного моделювання та удосконалювати сучасні інформаційні технології</p> <p><b>СК02.</b> Здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності.</p> <p><b>СК03.</b> Здатність здійснювати науково-педагогічну діяльність у вищій освіті та застосовувати інноваційні освітні технології вищої школи.</p> <p><b>СК04.</b> Здатність до системного наукового світогляду, загальнокультурного кругозору, застосування сучасних методологій та методів наукової діяльності за фахом.</p> <p><b>СК05.</b> Здатність дотримуватись етики досліджень, а також правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності.</p> <p><b>СК06.</b> Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні наукові проекти в Кібербезпеці та дотичні до неї міждисциплінарні проекти, застосовувати сучасні методи наукометрії та лідерство під час їх реалізації.</p> <p><b>СК07.</b> Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та інноваційних розробок українською та англійською мовами.</p> <p><b>СК08.</b> Здатність до свідомої самоосвіти; здатність до критики й самокритики; креативність, здатність до системного мислення.</p> <p><b>СК09.</b> Здатність до практичного застосування теоретичних основ професійної діяльності: уміння здійснювати системний аналіз освітніх процесів і явищ; методична готовність до популяризації педагогічних інновацій.</p> <p><b>СК10.</b> Здатність до проектування цілей навчання й прогнозування шляхів професійного становлення майбутнього спеціаліста; уміння конструювати методичні підходи і здатність передбачати можливі результати їх впровадження; володіння методами, технологіями, способами педагогічної взаємодії, методами навчання; уміння відбирати ефективні технології навчання та виховання; здатність використовувати засвоєнні знання для проектування новітніх педагогічних технологій</p>
-----	---	---



### Розділ 7. Програмні результати навчання

7.1	Програмні результати навчання (ПР)	<p><b>ПР01.</b> Розуміння сучасних методологічних і теоретичних основ безпеки інформаційних і комунікаційних систем, технічного захисту інформації, управління інформаційною безпекою</p> <p><b>ПР02.</b> Володіти навичками творчого використання евристичних прийомів і алгоритмів, методів і засобів теоретичних і прикладних дисциплін, сучасних можливостей обчислювальної техніки і прикладного програмного забезпечення для розв'язання практичних задач забезпечення захисту інформації</p> <p><b>ПР03.</b> Здатність використовувати професійно профільовані знання в галузі математики (математичної статистики) для статистичної обробки експериментальних даних і математичного моделювання у сфері захисту інформації</p> <p><b>ПР04.</b> Здатність використовувати математичний апарат для дослідження і розвитку методів і засобів аналізу та оцінювання ризиків інформаційної безпеки</p> <p><b>ПР05.</b> Здатність використовувати математичний апарат для освоєння теоретичних основ і практичного використання методів та засобів виявлення вторгнень в інформаційні системи.</p> <p><b>ПР06.</b> Здатність використовувати теоретичні знання й практичні навички з математики, фізики, електроніки, програмування для розвитку теорії й методів забезпечення безпеки інформації в інформаційних і комунікаційних системах</p> <p><b>ПР07.</b> Здатність використовувати професійно профільовані знання й практичні навички у галузі механіки, фізики, електрики, магнетизму, оптики, ядерної фізики для дослідження у сфері технічного захисту інформації</p> <p><b>ПР08.</b> Уміння проводити вимірювальний експеримент й оцінювання його результатів на основі знань про сучасні методи метрології й стандартизації, а також використання методів аналізу й діагностики стану програмно-апаратних засобів і систем захисту інформації</p> <p><b>ПР09.</b> Уміння проводити дослідження з виявлення й блокування каналів несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію</p> <p><b>ПР10.</b> Уміння проводити експериментальні дослідження щодо виявлення наявних загроз інформації в автоматизованих системах</p>
-----	------------------------------------	--



		<p><b>ПР11.</b> Здатність використовувати знання у галузі інформаційної безпеки для аналізу різного роду загроз, зокрема, інформаційному простору, а також вміння розробляти та досліджувати моделі загроз безпеки</p> <p><b>ПР12.</b> Здатність використовувати знання, уміння та навички розроблення систем управління інформаційною безпекою</p> <p><b>ПР13</b> Здатність використовувати знання про суб'єкти інформаційної безпеки та інформаційні аспекти кібербезпеки для захисту від терористичної діяльності та гібридних війн</p> <p><b>ПР14.</b> Вміти використовувати методи та засоби обробки та кодування інформаційних сигналів.</p> <p><b>ПР15.</b> Розуміння принципів функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації, а також систем управління інформаційною безпекою</p> <p><b>ПР16</b> Уміння обробляти отримані результати, аналізувати й осмислювати їх відповідно до наявних наукових і технологічних досягнень, представляти результати роботи й обґрунтовувати запропоновані рішення на сучасному науково-технічному рівні</p> <p><b>ПР17.</b> Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки, а також суміжних і прикладних областей</p> <p><b>ПР18.</b> Володіти навичками роботи в стандартному та спеціалізованому програмному забезпеченні для обробки та аналізу даних, що захищаються</p> <p><b>ПР19.</b> Володіти навичками проектування систем захисту інформації за допомогою сучасних технологій</p>
--	--	--

### Розділ 8. Ресурсне забезпечення реалізації програми

8.1	Кадрове забезпечення	<ol style="list-style-type: none"><li>1. Наукове керівництво аспірантом здійснюється активним дослідником, який має публікації з теми, що відповідає темі дисертаційного дослідження аспіранта, результати наукової роботи керівника публікуються чи практично впроваджуються не рідше, ніж раз на два роки.</li><li>2. До наукового керівництва аспірантами не допускаються особи, які були притягнуті до відповідальності за порушення академічної доброчесності.</li><li>3. До додаткового наукового консультування аспірантів за необхідності (відповідно до їх потреб) може бути залучений будь-який науково-педагогічний чи науковий працівник факультету аеронавігації, електроніки та телекомунікацій НАУ (структурний підрозділ, який</li></ol>
-----	----------------------	--




ОСВІТНЬО-НАУКОВА ПРОГРАМА  
«Кібербезпека»  
Спеціальність 125 - Кібербезпека  
Галузь знань 12 - Інформаційні технології  
Рівень вищої освіти - третій (освітньо-науковий)

Шифр  
документа

СМЯ НАУ  
ОНП \_\_\_\_ - 0\_ - 2021

Стор. 13 з 21

		<p>забезпечує реалізацію освітньо-наукової програми відповідно до п. 1.1) з організаційним забезпеченням такого залучення з боку гаранта освітньо-наукової програми та декана зазначеного факультету.</p> <p><b>4.</b> Навчальні дисципліни та інші освітні компоненти освітньо-наукової програми викладаються та забезпечуються науково-педагогічними та науковими працівниками, наукова діяльність яких (публікації, НДР, гранти, стажування тощо) відповідає змісту зазначених навчальних дисциплін та інших освітніх компонентів, які ними викладаються та / або забезпечуються.</p> <p><b>5.</b> Представники академічної та наукової спільноти, зокрема міжнародної, а також роботодавці залучаються до організації та реалізації освітнього процесу та / або наукового консультування аспірантів.</p> <p><b>6.</b> Ураховуються вимоги п. 30 Ліцензійних умов провадження освітньої діяльності (Постанова КМУ від 30.12.2015 р. № 1187).</p>
8.2	Матеріально-технічне забезпечення	<p>Для реалізації освітньої діяльності за освітньо-науковою програмою та здійснення наукових досліджень може бути залучене за необхідності (відповідно до потреб аспірантів та потреб реалізації освітніх компонентів) будь-яке обладнання та програмне забезпечення лабораторій та аудиторний фонд кафедр <b>Безпеки інформаційних технологій</b>, а також <b>Комп'ютеризованих систем захисту інформації</b>, які входять до складу факультету <b>Кібербезпеки, комп'ютерної та програмної інженерії</b> Національного авіаційного університету (структурний підрозділ, який забезпечує реалізацію освітньо-наукової програми відповідно до п. 1.1).</p> <p>В Університеті наявна вся необхідна соціально-побутова інфраструктура (гуртожитки, їдальня, спортивні зали та відкриті спортивні майданчики, тренажерні зали, медичний комплекс), кількість місць в гуртожитках відповідає вимогам.</p>
8.3	Інформаційне та навчально-методичне забезпечення	<p>Навчально-методичні матеріали навчальних дисциплін (конспекти лекцій, лабораторні практикуми тощо), репозитарій НАУ (<a href="https://er.nau.edu.ua">https://er.nau.edu.ua</a>), ресурси Науково-технічної бібліотеки НАУ (<a href="http://www.lib.nau.edu.ua">http://www.lib.nau.edu.ua</a>), безоплатні з локальної мережі університету доступ до повнотекстових ресурсів видавництва Springer, а також повнофункціональний доступ до наукометричних баз даних Scopus та WebofScience; для публікації та апробації результатів наукових досліджень аспірантів – фахові наукові журнали НАУ (<a href="http://jrnl.nau.edu.ua">http://jrnl.nau.edu.ua</a>, <a href="http://jrnl.nau.edu.ua/index.php/ZI">http://jrnl.nau.edu.ua/index.php/ZI</a>,</p>

	<b>ОСВІТНЬО-НАУКОВА ПРОГРАМА</b> «Кібербезпека» Спеціальність 125 - Кібербезпека Галузь знань 12 - Інформаційні технології Рівень вищої освіти - третій (освітньо-науковий)	Шифр документа	СМЯ НАУ ОНП ____ - 0_ - 2021
		Стор. 14 з 21	

		<a href="http://jrnl.nau.edu.ua/index.php/Infosecurity">http://jrnl.nau.edu.ua/index.php/Infosecurity</a> ), конференції “Безпека інформаційних технологій (ITsec)”, “Безпека ресурсів інформаційних систем (SITS)”, “Актуальні питання забезпечення кібербезпеки та захисту інформації (CICISIS)”, “Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS)”, організатором чи співорганізатором яких є НАУ та публікації в яких індексуються наукометричними базами даних Scopus та WebofScience ( <a href="http://ieec.nau.edu.ua">http://ieec.nau.edu.ua</a> ).
<b>Розділ 9. Академічна мобільність</b>		
9.1	Національна кредитна мобільність	Відповідно до Положення про порядок реалізації права на академічну мобільність у Національному авіаційному університеті, введеного в дію наказом ректора від 09.07.2019 р. № 336/од. Програми міжнародної академічної мобільності Erasmus+, Mevlana.
9.2	Міжнародна кредитна мобільність	
9.3	Навчання іноземних здобувачів вищої освіти	Реалізація освітньої та наукових складових освітньо-наукової програми англійською мовою для іноземців та осіб без громадянства (за потреби), врахування особливостей передумов, викладених у п. 1.8, умови вступу для іноземців та осіб без громадянства регулюються Правилами прийому до аспірантури та докторантури Національного авіаційного університету .


## 2. Перелік компонентів освітньо-наукової програми та їх логічна послідовність

### 2.1. Перелік компонентів

(Код н/д)	Компоненти освітньо-наукової програми	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
<b>Обов’язкові компоненти</b>				
1.1	<b><i>Цикл дисциплін з оволодіння загальнонауковими (філософськими) компетентностями</i></b>			
OK1.1.1	Філософія науки та інновацій	3	Екзамен	1
1.2	<b><i>Цикл дисциплін із набуття універсальних навичок дослідника та викладача</i></b>			
OK1.2.1	Правове, економічне та інформаційне забезпечення наукових досліджень	3	Диф. залік	1
1.3	<b><i>Цикл дисциплін із оволодіння глибинними знаннями зі спеціальності</i></b>			



OK1.3.1	Наукові засади управління інформаційною безпекою	4	Диф. залік	2
OK1.3.2	Методи і засоби аналізу та оцінювання ризиків інформаційної безпеки	3	Екзамен	3
1.4	<b>Цикл дисциплін зі здобуття мовних компетентностей</b>			
OK1.4.1	Англійська мова наукового спрямування	6	Екзамен	1
1.5	<b>Цикл практичної підготовки</b>			
OK1.5.1	Фахова науково-педагогічна практика	6	Диф. залік	2
	Дисертаційна робота доктора філософії		Захист	8
<b>Загальний обсяг обов'язкових компонентів:</b>		<b>25 кредитів ЄКТС</b>		
<b>Вибіркові компоненти*</b>				
Вибірковий блок 1				
ВК1	Сучасні методи викладання у вищій школі	3	Диф. залік	2
ВК2	Менеджмент			
Вибірковий блок 2				
ВК3	Інноваційні методи прийняття рішень в соціотехнічних та соціокультурних системах	3	Диф. залік	2
ВК4	Когнітивні технології прогнозування стану соціотехнічних та соціокультурних систем			
Вибірковий блок 3				
ВК5	Технології виявлення зловмисного програмного забезпечення	3	Диф. залік	4
ВК6	Теорія захисту інформаційних ресурсів обмеженого доступу			
Вибірковий блок 4				
ВК7	Методи і засоби аналізу та оцінювання ризиків інформаційної безпеки	4	Екзамен	2
ВК8	Технології виявлення вразливостей мережевих ресурсів			
Вибірковий блок 5				
ВК9	Методи та засоби виявлення вторгнень в інформаційних системах	6	Екзамен	3
ВК10	Методи та засоби обробки та кодування інформаційних сигналів			
Вибірковий блок 6				

	<b>ОСВІТНЬО-НАУКОВА ПРОГРАМА</b> «Кібербезпека» Спеціальність 125 - Кібербезпека Галузь знань 12 - Інформаційні технології Рівень вищої освіти - третій (освітньо-науковий)	Шифр документа	СМЯ НАУ ОНП ____ – 0_ – 2021
		Стор. 16 з 21	


ВК11	Методи та засоби компресії цифрових сигналів	6	Диф. залік	4
ВК12	Технології забезпечення безпеки мережевої інфраструктури			
<b>Загальний обсяг вибірових компонент 25 кредитів ЄКТС</b>				
<b>Загальний обсяг освітньої складової освітньо-наукової програми 50 кредитів ЄКТС</b>				

*\*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.*

#### 4. Наукова складова

Рік підготовки	Зміст наукової роботи здобувача вищої освіти (аспіранта)	Форма контролю
Перший рік	Вибір теми дисертаційного дослідження аспіранта, формування індивідуального плану роботи здобувача вищої освіти; виконання дисертаційної роботи під керівництвом наукового керівника; підготовка та подання до друку не менше однієї публікації за темою дисертації та участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей	Затвердження на вченій раді факультету / інституту, звітування двічі на рік про виконання індивідуального плану аспіранта
Другий рік	Виконання під керівництвом наукового керівника дисертаційного дослідження; підготовка та подання до друку не менше однієї публікації за темою дисертації відповідно чинних вимог; участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей	Звітування про хід виконання індивідуального плану аспіранта двічі на рік
Третій рік	Виконання під керівництвом наукового керівника дисертаційної роботи; підготовка та подання до друку не менше двох публікації за темою дисертації відповідно чинних вимог; участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей	Звітування про хід виконання індивідуального плану аспіранта двічі на рік
Четвертий рік	Завершення та оформлення дисертаційної роботи, підведення підсумків щодо повноти висвітлення результатів дисертації у наукових статтях відповідно чинних вимог; подання документів на попередню експертизу дисертації; підготовка наукової доповіді для підсумкової атестації (захисту дисертації) Звітування про хід виконання індивідуального плану аспіранта двічі на рік.	Надання висновку про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження



	<p>ОСВІТНЬО-НАУКОВА ПРОГРАМА «Кібербезпека» Спеціальність 125 - Кібербезпека Галузь знань 12 - Інформаційні технології Рівень вищої освіти - третій (освітньо-науковий)</p>	Шифр документа	СМЯ НАУ ОНП ____ – 0_ – 2021
		Стор. 17 з 21	

### 3. Форма атестації здобувачів вищої освіти

Підсумкова атестація здобувачів вищої освіти за освітньо-науковою програмою **Підготовки докторів філософії спеціальності 125 - Кібербезпека** проводиться у формі у дисертаційної роботи та завершується видачею документа встановленого зразка про присудження йому ступеня доктора філософії з присвоєнням кваліфікації «Доктор філософії з кібербезпеки».

*Відповідно до п. 30 «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук», затвердженого Постановою КМУ № 261 від 23.03.2016 р.:*

**3.1.** Атестація здобувачів вищої освіти ступеня доктора філософії здійснюється постійно діючою або разовою спеціалізованою вченою радою на підставі публічного захисту наукових досягнень у формі дисертації.

**3.2.** Стан готовності дисертації аспіранта до захисту визначається науковим керівником (або консенсусним рішенням двох керівників);

**3.3.** Обов'язковою умовою допуску до захисту є успішне виконання аспірантом його індивідуального навчального плану та індивідуального плану наукової роботи.



#### 4. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

	ОК 1.1.1	ОК 1.1.3	ОК 1.3.1	ОК 1.3.2	ОК 1.4.1	ОК 1.5.1	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК9	ВК10	ВК11	ВК12
ЗК01	X		X	X	X		X	X						X	X	X	
ЗК02		X					X		X	X			X				X
ЗК03	X		X	X	X	X		X			X	X		X	X	X	
ЗК04	X	X		X	X	X				X			X	X			
ЗК05	X							X	X		X						
ЗК06		X			X				X	X			X				
СК01			X	X								X	X	X			X
СК02				X										X	X		
СК03			X			X					X					X	
СК04			X										X				X
СК05				X							X			X			
СК06				X									X	X	X	X	
СК07				X	X								X	X	X	X	X
СК08			X			X					X	X					
СК09													X		X	X	
СК10			X	X		X					X			X			



### 5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК 1.1.1	ОК 1.1.3	ОК 1.3.1	ОК 1.3.2	ОК 1.4.1	ОК 1.5.1	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК9	ВК10	ВК11	ВК12
ПР01						X	X	X			X	X	X	X		X	
ПР02		X		X			X	X					X	X		X	
ПР03						X						X					
ПР04						X	X	X				X	X	X			X
ПР05						X	X	X			X	X	X	X	X		
ПР06								X						X		X	
ПР07							X	X	X	X	X	X	X	X			X
ПР08		X	X					X						X		X	
ПР09						X	X	X			X	X	X	X			
ПР10						X	X	X			X	X	X	X	X		
ПР11					X		X					X	X			X	X
ПР12		X		X			X		X	X	X	X	X			X	
ПР13						X	X	X				X	X	X	X		
ПР14							X	X			X		X	X		X	
ПР15								X						X			X
ПР16	X		X		X				X	X	X				X		
ПР17				X	X	X						X					
ПР18							X	X			X		X	X		X	
ПР19						X	X	X				X	X	X			



